USC
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

Curvas algebraicas y cuerpos de funciones

Andrea Martínez Sánchez

2018/2019

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

Curvas algebraicas y cuerpos de funciones

Andrea Martínez Sánchez

Julio 2019

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Trabajo propuesto

Área de Coñecemento: Álgebra
Título: Curvas algebraicas y cuerpos de funciones
Breve descrición do contido
En este trabajo trataremos los rudimentos del estudio algebraico de la geometría. En concreto, una curva algebraica define un cuerpo de funciones racionales que es una extensión de grado de trascendencia 1 sobre el cuerpo base. Se estudiará cómo reconstruir la curva a partir de este cuerpo y cómo estudiar alguna de sus propiedades básicas.
Recomendacións
Outras observacións

Índice general

Resumen

Este trabajo consiste en una primera aproximación al estudio de la geometría algebraica y su confluencia con el álgebra conmutativa. En primer lugar, se introduce la noción de plano proyectivo tanto de manera axiomática como analítica. El plano proyectivo surge de la idea de añadir nuevos puntos al plano afín, los cuales denominaremos puntos del infinito. Esto nos permitirá estudiar la forma natural de sumergir el plano afín en el plano proyectivo. Posteriormente, nos adentraremos en el estudio de las variedades algebraicas afines y proyectivas, así como la transferencia entre ellas. En concreto, profundizaremos en las curvas algebraicas, que son variedades de dimensión 1 y veremos que definen un cuerpo de funciones racionales, un objeto algebraico dotado de gran importancia. Finalmente, se estudiará cómo reconstruir la curva a partir de este cuerpo. Para ello, introduciremos el concepto de punto no singular de una curva y exploraremos los fundamentos de los anillos de valoración discreta.

Abstract

This work consists of a first approach to the study of algebraic geometry and its confluence with commutative algebra. First, the notion of the projective plane is introduced both axiomatically and analytically. The projective plane stems from the idea of adding new points to the affine plane, that we will denominate points at infinity. This will allow us to study the natural way of embedding the affine plane into the projective plane. Subsequently, we are going into the study of affine and projective algebraic varieties, as well as the transfer between them. In particular, we will delve into the algebraic curves, which are varieties of dimension 1, and we will see that they define a field of rational functions, an algebraic object endowed with great importance. Finally, we will study how to reconstruct the curve from this field. To that end, we will introduce the concept of non singular point of a curve and we will explore the fundamentals of discrete valuation rings.

Introducción

Una curva algebraica plana es el conjunto de puntos del plano que satiface una ecuación polinómica en dos variables. Las rectas satisfacen una ecuación lineal y el siguiente caso lo forman las cónicas, que satisfacen una ecuación de grado 2 y fueron estudiadas ya en la antiguedad por Apolonio. A partir del grado 3 la fenomenología de las curvas es más compleja y se requieren diversas técnicas para su estudio. Dado el planteamiento algebraico del problema, es razonable plantear su estudio sobre cuerpos de coeficientes arbitrarios. El teorema de los ceros de Hilbert garantiza un comportamiento razonable si el cuerpo es algebraicamente cerrado. En característica cero, esto supone centrarse en los números complejos, pero en característica positiva existen cuerpos algebraicamente cerrados que también son interesantes.

Además, la consideración del plano proyectivo permite trabajar de forma explícita con los puntos del infinito. Esto supone pasar a una ecuación homogénea en tres variables. En este trabajo construiremos ciertos invariantes algebraicos asociados a la curva. Si la curva es afín, mediante el ideal generado por su ecuación construimos el anillo de coordenadas. En el caso proyectivo se tiene un anillo graduado: el anillo de coordenadas homogéneas. Un objeto particularmente importante es el cuerpo de funciones racionales. Geométricamente, se interpreta como funciones regulares definidas sobre un abierto de la curva. Abstractamente, es un cuerpo de extensión de grado de trascendencia 1 sobre el cuerpo base. Es una versión algebraica del cuerpo de funciones meromorfas.

El teorema principal de este trabajo es que, a partir del cuerpo de funciones racionales de una curva plana no singular, es posible recuperar los puntos de una curva mediante un procedimiento algebraico. Los puntos se corresponden a los anillos de valoración discreta no triviales contenidos en el cuerpo. Un anillo de valoración discreta es un dominio de ideales principales que es local, es decir, que posee un único maximal. Esta construcción proporciona un puente entre la geometría de la curva y la aritmética de sus funciones.

Este trabajo consta de tres capítulos. En lineas generales el primer capítulo desarolla la noción de plano proyectivo, el segundo se centra en los fundamentos del estudio algebraico de la geometría y el último en el análisis de las propiedades locales de las curvas con el fin último de llegar a probar el teorema principal mencionado previamente.

A continuación se ofrece un esquema más detallado del contenido por capítulos.

El primer capítulo de este trabajo está íntegramente dedicado a la descripción del plano proyectivo. La motivación de la construcción de este plano se basa en el objetivo de reducir al mínimo los casos particulares que distingue la geometría afín del plano. En primer lugar, proporcionaremos una definición axiomática de plano proyectivo y veremos, a partir de ella, cómo extender el plano afín usual a un plano proyectivo. Veremos que hay planos proyectivos que se consiguen a través de espacios vectoriales, que son denominados analíticos, y daremos una descripción de los mismos. También comprobaremos que, en efecto, verifican la definición axiomática. Al final del capítulo estudiaremos la forma natural de inmersión del plano afín en el plano proyectivo. Veremos tres encajes posibles, donde cada uno de los cuales deja fuera su correspondiente recta del infinito. Los complementarios de tres rectas forman así un recubrimiento del plano proyectivo por tres planos afines. Además, calcularemos el punto del infinito de una recta afín general para mostrar que éste determina la clase de paralelismo de la recta que, a su vez, viene determinada por su pendiente.

El segundo capítulo se centra en el estudio de las variedades algebraicas con la intención de proporcionar un puente o diccionario entre los objetos algebraicos y geométricos. Partiendo de la idea intuitiva de que una curva plana afín es el conjunto de puntos del plano afín que son ceros de un polinomio, llegaremos a las definiciones, más generales, de conjunto algebraico e ideal de anulación. Mencionaremos tres versiones, débil, fuerte y geométrica, del teorema de los ceros de Hilbert. El teorema de los ceros de Hilbert, también conocido como *Nullstellensatz*, será clave en relación a la construcción del puente entre el álgebra y la geometría pues nos permitirá probar la correspondencia entre puntos del plano afín e ideales maximales en el anillo de polinomios en dos variables. Asimismo, ahondaremos en la cuestión de irreducibilidad de un conjunto algebraico. Definiremos el anillo de coordenadas y veremos que en el caso de variedades podemos considerar el cuerpo de funciones racionales, que es el cuerpo fracciones que lo contiene. A partir de estas ideas, daremos la definición de anillo local en un punto de una variedad y describiremos a su ideal maximal. Finalmente, trataremos la forma de extender los conceptos anteriores al plano proyectivo. Para ello será necesario describir los procesos de homogeneización y deshomogeneización

de polinomios e ideales, así como examinar la noción de clausura proyectiva.

El último capítulo está destinado a proporcionar los elementos necesarios para la prueba del teorema primordial de este trabajo, que afirma que los puntos de una curva plana no singular se corresponden a los anillos de valoración discreta no triviales contenidos en su cuerpo de funciones racionales. Estos elementos serán el concepto de punto singular, espacio tangente, cono tangente y anillos de valoración discreta, que se estudian durante las primeras secciones del capítulo. En la sección siguiente se probaran varios resultados que nos conducirán a la afirmación de que los anillos locales de los puntos de una curva plana no singular son anillos de valoración discreta. Concluiremos con una sección que recoge la demostración del teorema principal, así como los preliminares requeridos para su prueba.

Este trabajo ha sido desarollado a partir de la consulta de los libros que se incorporan en la bibliografía, tratando, en todo momento, de buscar la notación y explicación más conveniente con el propósito de lograr que su comprensión sea lo más intuitiva posible.

Capítulo 1

Plano proyectivo

1.1. Motivación

En el estudio de la posición relativa de dos rectas, la geometría afín del plano distingue dos casos. Si tomamos un par de rectas distintas se pueden dar dos situaciones: que se corten o que no (en este segundo caso, decimos que son paralelas). El objetivo es tratar de reducir estos dos casos a uno, para ello, se introducen nuevos puntos. La idea es añadir más puntos, los puntos del infinito, y decretar que dos rectas paralelas se cortan en uno de esos nuevos puntos. Estos puntos del infinito se disponen en una recta. Al añadir los puntos del infinito al plano afín obtendremos lo que se conoce como plano proyectivo. Veamos a continuación cómo llevar a cabo esta idea de forma precisa.

1.2. Plano proyectivo sintético

Veamos, en primer lugar, la definición axiomática del plano proyectivo.

Definición 1.1. Un plano proyectivo es una terna $(\mathcal{P}, \mathcal{L}, \mathrm{I})$. El conjunto $\mathcal{P}$ está formado por los puntos y el conjunto $\mathcal{L}$ por las rectas de la geometría. La inclusión $\mathrm{I} \subseteq \mathcal{P} \times \mathcal{L}$ es una relación de incidencia verificando los siguientes tres axiomas:

(i) Para cada par de puntos distintos, existe exactamente una recta que incide con ambos.

(ii) Para cada par de rectas distintas, existe exactamente un punto que incide con ambas.

(iii) Hay cuatro puntos distintos tales que ninguna recta incide con más de dos de ellos.

Observación 1.2. Nótese que (i) y (ii) describen una relación de simetría total entre puntos y rectas. Por otro lado, (iii) simplemente asegura que la estructura no es un caso trivial donde

la mayor parte de los puntos son colineales, entendiendo por puntos colineales aquellos que pertenecen a una misma recta, y, por tanto, no corresponde a la idea de plano.

Ejemplo 1.3. (Extensión del plano afín usual a un plano proyectivo)
Sea $\mathbb{A}^2 = (\mathcal{P}_\mathbb{A}, \mathcal{L}_\mathbb{A}, \mathrm{I}_\mathbb{A})$ el plano afín usual donde $\mathcal{P}_\mathbb{A}$ son los puntos, $\mathcal{L}_\mathbb{A}$ son las rectas e $\mathrm{I}_\mathbb{A}$ la relación de incidencia usual en dicho plano. Vamos a introducir ahora los elementos en el infinito.
Para una recta l, consideramos la clase de equivalencia $[l]$ de todas las rectas paralelas a l. Para cada clase de equivalencia, definimos un nuevo punto $p_{[l]}$ que será el punto del infinito incidente con todas las rectas de $[l]$. Además, definimos una recta en el infinito l_∞ en la que inciden todos los $p_{[l]}$. Formalmente resultaría:

- $\mathcal{P} = \mathcal{P}_\mathbb{A} \cup \{p_{[l]} \,|\, l \in \mathcal{L}_\mathbb{A}\}$,
- $\mathcal{L} = \mathcal{L}_\mathbb{A} \cup \{l_\infty\}$,
- $\mathrm{I} = \mathrm{I}_\mathbb{A} \cup \{(p_{[l]}, l) \,|\, l \in \mathcal{L}_\mathbb{A}\} \cup \{(p_{[l]}, l_\infty) \,|\, l \in \mathcal{L}_\mathbb{A}\}$.

$(\mathcal{P}, \mathcal{L}, \mathrm{I})$ satisface los axiomas de plano proyectivo. Veámoslo:

(i) Para ver que para cada par de puntos distintos existe exactamente una recta que incide con ambos distinguimos tres casos:

- Si $p, q \in \mathcal{P}_\mathbb{A}$, entonces la recta que incide con ambos es la que incide con ambos en el plano afín usual.
- Si $p \in \mathcal{P}_\mathbb{A}$ y $q = p_{[l]}$ para alguna recta $l \in \mathcal{L}_\mathbb{A}$, entonces la recta que incide con ambos en $\mathcal{P}$ es aquella recta $l' \in [l]$ que incide con p.
- Si $p = p_{[l]}$ y $q = p_{[m]}$ para dos rectas $l, m \in \mathcal{L}_\mathbb{A}$, entonces la recta que incide con ambos es la recta en el infinito l_∞.

(ii) Veamos ahora que para cada par de rectas distintas existe exactamente un punto que incide con ambas. Se pueden dar las siguientes situaciones:

- Si $l, m \in \mathcal{L}_\mathbb{A}$ y son no paralelas, entonces el punto que incide con ambas es el que incide con ellas en el plano afín usual.
- Si $l, m \in \mathcal{L}_\mathbb{A}$ y son paralelas, entonces el punto $p_{[l]} = p_{[m]}$ incide con ambas.
- Si $l = l_\infty$ y $m \in \mathcal{L}_\mathbb{A}$, entonces el punto que incide con ambas es $p_{[m]}$.

(iii) Falta ver que existen cuatro puntos distintos tales que ninguna recta incide con más de dos de ellos. Esto ya se verifica en el plano afín pues, dados $p, r, q \in \mathcal{P}_\mathbb{A}$ puntos no

alineados sean $l, m \in \mathcal{L}_{\mathbb{A}}$ tales que l incide con p y q y m incide con p y r. Considerando l', recta paralela a l incidente con r y m', recta paralela a m incidente con q obtenemos el punto $s = l' \cap m'$ que junto con los puntos p, q y r satisfacen el tercer axioma.

1.3. Plano proyectivo analítico

Una forma de conseguir planos proyectivos es a través de espacios vectoriales. Estos planos proyectivos se denominan analíticos, ya que se especifican mediante coordenadas, mientras que los planos proyectivos sintéticos se especifican axiomáticamente. Se pueden construir planos proyectivos sintéticos que no corresponden a un plano proyectivo analítico. Nosotros no haremos uso de estos objetos.

Sea $\mathbb{K}$ un cuerpo y sea $\mathbb{K}^3$ el espacio vertorial de dimensión tres sobre este cuerpo. Probaremos que si definimos los subespacios unidimensionales de $\mathbb{K}^3$ como puntos, los subespacios bidimensionales de $\mathbb{K}^3$ como rectas y la relacion de incidencia como la relación de contenido entre subespacios, obtenemos un plano proyectivo que se denominará plano proyectivo analítico.

Consideramos la relación de equivalencia $\sim_{\mathbb{K}}$ en $\mathbb{K}^3 - \{(0,0,0)\}$ dada por

$$x \sim_{\mathbb{K}} y \iff \exists \lambda \in \mathbb{K} - \{0\} \text{ tal que } x = \lambda \cdot y$$

La clase de equivalencia de $x = (x_1, x_2, x_3) \in \mathbb{K}^3$, que denotaremos por $[x]$ o por $(x_1 : x_2 : x_3)$ estará formada por todos los vectores de $\mathbb{K}^3 - \{(0,0,0)\}$ que difieran del vector x por un escalar no nulo, en otros términos, por la recta que pasa por x y el 0 sin contar este último. El conjunto de puntos del plano proyectivo es el conjunto de todas las clases de equivalencia y se denota por $\mathcal{P}_{\mathbb{K}} = \frac{\mathbb{K}^3 - \{(0,0,0)\}}{\sim_{\mathbb{K}}}$.

Una recta de $\frac{\mathbb{K}^3 - \{(0,0,0)\}}{\sim_{\mathbb{K}}}$ se corresponde con un subespacio vectorial $V \subset \mathbb{K}^3$ de dimensión 2.

Recordamos que, en general, si W es un $\mathbb{K}-$espacio vectorial, se define el dual de W, que se denota por $\hat{W}$, como el conjunto de las aplicaciones lineales de W en $\mathbb{K}$, es decir, $\hat{W} := \mathcal{L}(W, \mathbb{K})$. Podemos considerar entonces la paridad canónica:

$$\begin{aligned} W \times \hat{W} &\xrightarrow{\Phi} \mathbb{K} \\ (w, \varphi) &\longmapsto \varphi(w) \end{aligned}$$

Denominaremos a w vector y a φ covector.

Si la dimensión de W es finita, también lo es la de $\hat{W}$, y, además, coinciden. En este caso, podemos identificar W con $\mathbb{K}^n$ a través de una base $\mathcal{B} = \{w_1, \cdots, w_n\}$ y $\hat{W}$ con $\hat{\mathbb{K}}^n$ a través de una base $\hat{\mathcal{B}} = \{\varphi_1, \cdots, \varphi_n\}$, donde $\varphi_i(w_j) = 1$, si $j = i$ y $\varphi_i(w_j) = 0$, si $j \neq i$. Entonces:

$$\varphi(w) = \begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = a_1x_1 + \ldots + a_nx_n$$

Igualando a cero obtenemos el siguiente hiperplano

$$\varphi(w) = a_1x_1 + \ldots + a_nx_n = 0$$

Obsérvese la paridad canónica, aplicada al caso que nos ocupa

$$\mathbb{K}^3 \times \hat{\mathbb{K}}^3 \xrightarrow{\Phi} \mathbb{K},$$

donde $\hat{\mathbb{K}}^3 = \mathcal{L}(\mathbb{K}^3, \mathbb{K})$, definida por $\Phi(x, l) := l(x)$. Si V tiene dimensión 2, entonces el conjunto de los elementos anulados por V, $V^\perp$, tiene dimensión 1 y existirá un covector $l \in \hat{\mathbb{K}}^3$, $l \neq 0$ tal que $V^\perp = \langle l \rangle$, de modo que podemos representar V por l salvo múltiplo escalar.

Por tanto, $\mathcal{L}_\mathbb{K} = \frac{\hat{\mathbb{K}}^3 - \{(0,0,0)\}}{\sim_\mathbb{K}}$ es el conjunto de las rectas de nuestra geometría proyectiva.

Finalmente, la relación de incidencia $\mathrm{I}_\mathbb{K} \subseteq \mathcal{P}_\mathbb{K} \times \mathcal{L}_\mathbb{K}$ entre $[x] \in \mathcal{P}_\mathbb{K}$ y $[l] \in \mathcal{L}_\mathbb{K}$ la definimos como

$$[x]\mathrm{I}_\mathbb{K}[l] : \Longleftrightarrow \ l(x) = 0.$$

Nótese que dicha condición no depende de la clase de $x \in \mathbb{K}^3$ ni de la clase de $l \in \hat{\mathbb{K}}^3$.

Se tiene, por tanto, el siguiente resultado.

Teorema 1.4. *La terna $(\mathcal{P}_\mathbb{K}, \mathcal{L}_\mathbb{K}, I_\mathbb{K})$ verifica los axiomas de plano proyectivo.*

Demostración. Tenemos que ver que $(\mathcal{P}_\mathbb{K}, \mathcal{L}_\mathbb{K}, \mathrm{I}_\mathbb{K})$ verifica los tres axiomas de la definición de plano proyectivo sintético.

(i) Veamos que para cada par de puntos distintos existe exactamente una recta que incide con ambos: sean $[x], [y] \in \mathcal{P}_\mathbb{K}$ distintos con $x = (x_1, x_2, x_3)$ e $y = (y_1, y_2, y_3)$, entonces la matriz:

$$\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \end{pmatrix}$$

tiene rango 2 pues x e y no se diferencian por un múltiplo escalar no nulo. Luego, la clase de $l = (l_1, l_2, l_3)$ tal que satisface:

$$\begin{pmatrix} l_1 & l_2 & l_3 \end{pmatrix} \cdot \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

es la recta que incide con $[x]$ e $[y]$. En términos de la paridad Φ, podemos escribir $\langle l \rangle = \langle x, y \rangle^{\perp}$.

(ii) Veamos ahora, de un modo análogo al anterior, que para cada par de rectas distintas, existe exactamente un punto que incide con ambas: sean $[l], [m] \in \mathcal{L}_{\mathbb{K}}$ distintas con $l = (l_1, l_2, l_3)$ e $m = (m_1, m_2, m_3)$, entonces la matriz:

$$\begin{pmatrix} l_1 & l_2 & l_3 \\ m_1 & m_2 & m_3 \end{pmatrix}$$

tiene rango 2 pues l y m no se diferencian por un múltiplo escalar no nulo. Luego, la clase de $x = (x_1, x_2, x_3)$ tal que satisface:

$$\begin{pmatrix} l_1 & l_2 & l_3 \\ m_1 & m_2 & m_3 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

es el punto que incide con $[l]$ y $[m]$.Como antes, en términos de la paridad Φ, $\langle x \rangle = {}^{\perp}\langle l, m \rangle$.

(iii) Falta ver que existen cuatro puntos distintos tales que ninguna recta incide con más de dos de ellos. Como $\mathbb{K}$ es un cuerpo, contiene elemento neutro para la suma, 0, y elemento neutro para la multiplicación, 1. Basta considerar entonces los puntos $[(0,0,1)]$, $[(0,1,1)]$, $[(1,0,1)]$ y $[(1,1,1)]$ para probar el tercer axioma.

□

1.4. Inmersión del plano afín en el plano proyectivo

Existe una forma natural de introducir el plano afín estándar $\mathbb{A}^2(\mathbb{K})$ dentro de $\mathbb{P}^2(\mathbb{K})$. Sea $\mathbb{A}^2(\mathbb{K})$ el plano afín con espacio vectorial asociado $\mathbb{K}^2$. En $\mathbb{K}^3$ identificamos $\mathbb{A}^2(\mathbb{K})$ con

el plano de ecuación $Z = 1$. Así, los puntos $(x, y) \in \mathbb{A}^2(\mathbb{K})$ los podemos ver como puntos de $\mathbb{P}^2(\mathbb{K})$ de la siguiente manera

$$\begin{aligned} \varphi_2 : \mathbb{A}^2(\mathbb{K}) &\longrightarrow \mathbb{P}^2(\mathbb{K}) \\ (x, y) &\longmapsto (x : y : 1). \end{aligned}$$

Mediante la anterior aplicación inyectiva hemos identificado $\mathbb{A}^2(\mathbb{K})$ con el subconjunto de $\mathbb{P}^2(\mathbb{K})$ dado por $\{(x : y : 1) \in \mathbb{P}^2(\mathbb{K}) \,|\, x, y \in \mathbb{K}\}$. De este modo, recorremos todos los puntos del plano proyectivo salvo aquellos tales que $z = 0$, pues cualquier otro será un múltiplo de la terna $(x : y : 1)$. En efecto, dado el punto $(x : y : z) \in \mathbb{P}^2(\mathbb{K})$, éste también puede verse como el punto $(x/z : y/z : 1)$, que se identifica con el punto $(x/z, y/z)$ del plano afín. Los puntos de la forma $(x : y : 0)$ conforman una recta en el plano proyectivo $\mathbb{P}^2(\mathbb{K})$, son las clases de los vectores no nulos de un subespacio bidimensional de $\mathbb{K}^3$. Esta recta es la denominada recta del infinito y dos rectas paralelas del espacio afín llevadas al plano proyectivo se cortan en un punto de esta recta del infinito. Una forma de visualizar esto es pensar que cada uno de los puntos de la recta del infinito representa una dirección en el espacio afín.

Consideremos la recta $aX + bY + c = 0$ en el plano afín. Su correspondiente clausura proyectiva, veremos posteriormente que viene dada por $aX + bY + cZ = 0$. Para calcular su punto del infinito basta intersecar $aX + bY + cZ = 0$ con la recta del infinito $Z = 0$. Esta intersección se produce en el punto $(b : -a : 0) = (1 : -a/b : 0)$, si $b \neq 0$. Observamos entonces que $-a/b$ es la pendiente de la recta inicial en el plano afín y que c no interviene. Es claro, por tanto, que el punto del infinito es el mismo para todas las rectas paralelas a la inicial, esto es, el punto del infinito determina la clase de paralelismo de la recta y esta clase está determinada por su pendiente.

Observación 1.5. Nótese que, de la misma forma que en este caso hemos introducido un 1 en la última posición, éste podría introducirse en cualquiera de las otras dos posiciones, dando lugar a dos nuevos encajes del plano proyectivo que vendrían dados por

$$\begin{aligned} \varphi_0 : \mathbb{A}^2(\mathbb{K}) &\longrightarrow \mathbb{P}^2(\mathbb{K}) \\ (x, y) &\longmapsto (1 : y : z) \end{aligned}$$

$$\begin{aligned} \varphi_1 : \mathbb{A}^2(\mathbb{K}) &\longrightarrow \mathbb{P}^2(\mathbb{K}) \\ (x, y) &\longmapsto (x : 1 : z) \end{aligned}$$

De esta modo, estaríamos identificando $\mathbb{A}^2(\mathbb{K})$ con el subconjunto de $\mathbb{P}^2(\mathbb{K})$ dado por

$$\{(1 : y : z) \in \mathbb{P}^2(\mathbb{K}) \,|\, y, z \in \mathbb{K}\},$$

o con

$$\{(x : 1 : z) \in \mathbb{P}^2(\mathbb{K}) \,|\, x, z \in \mathbb{K}\},$$

respectivamente. De esta forma, se recorren todos los puntos del plano proyectivo salvo aquellos tales que $x = 0$ en el caso de φ_0, o aquellos tales que $y = 0$ en el caso de φ_1. En este sentido, podemos ver el plano proyectivo $\mathbb{P}^2(\mathbb{K})$ como la unión de $\mathbb{A}^2(\mathbb{K})$ con la recta del infinito correspondiente a cada caso. Denominando $\mathcal{U}_i$ a la imagen de φ_i observamos también que $\mathbb{P}^2(\mathbb{K}) = \mathcal{U}_2 \cup \mathcal{U}_1 \cup \mathcal{U}_0$.

Capítulo 2

Curvas algebraicas

2.1. Curvas afines

Intuitivamente, una curva plana afín será el conjunto de puntos del plano afín que son ceros de un polinomio.

Definición 2.1. Sea $\mathbb{A}^2(\mathbb{K})$ el plano afín y sea f un polinomio en $\mathbb{K}[X,Y]$. Un punto $(x,y) \in \mathbb{A}^2(\mathbb{K})$ se dice un cero de f si $f(x,y) = 0$.

Definición 2.2. Sea $\mathbb{A}^2(\mathbb{K})$ el plano afín y sea f un polinomio no constante en $\mathbb{K}[X,Y]$. El conjunto de ceros de f,

$$v(f) = \{(x,y) \in \mathbb{A}^2(\mathbb{K}) \mid f(x,y) = 0\},$$

se llama curva plana afín. El grado de f se dice grado de $v(f)$ u orden de $v(f)$. En general, si $S \subset \mathbb{K}[X,Y]$ se define el conjunto de ceros de S como

$$v(S) = \{(x,y) \in \mathbb{A}^2(\mathbb{K}) \mid f(x,y) = 0, \forall f \in S\}.$$

Esto es, el conjunto de puntos del plano afín que son ceros comunes a un conjunto S de polinomios en $\mathbb{K}[X,Y]$.

Observación 2.3. Nótese que por las definiciones previas se tiene que $v(S) = \cap_{f \in S} v(f)$.

Observación 2.4. Si $\langle S \rangle \subset \mathbb{K}[X,Y]$ es el ideal generado por S, entonces $v(S) = v(\langle S \rangle)$. De esta forma, hemos asociado un conjunto de polinomios (o el ideal que generan) con un conjunto de puntos del plano afín.

Definición 2.5. Un anillo conmutativo unitario A se dice que es un anillo noetheriano si todos sus ideales son finitamente generados.

Observación 2.6. Nótese que, por el teorema de la base de Hilbert [AM, Cap. 7, Teor. 7.5.], sabemos que $\mathbb{K}[X,Y]$ es un anillo noetheriano, ya que $\mathbb{K}$ es un cuerpo y todo cuerpo es un anillo noetheriano, luego todo ideal de $\mathbb{K}[X,Y]$ estará finitamente generado. Por lo tanto, esto nos permite afirmar que aunque S sea un conjunto infinito, $v(S)$ siempre se puede expresar como el conjunto de ceros comunes a un conjunto finito de polinomios.

2.2. Conjuntos algebraicos

Definición 2.7. Un subconjunto $V \subset \mathbb{A}^2(\mathbb{K})$ es un conjunto algebraico afín, o simplemente un conjunto algebraico, si $V = v(S)$ para algún $S \subset \mathbb{K}[X,Y]$.

Proposición 2.8. *La intersección de conjuntos algebraicos es un conjunto algebraico y la unión finita de conjuntos algebraicos es un conjunto algebraico. Además,* $\mathbb{A}^2(\mathbb{K})$ *y* $\varnothing$ *son conjuntos algebraicos.*

Demostración. Supongamos que $\{V_i = v(S_i), i \in I\}$ es una familia de conjuntos algebraicos entonces, dado que $\bigcap_{i\in I} V_i = v(\bigcup_{i\in I} S_i)$, se tiene que la intersección es un conjunto algebraico.

Sean ahora $V_1 = v(S_1)$ y $V_2 = v(S_2)$ dos conjuntos algebraicos, veremos que $V_1 \cup V_2$ es un conjunto algebraicos comprobando que $V_1 \cup V_2 = v(S_1S_2)$, donde S_1S_2 el conjunto de todos los productos de elementos de S_1 con elementos de S_2. Para ello probamos ambos contenidos:
"$\subset$": Sea $P \in V_1 \cup V_2$, entonces $P \in V_1$ ó $P \in V_2$ y, por lo tanto, P es un cero de todo polinomio de S_1 ó P es un cero de todo polinomio de S_2. En consecuencia, por cómo hemos definido S_1S_2, P será un cero de todo polinomio de S_1S_2, es decir, $P \in v(S_1S_2)$.
"$\supset$": Sea $P \in v(S_1S_2)$ y supongamos que $P \notin V_1$, entonces existe $f \in S_1$ tal que $f(P) \neq 0$. Para todo $g \in S_2$, $fg(P) = 0$, se tiene que $g(P) = 0$ y, por lo tanto, $P \in V_2$, luego $P \in V_1 \cup V_2$.

Finalmente, $\mathbb{A}^2(\mathbb{K})$ y $\varnothing$ son conjuntos algebraicos pues $\mathbb{A}^2(\mathbb{K}) = v(0)$ y $\varnothing = v(1)$. □

Nótese que la proposición previa nos indica que los conjuntos algebraicos son los cerrados de alguna topología en $\mathbb{A}^2(\mathbb{K})$. La topología que resulta de tomar como abiertos los complementarios de los conjuntos algebraicos se denomina topología de Zariski.

Observación 2.9. Para cada punto $(x,y) \in \mathbb{A}^2(\mathbb{K})$, $v(X-x, Y-y) = \{(x,y)\}$, luego, todo punto es un conjunto algebraico. Es también usual referirse a un conjunto algebraico mediante las ecuaciones que lo definen, es decir, en lugar de escribir $v(X-x, Y-y) = \{(x,y)\}$,

podemos decir que $\{(x, y)\}$ es el conjunto algebraico determinado por las ecuaciones $X = x$ e $Y = y$.

Notamos que un mismo conjunto algebraico puede definirse mediante distintos sistemas de ecuaciones, una forma de evitar que los resultados dependan de las ecuaciones particulares con las que definimos nuestro conjunto algebraico, es considerar todas las ecuaciones posibles. Para ello, veamos a continuación cómo relacionar un conjunto de puntos del plano afín con un ideal del anillo de polinomios.

Definición 2.10. Sea V un subconjunto de $\mathbb{A}^2(\mathbb{K})$. Definimos el ideal de anulación de V como

$$i(V) = \{f \in \mathbb{K}[X, Y] \mid f(x, y) = 0, \forall (x, y) \in V\},$$

es decir, como el conjunto de todos los polinomios de $\mathbb{K}[X, Y]$ que se anulan en los puntos de V.

Enunciamos a continuación algunas propiedades de los conjuntos algebraicos e ideales de anulación.

Proposición 2.11. *Se verifican las siguientes propiedades:*

(*i*) *Si* $S, T \subset \mathbb{K}[X, Y]$ *tales que* $S \subset T$, *entonces* $v(S) \supset v(T)$.

(*ii*) *Si* $V, W \subset \mathbb{A}^2(\mathbb{K})$ *tales que* $V \subset W$, *entonces* $i(V) \supset i(W)$.

(*iii*) $i(\emptyset) = \mathbb{K}[X, Y]$.

(*iv*) $i(\mathbb{A}^2(\mathbb{K})) = \{0\}$ *si, y solo si,* $\mathbb{K}$ *es infinito.*

(*v*) $i(V \cup W) = i(V) \cap i(W)$, $\forall V, W \subset \mathbb{A}^2(\mathbb{K})$.

(*vi*) *Si* $S \subset \mathbb{K}[X, Y]$, *entonces* $S \subset i(v(S))$.

(*vii*) *Si* $V \subset \mathbb{A}^2(\mathbb{K})$, *entonces* $V \subset v(i(V))$. *Si* V *es un conjunto algebraico, entonces se tiene la igualdad, es decir,* $V = v(i(V))$.

Observamos que todo conjunto algebraico afín $V \subset \mathbb{A}^2(\mathbb{K})$ puede ser asociado a un ideal de $\mathbb{K}[X, Y]$, $i(V)$, el ideal de todos los polinomios que se anulan en V. Entonces se tiene la siguiente aplicación

$$\begin{aligned} \{\text{conjuntos algebraicos afines}\} &\xrightarrow{i} \{\text{ideales de } \mathbb{K}[X, Y]\} \\ V &\longmapsto i(V). \end{aligned}$$

Inversamente, dado un ideal $I \subseteq \mathbb{K}[X,Y]$, podemos definir el conjunto algebraico $v(I)$. Por lo tanto, tenemos otra aplicación

$$\begin{aligned} \{\text{ideales de } \mathbb{K}[X,Y]\} &\xrightarrow{v} \{\text{conjuntos algebraicos afines}\} \\ I &\longmapsto v(I). \end{aligned}$$

Estas dos aplicaciones definen la correspondencia entre ideales y conjuntos algebraicos afines. Sin embargo, notamos que la primera aplicación no es inyectiva pues diferentes ideales pueden definir los mismos conjuntos algebraicos. Por ejemplo, $\langle X, Y\rangle$ y $\langle X^2, Y\rangle$ son diferentes pero ambos definen el mismo conjunto algebraico, el $\{(0,0)\}$. Además, si el cuerpo $\mathbb{K}$ no es algebraicamente cerrado surgen más problemas, pues diferentes polinomios pueden generar distintos ideales que definen el mismo conjunto algebraico. En particular, si no tienen raíces en el cuerpo, todos ellos definirán el conjunto algebraico vacío. En base a esto cabe preguntarse, ¿desaparece el problema de tener diferentes ideales representando el conjunto algebraico vacío si el cuerpo es algebraicamente cerrado? La respuesta es afirmativa, esta condición es suficiente para garantizar que el único ideal que representa el conjunto algebraico vacío es todo el anillo de polinomios $\mathbb{K}[X,Y]$. Esto es lo que se conoce como teorema débil de los ceros de Hilbert o Nullstellensatz.

Teorema 2.12 (versión débil del teorema de los ceros de Hilbert)**.** *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado y sea $I \subset \mathbb{K}[X,Y]$ un ideal tal que $v(I) = \emptyset$. Entonces, $I = \mathbb{K}[X,Y] = \langle 1\rangle$.*

Demostración. [LVO, Cap. 1, Teor. 5.1.] □

Observación 2.13. Nótese que, en general, si $I = \langle 1\rangle$, entonces $v(I) = \emptyset$, por lo que en el caso de cuerpos algebraicamente cerrados se tiene la equivalencia.

Podríamos pensar que la correspondencia entre ideales y conjuntos algebraicos es biyectiva si nos restringimos a cuerpos algebraicamente cerrados, pero esto no es así, pues el ejemplo anterior: $v(\langle X,Y\rangle) = v(\langle X^2,Y\rangle) = \{(0,0)\}$, funciona para todo cuerpo. A pesar de ello, el ejemplo nos ilustra la razón por la cuál diferentes ideales pueden definir el mismo conjunto algebraico: la potencia de un polinomio se anula en el mismo conjunto de puntos que el polinomio original.

Teorema 2.14 (versión fuerte del teorema de los ceros de Hilbert)**.** *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Si $f, f_1, \ldots, f_s \in \mathbb{K}[X,Y]$ son tales que $f \in v(f_1, \ldots, f_s)$, entonces existe $r \geq 0$ tal que $f^r \in \langle f_1, \ldots, f_s\rangle$ y recíprocamente.*

Demostración. [LVO, Cap. 1, Teor. 5.2.] □

Del teorema previo se deriva el siguiente Lema.

Lema 2.15. *Sea V un conjunto algebraico afín. Si $f^r \in i(V)$, entonces $f \in i(V)$.*

Esto es, un ideal consistente en todos los polinomios que se anulan en un conjunto algebraico tiene la propiedad de que si alguna potencia del polinomio pertenece al ideal, entonces el polinomio ha de pertenecer al ideal.

El lema inspira la siguiente definición.

Definición 2.16. Sea I un ideal de $\mathbb{K}[X,Y]$. Definimos el radical del ideal I como

$$\mathrm{Rad}(I) = \{f \in \mathbb{K}[X,Y] \mid f^n \in I \,\text{para algún}\, n \in \mathbb{N}\}.$$

Entonces $\mathrm{Rad}(I)$ es un ideal que contiene a I, en particular, $\mathrm{Rad}(I)$ es el menor ideal radical que contiene a I. Diremos que I es un ideal radical si $I = \mathrm{Rad}(I)$.

Observación 2.17. Todo ideal primo es radical.

Observación 2.18. El ideal de anulación $i(V)$ es un ideal radical para cualquier $V \subset \mathbb{A}^2(\mathbb{K})$.

Teorema 2.19 (versión geométrica del teorema de los ceros de Hilbert)**.** *Si $\mathbb{K}$ es un cuerpo algebraicamente cerrado, para cada ideal I de $\mathbb{K}[X,Y]$,*

$$i(v(I)) = \mathrm{Rad}(I).$$

Demostración. [M, Cap. 2, Teor. 2.16.] □

En particular, si el ideal I es radical tenemos que $i(v(I)) = I$, por lo tanto, la aplicación que asocia cada ideal I con $v(I)$ es biyectiva y su inversa es la aplicación que asocia cada conjunto algebraico V con $i(V)$. Ambas correspondencias invierten las inclusiones.

La consecuencia más importante del Nullstellensatz es que nos permite establecer un diccionario entre el álgebra y la geometría

$$\{\text{ideales radicales de } \mathbb{K}[X,Y]\} \longleftrightarrow \{\text{conjuntos algebraicos afines}\}$$

a través de las funciones v e i.

Un conjunto algebraico puede escribirse como unión de dos o más conjuntos algebraicos. Veamos a continuación lo que entenderemos por conjunto algebraico afín irreducible o variedad afín, una caracterización de la irreducibilidad en función del ideal correspondiente y la descomposición de los conjuntos algebraicos en variedades.

Definición 2.20. Sea V un conjunto algebraico afín. Diremos que V es irreducible si no se puede expresar como unión de conjuntos algebraicos afines estrictamente contenidos en V, es decir, si $V = V_1 \cup V_2$, entonces necesariamente $V = V_1$ ó $V = V_2$. Los conjuntos algebraicos irreducibles se denominan variedades. Un conjunto algebraico que no es irreducible se dice que es reducible.

Para comprobar si un conjunto algebraico es irreducible tenemos el siguiente resultado.

Proposición 2.21. *Sea V un conjunto algebraico afín no vacío. Entonces,*

$$V \text{ es irreducible} \iff i(V) \text{ es un ideal primo.}$$

Demostración. Veamos que se dan ambas implicaciones:
"$\Rightarrow$": Supongamos que V es irreducible y veamos que $i(V)$ es un ideal primo. Para ello tomemos $f \cdot g \in i(V)$. Tenemos que comprobar que $f \in i(V)$ o bien $g \in i(V)$. Definamos $V_1 = V \cap v(f)$ y $V_2 = V \cap v(g)$. Entonces, $V = V_1 \cup V_2$, pues $(V \cap v(f)) \cup (V \cap v(g)) = V \cap (v(f) \cup v(g)) = V$. Esto es así, pues $v(f) \cup v(g) = v(f \cdot g) \supset V$ ya que $f \cdot g \in i(V)$, por lo que $\langle f \cdot g \rangle \subset i(V)$, y como v invierte las inclusiones, $V \subset v(i(V)) \subset v(f \cdot g)$. Finalmente, como V es irreducible, $V = V_1$ ó $V = V_2$, luego $f \in i(V)$ ó $g \in i(V)$.

"$\Leftarrow$": Supongamos ahora que $i(V)$ es un ideal primo y veamos que V es irreducible. Sea $V = V_1 \cup V_2$ de forma que $V \neq V_1$, tenemos que ver que $V = V_2$. Para ello, veremos que $i(V) = i(V_2)$. Sabemos que $i(V) \subset i(V_2)$, probemos la otra inclusión: como $V_1 \subsetneq V$, $i(V) \subsetneq i(V_1)$. Sea entonces $f \in i(V_1)$ tal que $f \notin i(V)$ y sea $g \in i(V_2)$. Consideremos $f \cdot g$. Como f se anula en V_1 y g en V_2, el producto se anulará en la unión, esto es, $f \cdot g \in i(V)$, pero por hipótesis, $i(V)$ es un ideal primo, entonces $f \in i(V)$ ó $g \in i(V)$. Dado que $f \notin i(V)$, se tiene entonces que $g \in i(V)$. □

Como todo ideal primo es radical, utilizando la correspondencia entre los ideales radicales y los conjuntos algebraicos afines obtenemos el siguiente corolario.

Corolario 2.22. *Cuando $\mathbb{K}$ es un cuerpo algebraicamente cerrado, las aplicaciones i y v inducen una biyección entre los conjuntos algebraicos irreducibles y los ideales primos de $\mathbb{K}[X, Y]$.*

Las variedades más simples son los puntos, que además se corresponden con los ideales maximales, pues la correspondencia entre ideales radicales y conjuntos algebraicos invierte las inclusiones y los puntos no contienen variedades menores. Por lo tanto, todo punto $(x, y) \in \mathbb{A}^2(\mathbb{K})$ se corresponde con un ideal maximal incluso si $\mathbb{K}$ es finito. Veamos a continuación cómo son los ideales maximales en el caso en el que $\mathbb{K}$ es un cuerpo algebraicamente cerrado.

Teorema 2.23. *Si $\mathbb{K}$ es algebraicamente cerrado, entonces todo ideal maximal de $\mathbb{K}[X,Y]$ es de la forma $\langle X-x, Y-y\rangle$ para algún $(x,y) \in \mathbb{A}^2(\mathbb{K})$*

Demostración. Sea I un ideal maximal de $\mathbb{K}[X,Y]$. Como $I \neq \mathbb{K}[X,Y]$, se tiene que $v(I) \neq \varnothing$ por el teorema débil de los ceros de Hilbert. Por lo tanto, existe algún $(x,y) \in v(I)$. Pasando a ideales, se tiene:

$$i(v(I)) \subseteq i(\{(x,y)\}),$$

pero $i(v(I)) = \mathrm{Rad}(I)$, por la versión geométrica del teorema de los ceros de Hilbert 2.19. Ahora, dado que I es maximal por hipótesis, se tiene que $\mathrm{Rad}(I) = I$. Entonces:

$$I \subseteq i(\{(x,y)\}) = \langle X-x, Y-y\rangle \neq \mathbb{K}[X,Y].$$

Pero, dado que I es maximal, concluimos que $I = \langle X-x, Y-y\rangle$. □

Corolario 2.24. *Cuando $\mathbb{K}$ es un cuerpo algebraicamente cerrado, existe una biyección entre los puntos de $\mathbb{A}^2(\mathbb{K})$ y los ideales maximales de $\mathbb{K}[X,Y]$.*

Observación 2.25. Hemos ampliado nuestro diccionario entre el álgebra y la geometría: sobre un cuerpo algebraicamente cerrado, todo conjunto algebraico irreducible no vacío se corresponde con un ideal primo y recíprocamente. Todo punto se corresponde con un ideal maximal y recíprocamente.

Veamos ahora que todo conjunto algebraico afín se puede escribir de forma única como unión de variedades. Para ello, previamente introducimos un nuevo concepto en la definición de anillo noetheriano.

Definición 2.26. Un anillo conmutativo unitario A se dice que es un anillo noetheriano si todos sus ideales son finitamente generados. Esto es equivalente a la condición de cadena ascendente, esto es:

$$I_1 \subset I_2 \subset \cdots \subset I_n = I_{n+1} = \cdots .$$

Dado que $\mathbb{K}[X,Y]$ es un anillo noetheriano, $\mathbb{K}[X,Y]$ verifica la condición de cadena ascendente. Como las variedades correspondientes a los ideales de $\mathbb{K}[X,Y]$ invierten las inclusiones, verificarán la condición de cadena descendente en el plano afín, es decir, serán de la forma:

$$V_1 \supset V_2 \supset \cdots \supset V_n = V_{n+1} = \cdots .$$

Empleando esta propiedad, probaremos que todo conjunto algebraico afín se puede escribir como unión finita de variedades.

Teorema 2.27. *Todo conjunto algebraico afín V se escribe como unión de variedades afines, $V = V_1 \cup \cdots \cup V_n$.*

Demostración. Lo probaremos por reducción al absurdo. Supongamos que no fuese así, entonces V no sería irreducible, luego $V = V_1 \cup V_1'$, siendo $V_1, V_1' \neq V$. Además, al menos uno no puede ponerse como unión finita de variedades. Supongamos entonces que V_1 no es unión finita de variedades. Analógamente a lo que ocurría anteriormente con V, V_1 no sería irreducible, luego $V_1 = V_2 \cup V_2'$, siendo $V_2, V_2' \neq V_1$ y de forma que al menos uno no puede ponerse como unión finita de variedades. Supongamos entonces que V_2 no puede ser expresado como unión finita de variedades. Siguiendo este procedimiento, construimos una cadena estrictamente decreciente de variedades $V \supset V_1 \supset V_2 \supset \cdots$, que constituye una contradicción con la condición de cadena ascendente que verifica $\mathbb{K}[X, Y]$. Por lo tanto, V se puede escribir como unión finita de variedades. □

Definición 2.28. Sea V un conjunto algebraico con descomposición $V = V_1 \cup V_2 \cup \cdots \cup V_n$, donde V_i es una variedad $\forall i = 1, \ldots, n$. Esta descomposición se dice minimal si $V_i \not\subset V_j$, $\forall i \neq j$.

Teorema 2.29. *Sea $V \subset \mathbb{A}^2(\mathbb{K})$. V tiene una única descomposición minimal.*

Demostración. La existencia es inmediata pues en caso de tener $V = V_1 \cup \cdots \cup V_n$ con i y j tales que $V_i \subset V_j$, eliminaríamos V_i de la descomposición y ya tendríamos una descomposición minimal. Veamos pues la unicidad: supongamos dos descomposiciones minimales de V distintas $V = V_1 \cup \cdots \cup V_m$ y $V = V_1' \cup \cdots \cup V_l'$. Entonces, $\forall i$, $V_i = V_i \cap V = V_i \cap (V_1' \cup \cdots \cup V_l') = (V_i \cap V_1') \cup (V_i \cap V_2') \cup \cdots \cup (V_i \cap V_l')$. Como V_i es irreducible, existe j tal que $V_i \subset V_j'$. Razonando análogamente, existe k tal que $V_j' \subset V_k$. Por lo tanto $V_i \subset V_j' \subset V_k$, y, como es minimal, $V_i = V_j' = V_k$. Razonando de esta forma con todos los factores se obtiene la unicidad. □

Corolario 2.30. *Si $\mathbb{K}$ es algebraicamente cerrado, todo ideal es intersección finita de ideales primos. Si además es minimal, ésta es única.*

Demostración. Basta aplicar i a la descomposición en variedades. □

En nuestro caso particular de las curvas planas afines podemos razonar lo siguiente: sea $v(f) \subset \mathbb{A}^2(\mathbb{K})$ una curva plana afín y sea $f = f_1 \cdot \ldots \cdot f_n$ la descomposición de f en factores irreducibles. Entonces $v(f) = v(f_1) \cup \cdots \cup v(f_n)$ es la descomposición de $v(f)$ en variedades, ya que cada $v(f_i)$ es irreducible, pues $i(v(f_i)) = \langle f_i \rangle$ es primo. Además, $v(f_i) \not\subset v(f_j)$ para $i \neq j$, pues, de lo contrario, $\langle f_i \rangle \subset \langle f_j \rangle$ y, entonces, $f_i \mid f_j$, lo que implicaría que $f_i = f_j$. Concluimos así que una curva plana es irreducible si, y solo si, el polinomio que la define es irreducible o, a lo sumo, la potencia de un polinomio irreducible. En cualquier caso, una curva plana irreducible puede definirse siempre mediante un polinomio irreducible.

2.3. Anillo de coordenadas

En esta sección estudiaremos las funciones que conectan los conjuntos algebraicos, las funciones polinómicas.

Definición 2.31. Sean $V, W \subset \mathbb{A}^2(\mathbb{K})$ dos conjuntos algebraicos. Una aplicación $\phi\colon V \to W$ se dice aplicación polinómica si $\forall (x,y) \in V$, $\phi((x,y)) = (f_1((x,y)), f_2((x,y)))$, siendo $f_1, f_2 \in \mathbb{K}[X,Y]$. Diremos que ϕ es un isomorfismo si es una aplicación polinómica biyectiva con inversa polinómica.

Nuestro interés se centrará en el caso en el que $W = \mathbb{K}$, donde ϕ se convierte en una función polinómica escalar definida sobre V. La razón de considerar estas funciones es que una aplicación polinómica general $\phi : V \to \mathbb{A}^2(\mathbb{K})$ se construye con dos funciones polinómicas de V en $\mathbb{K}$ como componentes.

Definición 2.32. Sea $V \subset \mathbb{A}^2(\mathbb{K})$ un conjunto algebraico no vacío. Se define el anillo de coordenadas de V como

$$A(V) = \{f\colon V \to \mathbb{K} \mid f \text{ función polinómica}\}.$$

Se trata de un anillo conmutativo y unitario con la suma y el producto usual de funciones. Se tiene además que

$$A(V) \cong \tfrac{\mathbb{K}[X,Y]}{i(V)}$$

y se deduce que V es irreducible si, y solo si, $i(V)$ es primo o, equivalentemente, si $A(V)$ es un dominio.

Dada una aplicación polinómica $\phi\colon V \to W$, ésta induce un homomorfismo de anillos $\phi^*\colon A(W) \to A(V)$, que se define como $\phi^*(f) = f \circ \phi$ que es un homomorfismo de $\mathbb{K}$-álgebras. De forma inversa si $h\colon A(W) \to A(V)$ es un homomorfismo de anillos $\mathbb{K}$-lineal, existe unha aplicación polinómica $\phi\colon V \to W$ tal que $\phi^* = h$. De hecho, h será isomorfismo si, y solo si, lo es ϕ.

Definición 2.33. Sea V un conjunto algebraico afín. Se define la dimensión de V, que denotaremos por $\dim V$, como el supremo de todos los enteros, n, tales que existe una cadena $Z_0 \subsetneq Z_1 \subsetneq \ldots \subsetneq Z_n$ de variedades afines contenidas en V.

Definición 2.34. Sea A un anillo. Se define la dimensión de Krull de A como el supremo de las longitudes de las cadenas crecientes de ideales primos en A. Es decir, un anillo A tendrá dimensión de Krull n cuando admita alguna cadena de ideales primos $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ y cualquier otra cadena de ideales primos de A tenga longitud menor o igual que n.

Observación 2.35. Un cuerpo tiene dimensión de Krull 0 y cualquier dominio de ideales principales que no sea un cuerpo tiene dimensión de Krull 1, ya que sus ideales primos son maximales.

Proposición 2.36. *Sea V un conjunto algebraico afín. La dimensión de V es igual a la dimensión de Krull de su anillo de coordenadas $A(V)$.*

Demostración. Es consecuencia de que las cadenas estrictamente crecientes de variedades contenidas en V, $Z_0 \subsetneq Z_1 \subsetneq \ldots \subsetneq Z_n$, se corresponden de forma biunívoca con las cadenas estrictamente decrecientes de ideales primos en $\mathbb{K}[X,Y]$ que contienen a $i(V)$ mediante la aplicación i, y éstas a su vez, con las cadenas estrictamente decrecientes de ideales primos en $A(V)$. □

Definición 2.37. Sea A un anillo conmutativo y sea $\mathfrak{p}$ un ideal primo de A. Se define la altura de $\mathfrak{p}$, que denotaremos por $h(\mathfrak{p})$, como el supremo de las longitudes de las cadenas ascendentes de ideales primos contenidos en $\mathfrak{p}$.

Observación 2.38. Nótese que, entonces, la dimensión de Krull de A es el supremo de las alturas $h(\mathfrak{p})$ con $\mathfrak{p}$ ideal primo de A. Por convenio, si 0 es ideal primo de A, definiremos $h(0) := -\infty$. Si I es cualquier ideal, su altura será el ínfimo de las alturas de los ideales primos que contienen a I.

Teorema 2.39. *Sea $\mathbb{K}$ un cuerpo y A una $\mathbb{K}$-álgebra dominio finitamente generada de dimensión de Krull n. Entonces, el grado de trascendencia de $\mathbb{K}(A)$ sobre $\mathbb{K}$ es n y existen $t_1, \ldots, t_n \in A$, algebraicamente independientes sobre $\mathbb{K}$ tales que*

$$\mathbb{K}[t_1, \ldots, t_n] \subset A$$

de forma que A es un $\mathbb{K}[t_1, \ldots, t_n]$-módulo finitamente generado.

Demostración. [AK, Cap. 15, Lema. 15.1] □

2.4. Funciones racionales y anillos locales

Dado que para toda variedad no vacía $V \subset \mathbb{A}^2(\mathbb{K})$, $i(V)$ es un ideal primo, se tiene que $A(V)$ es un dominio, esto es, no tiene divisores de cero, luego, podemos considerar el cuerpo de fracciones que lo contiene.

Definición 2.40. Sea $V \subset \mathbb{A}^2(\mathbb{K})$ una variedad no vacía. Definimos el cuerpo de funciones racionales de V que denotaremos por $\mathbb{K}(V)$, como el cuerpo de fracciones de $A(V)$. Si $\alpha \in \mathbb{K}(V)$, diremos que α es una función racional en V.

Para que las funciones racionales estén bien definidas tenemos que evitar los ceros del denominador. Esto motiva la siguiente definición.

Definición 2.41. Sea α es una función racional en V y $(x, y) \in V$ diremos que α es regular o que está definida en (x, y) si existen $[\beta], [\gamma] \in A(V)$ tales que $\alpha = [\beta]/[\gamma]$, con $[\gamma](x, y) \neq 0$. En tal caso definimos $\alpha(x, y) = \frac{[\beta](x,y)}{[\gamma](x,y)}$. Si α está definida en (x, y), para todo $(x, y) \in U$ con $U \subset V$ un abierto, α define una función $\alpha : U \to \mathbb{K}$. El conjunto de las $\alpha \in \mathbb{K}(V)$ que son regulares en U se denota $\mathcal{O}(U)$. Obsérvese que $\mathcal{O}(V) = A(V)$.

Definición 2.42. Sea α es una función racional en V y $(x, y) \in V$ diremos que α es singular en el punto (x, y), o que (x, y) es una singularidad de α si α no es regular en (x, y).

Para estudiar el comportamiento de una curva en un punto será esencial introducir el concepto de anillo local, éste se definirá como el conjunto de las funciones racionales de la variedad que son regulares en dicho punto.

Definición 2.43. Diremos que un anillo es local si tiene un único ideal maximal.

Definición 2.44. Sea $V \subset \mathbb{A}^2(\mathbb{K})$ una variedad y sea $(x, y) \in V$. Definimos el anillo local de V definido en (x, y), $\mathscr{O}_{(x,y)}(V)$, como el conjunto de funciones racionales de V que están definidas en (x, y). Esto es:

$$\mathscr{O}_{(x,y)}(V) = \{\alpha = [\beta]/[\gamma] \in \mathbb{K}(V) \,|\, [\gamma](x, y) \neq 0\}$$

Observación 2.45. Notemos que $\mathscr{O}_{(x,y)}(V)$ es un subanillo de $\mathbb{K}(V)$ que contiene a $A(V)$.

Nótese que $\mathscr{O}_{(x,y)}(V)$ es en efecto un anillo local, su ideal maximal vendrá dado por la siguiente proposición.

Proposición 2.46. *El ideal maximal de $\mathscr{O}_{(x,y)}(V)$ viene dado por las funciones racionales que se anulan en (x, y):*

$$\mathfrak{m}_{(x,y)}(V) = \{\alpha = [\beta]/[\gamma] \in \mathscr{O}_{(x,y)}(V) \,|\, [\beta](x, y) = 0\}$$

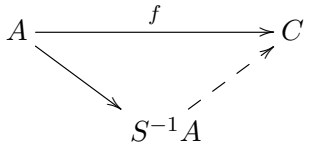
Sea $\mathrm{ev}_{(x,y)} : \mathscr{O}_{(x,y)}(V) \to \mathbb{K}$ el homomorfismo evaluación en el punto $(x, y) \in V$, es decir, el homomorfismo que relaciona cada función $\alpha \in \mathscr{O}_{(x,y)}(V)$ con $\alpha(x, y)$. Esta aplicación es sobreyectiva y su núcleo es el ideal maximal definido previamente, ya que $\alpha(x, y) = 0$ si, y solo si, $\alpha \in \mathfrak{m}_{(x,y)}(V)$, por lo tanto: $\frac{\mathscr{O}_{(x,y)}(V)}{\mathfrak{m}_{(x,y)}(V)} \cong \mathbb{K}$, luego, efectivamente, $\mathfrak{m}_{(x,y)}(V)$ es el ideal maximal del anillo local de V en (x, y).

Además, un elemento $\alpha \in \mathscr{O}_{(x,y)}(V)$ es una unidad si, y solo si, $\alpha(x,y) \neq 0$, o lo que es lo mismo, si $\alpha \notin \mathfrak{m}_{(x,y)}(V)$, luego $\mathfrak{m}_{(x,y)}(V)$ es el conjunto de los elementos que no son unidades de $\mathscr{O}_{(x,y)}(V)$.

Desde el punto de vista algebraico podemos dar otra descripción de $\mathscr{O}_{(x,y)}(V)$ basándonos en la teoría de localización en un dominio. En términos generales, sea S un subgrupo multiplicativo en un dominio A, esto es, $1 \in S$ y $s_1 \cdot s_2 \in S, \forall s_1, s_2 \in S$. Podemos considerar la relación de equivalencia dada por

$$(a,s) \sim (a',s') \iff s'a = a's,$$

y, a partir de ella, construir el el anillo de fracciones $S^{-1}A = \{\frac{a}{s} \,|\, a \in A, s \in S\}$, que denominamos localización de A en S. Nótese que podemos incluir A en $S^{-1}A$ mediante la aplicación canónica que lleva un elemento $a \in A$ en $a/1 \in S^{-1}A$. Tiene la propiedad de que si $f : A \longrightarrow B$ es un homomorfismo de anillos tal que $f(S) \subset U(B)$, donde $U(B)$ denota el conjunto de las unidades de B, es decir, convierte a los elementos de S en unidades, entonces existe una unica aplicación de $S^{-1}A$ en B de forma que el siguiente diagrama conmuta.



Esta aplicación asocia a cada elemento $a/s \in S^{-1}A$ un elemento $f(a) \cdot f(s)^{-1} \in B$, que está bien definida pues hemos supuesto que $f(S) \subset U(B)$.

Por lo tanto, teniendo lo anterior en cuenta, podemos dar una descripción de $\mathscr{O}_{(x,y)}(V)$ como sigue: sea V una variedad afín y $A(V) = \frac{\mathbb{K}[X,Y]}{i(V)}$ su correspondiente anillo de coordenadas. Hemos visto que todo punto $(x,y) \in V$ se corresponde a un ideal maximal de $\mathbb{K}[X,Y]$ que, a su vez, se corresponde a un ideal maximal de $A(V)$ que contiene a $i(V)$. Sea $\mathfrak{m}$ el maximal correspondiente a P en $A(V)$. Obsérvese que $\mathfrak{m} = \frac{i(\{(x,y)\})}{i(V)} \subset A(V) = \frac{\mathbb{K}[X,Y]}{i(V)}$. El subconjunto $S = A(V) \setminus \mathfrak{m}$ es un subconjunto multiplicativo de $A(V)$ por ser $\mathfrak{m}$ un ideal primo. Se tiene que $\mathcal{O}_{(x,y)}(V) = A(V)_{\mathfrak{m}}$, donde denotamos $A(V)_{\mathfrak{m}} = S^{-1}A(V)$. Como $S = A(V) \setminus \mathfrak{m} \subset A(V) \setminus \{0\}$, se sigue que $A(V)_{\mathfrak{m}} \subset \mathbb{K}(V)$, lo que concuerda con la definición geométrica previa.

A continuación, veremos cómo extender todas estas ideas al plano proyectivo. Comenzaremos definiendo los conjuntos algebraicos proyectivos de forma paralela a lo visto para el caso afín.

2.5. Conjuntos algebraicos proyectivos

En esta sección consideraremos al anillo de polinomios $\mathbb{K}[X, Y, Z]$ como un anillo graduado. Por ello, previamente explicamos brevemente el concepto de anillo graduado.

Definición 2.47. Un anillo graduado es un anillo S junto con la descomposición de S en suma directa de grupos abelianos S_d, $S = \bigoplus_{d\geq 0} S_d$, tales que para cada $d, e \geq 0$, $S_d \cdot S_e \subseteq S_{d+e}$. Un elemento S_d se dice elemento homogéneo de grado d. Por lo tanto, cualquier elemento de S se puede escribir de forma unica como suma (finita) de elementos homogéneos.

Definición 2.48. Un ideal $I \subseteq S$ es un ideal homogéneo si $I = \bigoplus_{d\geq 0}(I \cap S_d)$.

Observación 2.49. Un ideal es homogéneo si, y solo si, es generado a partir de elementos homogéneos. La suma, producto, intersección y radical de ideales homogéneos es homogéneo. Para probar que un ideal homogéneo es primo basta ver que para cualesquiera f, g elementos homogéneos tales que $f \cdot g \in I$ se tiene que $f \in I$ ó $g \in I$.

En nuestro caso, los elementos homogéneos serán polinomios homogéneos de $\mathbb{K}[X, Y, Z]$.

Definición 2.50. Un polinomio $F \in \mathbb{K}[X, Y, Z]$ se dice homogéneo de grado d si todos sus monomios son de grado d.

Observación 2.51. Un polinomio $F \in \mathbb{K}[X, Y, Z]$ homogéneo de grado d verifica $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z), \forall \lambda \in \mathbb{K}$.

Definición 2.52. Diremos que un ideal $I \subset \mathbb{K}[X, Y, Z]$ es homogéneo si está generado por polinomios homogéneos.

Definición 2.53. Sea $\mathbb{P}^2(\mathbb{K})$ el plano proyectivo y sea F un polinomio homogéneo en $\mathbb{K}[X, Y, Z]$. Un punto $(x : y : z) \in \mathbb{P}^2(\mathbb{K})$ se dice un cero de F si $F(x, y, z) = 0$.

Observación 2.54. Nótese que el valor de F en el punto $(x : y : z)$ no está definido pero la condición de que $(x : y : z)$ sea un cero de F sí.

Definición 2.55. Sea $S \subset \mathbb{K}[X, Y, Z]$ un conjunto de polinomios homogéneos. Se define el conjunto de ceros de S como

$$v_+(S) = \{(x : y : z) \in \mathbb{P}^2(\mathbb{K}) \,|\, F(x, y, z) = 0, \forall F \in S\},$$

esto es, el conjunto de puntos del plano proyectivo que son ceros comunes a un conjunto S de polinomios homogéneos en $\mathbb{K}[X, Y, Z]$.

Observación 2.56. Si $\langle S\rangle \subset \mathbb{K}[X,Y]$ es el ideal generado por S, entonces $v_+(S) = v_+(\langle S\rangle)$. De esta forma, hemos asociado un conjunto de polinomios homogéneos (o el ideal que generan) con un conjunto de puntos del plano proyectivo. Como $\mathbb{K}[X,Y,Z]$ es un anillo noetheriano para todo conjunto de polinomios homogéneos S, $v_+(S)$ siempre se puede expresar como el conjunto de ceros comunes a un conjunto finito de polinomios homogéneos.

Definición 2.57. Un conjunto $V \subset \mathbb{P}^2(\mathbb{K})$ es un conjunto algebraico proyectivo si $V = v_+(S)$, para algún conjunto de polinomios homogéneos $S \in \mathbb{K}[X,Y,Z]$.

Al igual que en el caso afín, es habitual determinar en la práctica los conjuntos algebraicos por las ecuaciones que los definen.

Observación 2.58. $\mathbb{P}^2(\mathbb{K})$ y $\varnothing$ son conjuntos algebraicos proyectivos. La intersección de conjuntos algebraicos proyectivos es un conjunto algebraico proyectivo y la unión finita de conjuntos algebraicos proyectivos es un conjunto algebraico proyectivo.

Del mismo modo, asociaciaremos a un conjunto de puntos del plano proyectivo un ideal del anillo de polinomios.

Definición 2.59. Sea V un subconjunto de $\mathbb{P}^2(\mathbb{K})$. Definimos el ideal de anulación de V como

$$i_+(V) = \{F \in \mathbb{K}[X,Y,Z] \text{ homogéneo } \mid F(x,y,z) = 0, \forall (x:y:z) \in V\},$$

es decir, como el conjunto de todos los polinomios de $\mathbb{K}[X,Y,Z]$ que se anulan en los puntos de V.

Observación 2.60. $i_+(V)$ es un ideal graduado de $\mathbb{K}[X,Y,Z]$.

Observación 2.61. Si $\mathbb{K}$ es infinito, entonces el ideal de anulación $i_+(V)$ será un ideal homogéneo. Esto no sucede en otro caso, por ejemplo en $\mathbb{F}_2 = \frac{\mathbb{Z}}{2\mathbb{Z}}$, el polinomio $f(X,Y) = X^2Y + XY$ no es homogéneo, pero verifica que $f(\lambda x, \lambda y) = f(x,y)$ para $(x,y) \in \mathbb{F}_2$, pues se anula en todos los puntos de $\mathbb{F}_2$.

Observamos que todo conjunto algebraico proyectivo $V \subset \mathbb{P}^2(\mathbb{K})$ puede ser asociado a un ideal graduado de $\mathbb{K}[X,Y,Z]$, el ideal $i_+(V)$. Entonces se tiene la siguiente aplicación

$$\begin{aligned} \{\text{conjuntos algebraicos proyectivos}\} &\xrightarrow{i_+} \{\text{ideales graduados de } \mathbb{K}[X,Y,Z]\} \\ V &\longmapsto i_+(V). \end{aligned}$$

Inversamente, dado un ideal graduado $I \subseteq \mathbb{K}[X,Y,Z]$, podemos definir el conjunto algebraico proyectivo $v_+(I)$. Por lo tanto, tenemos otra aplicación

$$\begin{aligned} \{\text{ideales graduados de } \mathbb{K}[X,Y,Z]\} &\xrightarrow{v_+} \{\text{conjuntos algebraicos proyectivos}\} \\ I &\longmapsto v_+(I). \end{aligned}$$

Definición 2.62. Sea V un conjunto algebraico proyectivo. Diremos que V es irreducible si no se puede expresar como unión de conjuntos algebraicos afines estrictamente contenidos en V. Es decir, si $V = V_1 \cup V_2$, entonces necesariamente $V = V_1$ ó $V = V_2$. Los conjuntos algebraicos proyectivos irreducibles se denominan variedades proyectivas.

Un conjunto algebraico proyectivo se descompone también de forma única en unión finita de variedades proyectivas no contenidas unas en otras. Asimismo, un conjunto algebraico proyectivo no vacío es irreducible si, y solo si, su ideal de anulación es primo.

Definición 2.63. Una curva plana proyectiva es un subconjunto de $\mathbb{P}^2(\mathbb{K})$ dado por

$$v_+(F) = \{(x : y : z) \in \mathbb{P}^2(\mathbb{K}) \mid F(x, y, z) = 0\},$$

donde $F \in \mathbb{K}[X, Y, Z]$ es un polinomio homogéneo no constante. El grado de F se dice grado de la curva. Si F es un polinomio irreducible, se dice que la curva $v_+(F)$ es irreducible.

Definición 2.64. Sea $V \subset \mathbb{P}^2(\mathbb{K})$ un conjunto algebraico proyectivo y $i_+(V)$ su correspondiente ideal en $\mathbb{K}[X, Y, Z]$. Definimos el anillo de coordenadas homogéneas de V como

$$S(V) = \tfrac{\mathbb{K}[X,Y,Z]}{i_+(V)}.$$

Observación 2.65. Al contrario de lo que ocurre con los conjuntos algebraicos afines, ningún elemento de $S(V)$, salvo las constantes, determinan funciones en V. En consecuencia, para construir funciones efectivas entre conjuntos algebraicos proyectivos tenemos que considerar las siguientes funciones: $\frac{[F]}{[G]}$, donde $[F]$ y $[G]$ son elementos homogéneos en $S(V)$ *del mismo grado* con $[G]$ no nulo.

Definición 2.66. Sea V una variedad proyectiva en $\mathbb{P}^2(\mathbb{K})$. El cuerpo de funciones de V, que denotaremos por $\mathbb{K}(V)$ será el conjunto de las funciones definidas con anterioridad. A los elementos de $\mathbb{K}(V)$ se les denomina *funciones racionales* de V.

Definición 2.67. Sea V una variedad proyectiva, $(x : y : z) \in V$ y $\frac{\phi}{\psi} \in \mathbb{K}(V)$, ϕ y ψ homogéneos del mismo grado. Diremos que $\frac{\phi}{\psi}$ está definida en $(x : y : z)$ si $\frac{\phi}{\psi} = \frac{[F]}{[G]}$ para $[F]$ y $[G]$ elementos homogéneos con $[G](x : y : z) = G(x, y, z) \neq 0$.

Definición 2.68. Sea $V \subset \mathbb{P}^2(\mathbb{K})$ una variedad proyectiva y sea $P = (x : y : z) \in V$. Definimos el anillo local de V definido en P, $\mathscr{O}_P(V)$, como el conjunto de funciones racionales de V que están definidas en $(x : y : z)$.Esto es:

$$\mathscr{O}_P(V) = \{\tfrac{\phi}{\psi} \in \mathbb{K}(V) \mid \tfrac{\phi}{\psi} = \tfrac{[F]}{[G]}, [G](x, y, z) \neq 0\}$$

Observación 2.69. Notemos que $\mathscr{O}_P(V)$ es un subanillo de $\mathbb{K}(V)$.

Proposición 2.70. *$\mathscr{O}_P(V)$ es un anillo local cuyo único ideal maximal viene dado por:*

$$\mathfrak{m}_P(V) = \{\tfrac{\phi}{\psi} \in \mathbb{K}(V) \mid \tfrac{\phi}{\psi} = \tfrac{[F]}{[G]}, [G](x : y : z) \neq 0, [F](x, y, z) = 0\}.$$

2.6. Transferencia afín-proyectiva de conjuntos algebraicos

Ahora estudiamos la relación entre los conjuntos algebraicos afines y los conjuntos algebraicos proyectivos viendo cómo los ideales en $\mathbb{K}[X,Y]$ están relacionados con los ideales graduados en $\mathbb{K}[X,Y,Z]$.

En el capítulo anterior vimos la inmersión del plano afín en el plano proyectivo mediante la función:

$$\begin{aligned}\varphi_2\colon \mathbb{A}^2(\mathbb{K}) &\longrightarrow \mathbb{P}^2(\mathbb{K})\\ (x,y) &\longmapsto (x:y:1).\end{aligned}$$

Ésta define una función polinómica de $\mathbb{A}^2(\mathbb{K})$ a $\mathbb{A}^3(\mathbb{K})$ donde este último es, por definición, el cono afín de $\mathbb{P}^2(\mathbb{K})$. Esto induce el siguiente homomorfismo de anillos:

$$\begin{aligned}\phi_*\colon \mathbb{K}[X,Y,Z] &\longrightarrow \mathbb{K}[X,Y]\\ F &\longmapsto F(X,Y,1),\end{aligned}$$

que nos relaciona los polinomios en $\mathbb{K}[X,Y]$ con los polinomios homogéneos en $\mathbb{K}[X,Y,Z]$.

Veamos a continuación cómo pasar de una curva en el plano afín a una en el plano proyectivo. La relación entre la geometría afín y la proyectiva se basará en las correspondencias entre polinomios homogéneos $F \in \mathbb{K}[X,Y,Z]$ y polinomios $f \in \mathbb{K}[X,Y]$.

Definición 2.71. Sea $\mathbb{K}$ un cuerpo, $F \in \mathbb{K}[X,Y,Z]$ un polinomio homogéneo de grado d. Llamaremos deshomogeneización de F a

$$F_* = \phi_*(F) = F(X,Y,1) \in \mathbb{K}[X,Y].$$

Al paso de F a F_* lo llamaremos deshomogeneizar el polinomio F.

Ejemplo 2.72. Consideremos el polinomio $F \in \mathbb{K}[X,Y,Z]$ dado por $F(X,Y,Z) = 6X^3 + 2XYZ + 3X^2Y + 3Y^2X$. Según la definición previa, la deshomogeneización de F será $F_*(X,Y) = F(X,Y,1) = 6X^3 + 2XY + 3X^2Y + 3XY^2 \in \mathbb{K}[X,Y]$.

Definición 2.73. Sea $\mathbb{K}$ un cuerpo, $f \in \mathbb{K}[X,Y]$ un polinomio de grado d.. Llamaremos homogeneización de f a

$$f^* = Z^d f(X/Z, Y/Z) \in \mathbb{K}[X,Y,Z].$$

Al paso de f a f^* lo llamaremos homogeneizar el polinomio f.

Observación 2.74. A diferencia de la deshomogeneización, la homogeneización no es un homomorfismo de anillos.

Ejemplo 2.75. Consideremos el polinomio $f \in \mathbb{K}[X,Y]$ dado por $f(X,Y) = 3X^7 + 2X^5Y + 4X^2 + 6Y^2 + XY + X + 8$, según la definición previa la homogeneización de f será $f^*(X,Y,Z) = Z^7 f(X/Z, Y/Z) = 3X^7 + 2X^5YZ + 4X^2Z^5 + 6Y^2Z^5 + XYZ^5 + XZ^6 + 8Z^7 \in \mathbb{K}[X,Y,Z]$.

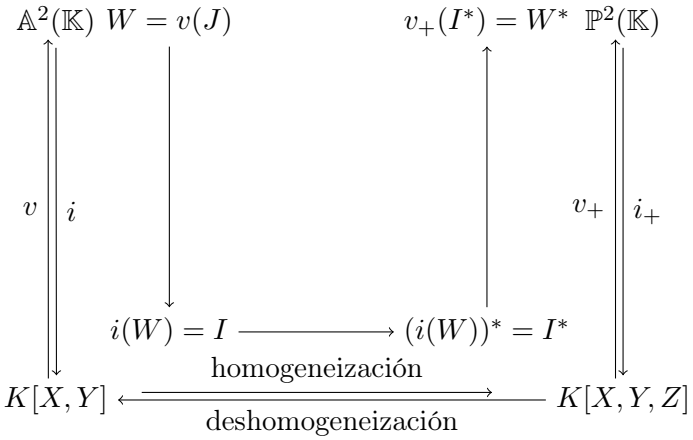
Es evidente que si se toma un polinomio, se homogeniza y posteriormente se deshomogeniza, se obtiene el polinomio de partida. Sin embargo, el recíproco no se verifica, basta considerar $F \in \mathbb{K}[X,Y,Z]$ dado por $F(X,Y,Z) = 6X^3Z + 2XYZ^2 + 3X^2YZ + 3Y^2XZ$. Obsérvese que $(F_*)^* = 6X^3 + 2XYZ + 3X^2Y + 3Y^2X$, es decir, F y $(F_*)^*$ se diferencian en un factor Z. En general, si $F \in \mathbb{K}[X,Y,Z]$ es homogéneo entonces $\exists r > 0$ tal que $F = (F_*)^* Z^r$ y $(F_*)^*$ no es un múltiplo de Z.

Definición 2.76. Sea I un ideal de $\mathbb{K}[X,Y]$. Definimos la homogeneización de I como el ideal en $\mathbb{K}[X,Y,Z]$ generado por $\{f^*/f \in I\}$, al cual denotaremos por I^*. Sea ahora I un ideal de $\mathbb{K}[X,Y,Z]$. Definimos la deshomogeneización de I como el ideal $\phi_*(I)$ de $\mathbb{K}[X,Y]$, al cual denotaremos por I_*.

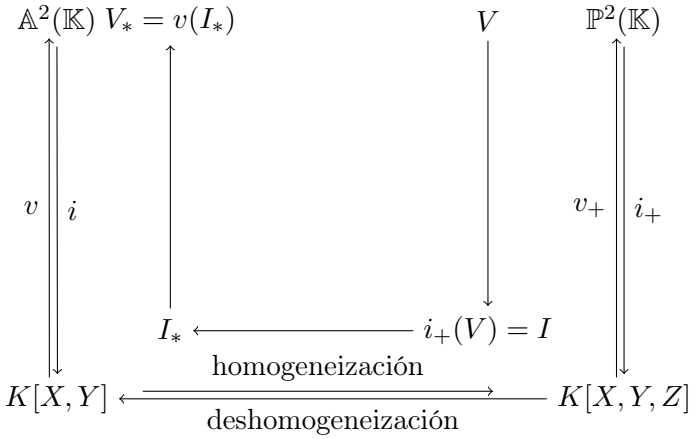
Observación 2.77. Si I es un ideal graduado en $\mathbb{K}[X,Y,Z]$, generalmente se tiene que $(I_*)^* \neq I$. Basta considerar el siguiente ejemplo: $I = \langle ZX, ZY \rangle \subset \mathbb{K}[X,Y,Z]$ pues, si consideramos la deshomogeneización de I, tenemos que $X, Y \in (I_*)^*$, sin embargo $X, Y \notin I$.

Definición 2.78. La curva proyectiva $v_+(F)$ donde $F \in \mathbb{K}[X,Y,Z]$ es la homogeneización de un polinomio $f \in \mathbb{K}[X,Y]$, se llama clausura proyectiva de la curva afín $v(f)$.

Trataremos ahora de asociar una variedad proyectiva a una afín. Para esto, podemos pensar en asociar a la variedad afín $v(f)$ la variedad proyectiva $v_+(f^*)$, donde f^* es el polinomio homogeneizado de f. Sin embargo, si lo que pretendemos es obtener la menor variedad proyectiva que contiene a $\varphi_2(v(f))$, esto no es válido en general. Dado I un ideal de $\mathbb{K}[X,Y]$, el procedimiento que seguiremos se ilustra en el siguiente diagrama:



siendo I^* el ideal homogeneizado de I. Vemos por lo tanto que tenemos que homogeneizar el ideal y no el polinomio. Diremos que W^* es la clausura proyectiva de W. El procediemento inverso también se puede hacer:



El siguiente teorema muestra algunas propiedades con respecto a la clausura proyectiva.

Teorema 2.79. *Se verifican las siguientes propiedades:*

(i) Si $V \subset \mathbb{A}^2(\mathbb{K})$ es una variedad, $\varphi_2(V) = V^* \cap \mathcal{U}_2$. Además, $(V^*)_* = V$.

(ii) Si $V \subset W \subset \mathbb{A}^2(\mathbb{K})$, entonces $V^* \subset W^* \subset \mathbb{P}^2(\mathbb{K})$. Reciprocamente, si $V \subset W \subset \mathbb{P}^2(\mathbb{K})$, entonces $V_* \subset W_* \subset \mathbb{A}^2(\mathbb{K})$.

(iii) Si V es irreducible en $\mathbb{A}^2(\mathbb{K})$, V^* es irreducible en $\mathbb{P}^2(\mathbb{K})$.

(iv) Si $V = \bigcup_{i=1}^r V_i$ es descomposición de V en irreducibles, $V^* = \bigcup_{i=1}^r V_i^*$ es descomposición de V^* en irreducibles.

(v) Si $V \subset \mathbb{A}^2(\mathbb{K})$, V^* es la menor variedad proyectiva que contiene a $\varphi_2(V)$.

Demostración. (i) Veamos primero que $\varphi_2(V) = V^* \cap \mathcal{U}_2$. Para ello, probaremos ambos contenidos:
"$\subset$": Sea $P = (x : y : z) \in \varphi_2(V)$, entonces $\varphi_2^{-1}(P) \in V$, siendo

$$\begin{aligned} \varphi_2^{-1} : \mathcal{U}_2 &\longrightarrow \mathbb{A}^2(\mathbb{K}) \\ (x : y : z) = (x/z : y/z : 1) &\longmapsto (x/z, y/z). \end{aligned}$$

Como $P \in \mathcal{U}_2$ por definición, tenemos que ver que $P \in V^*$. Veremos que P es un cero de todos los polinomios $F \in i(V)^*$. Sea F un generador de $i(V)^*$, entonces $F = G^*$ con $G \in i(V)$. Podemos escribir $P = (x/z : y/z : 1)$, y así:

$$F(P) = F(x/z, y/z, 1) = G(x/z, y/z) = G(\varphi_2^{-1}(P)) = 0.$$

Por lo tanto, $P \in v_+(i(V)^*) = V^*$.

"$\supset$": Sea $P \in V^* \cap \mathcal{U}_2$, entonces $P = (x/z : y/z : 1)$ y $F(P) = 0, \forall F \in i(V)^*$. Tenemos que ver que $P \in \varphi_2(P)$, o, equivalentemente, que $\varphi_2^{-1}(P) \in V$. Sea $G \in i(V)$. Tenemos que probar que $G(\varphi_2^{-1}(P)) = 0$. En efecto:

$$G(\varphi_2^{-1}(P)) = G(x/z, y/z) = G^*(x/z, y/z, 1) = 0,$$

pues $G^* \in i(V)^*$. Por lo tanto, $\varphi_2^{-1}(P) \in V$.

Veamos ahora que $(V^*)_* = V$, tenemos que comprobar ambos contenidos:
"$\subset$": Veamos si $\varphi_2(V_*) \subset V$ ya que, en ese caso $(V_*)^* = \overline{\varphi_2(V_*)} \subset V$. En efecto, $P \in \varphi_2(V_*), P \in \mathcal{U}_2 \implies P = (x : y : 1)$ y $\varphi_2^{-1}(P) \in V_* = v(i_+(V)_*)$. Si $F \in i_+(V), F(P) = F(x, y, 1) = F_*(x, y) = F_*(\varphi_2^{-1}(P)) = 0$ y por lo tanto, $P \in V$.

"$\supset$": Será suficiente con ver que $i(V_*)^* \subset i_+(V)$ pues $v_+(i(V_*)^*) \supset v_+(i_+(V)) = V$. Como $i(V_*) = i(v(i_+(V)_*)) = \mathrm{Rad}(i_+(V)_*)$, entonces $G \in i(V_*) \implies G \in \mathrm{Rad}(i_+(V)_*) \implies \exists n \in \mathbb{N}$ tal que $G^n \in i_+(V)_* \implies \exists F \in i_+(V)$ tal que $G^n = F_*$. Ahora dado que $(G^*)^n = (G^n)^* = (F_*)^*$, existe r tal que $Z^r(F_*)^* = Z^r(G^*)^n = F \in i_+(V)$ o bien $G^* \in i_+(V)$ ó $Z \in i_+(V)$ pero en este caso $H_\infty = v_+(Z) \supset v_+(i_+(V))$ lo cual es imposible. Por lo tanto, $i(V_*)^* \subset i_+(V)$.

(ii) Inmediata por la definición de clausura proyectiva de una variedad afín.

(iii) Sabemos que $i_+(V^*) := i(V)^*$. Basta con comprobar que si I es un ideal primo, entonces I^* también lo es. Sea $f \cdot g \in I^*$, entonces $f_* \cdot g_* \in I$. Como I es primo se tiene que $f_* \in I$ ó $g_* \in I$. Entonces, $(f_*)^* \in I^*$ ó $(g_*)^* \in I^*$. Dado que $f = Z^r(f_*)^*$ para algún $r > 0$ y $g = Z^s(g_*)^*$ para algún $s > 0$, concluimos que $f = Z^r(f_*)^* \in I^*$ ó $g = Z^s(g_*)^* \in I^*$.

(iv) Es consecuencia de los apartados (ii) y (iii).

(v) Es obvio que V^* contiene a $\varphi_2(V)$, pues $\varphi_2(V) = V^* \cap \mathcal{U}_2 \subset V^*$. Veamos que es la menor variedad proyectiva que lo contiene. Sea W una variedad proyectiva tal que $\varphi_2(V) \subset W$ y comprobemos que entonces, $V^* \subset W$. Supongamos $P = (x : y : z) \in V^*$, esto es, $F(P) = 0, \forall F \in i(V)^*$. Es suficiente con ver que $P \in \varphi_2(V)$, o lo que es lo mismo, que $\varphi_2^{-1}(P) \in V$. En efecto, si $G \in i(V)$ se tiene:

$$G(\varphi_2^{-1}(P)) = G((x/z, y/z)) = G^*((x/z, y/z, 1)) = 0,$$

pues $G^* \in i(V)^*$. Luego, $P \in \varphi_2(V) \subset W$. Por lo tanto, $V^* \subset W$.

□

Capítulo 3

Estudio local de curvas

3.1. Singularidades y espacios tangentes

Ahora veremos lo que entenderemos por punto singular y no singular de una curva y sus correspondientes rectas tangentes a la curva en el mismo.

Para ello, consideramos la curva plana $C = v(f)$ y sea (x, y) un punto de la curva. Empleando el método usual del cálculo diferencial obtendríamos que el espacio tangente a (x, y) está dado por la ecuación

$$\frac{\partial f}{\partial X}(x, y)(X - x) + \frac{\partial f}{\partial Y}(x, y)(Y - y) = 0.$$

Esta ecuación es la ecuación de una recta salvo que $\frac{\partial f}{\partial X}(x, y) = 0$ y $\frac{\partial f}{\partial Y}(x, y) = 0$, en cuyo caso, sería la ecuación de todo el plano. Obsérvese que la diferencial tiene sentido algebraicamente porque f es un polinomio, la derivada del monomio x^n se define como nx^{n-1} y se extiende a un polinomio general por linealidad.

Definición 3.1. Si $P = (x, y)$ es un punto de la curva plana afín $C = v(f)$, entonces el espacio tangente a C en P, que denotaremos por $T_P(C)$, es el conjunto algebraico definido por la ecuación

$$\frac{\partial f}{\partial X}(x, y)(X - x) + \frac{\partial f}{\partial Y}(x, y)(Y - y) = 0.$$

Diremos que $P = (x, y)$ es un punto no singular de la curva C si $\frac{\partial f}{\partial X}(x, y) \neq 0$ ó $\frac{\partial f}{\partial Y}(x, y) \neq 0$, y, en este caso, $T_P(C)$ sería una recta tangente a C en P. En otro caso, $T_P(C)$ tiene dimensión 2 y decimos que $P = (x, y)$ es un punto singular de la curva C. Una curva que solo tiene puntos no singulares se llama curva no singular.

Ejemplo 3.2. Consideremos la curva plana $C = v(f)$ dada por $f(X, Y) = Y^2 - X^2(X+1)$. El espacio tangente a C en $P = (x, y)$ viene dado por la ecuación

$$-x(3x+2)(X-x)+2y(Y-y)=0.$$

Dado que $-x(3x+2)=0 \iff x=0$ ó $x=-2/3$ y $2y=0 \iff y=0$ se tiene que $(0,0)$ es el único punto singular de C pues $(-2/3,0)$ no es un cero de f y, por lo tanto, no es un punto de la curva.

Proposición 3.3. *El conjunto de puntos no singulares de una curva plana forma un subconjunto abierto denso de la curva.*

Demostración. Sea $C=v(f)$ donde f es un polinomio no constante en $\mathbb{K}[X,Y]$ sin factores múltiples. Bastará con ver que el conjunto de puntos no singulares de C forma un subconjunto abierto denso de cada una de las componentes irreducibles de C, y, en consecuencia, supondremos que C, es irreducible. Luego, f también es irreducible. Tenemos, entonces, que demostrar que el conjunto de puntos singulares de C es un subconjunto cerrado propio. Como el conjunto de puntos singulares es el conjunto de ceros comunes de los polinomios f, $\frac{\partial f}{\partial X}$ y $\frac{\partial f}{\partial Y}$, es algebraico, y, por tanto, cerrado. Será propio siempre que $\frac{df}{dX}$ y $\frac{df}{dY}$ no sean iguales a cero en C. Claramente $\frac{\partial f}{\partial X}=0$ si, y solo si, f es un polinomio en Y, si la característica del cuerpo es 0 o si es un polinomio en X^p e Y, si la característica del cuerpo es p. Un argumento similar se da para $\frac{\partial f}{\partial Y}=0$. Por tanto, $\frac{\partial f}{\partial X}$ y $\frac{\partial f}{\partial Y}$ serán iguales a cero si f es constante, cuando la característica del cuerpo es 0 o un polinomio en X^p e Y^p, cuando la característica del cuerpo es p, pero esto se contradice con nuestras suposiciones dado que sería una potencia de p, y, por consiguiente, no sería irreducible, ya que la aplicación "elevar a la p-ésima potencia" es un homomorfismo sobre un cuerpo de característica p. Así, el conjunto de puntos singulares es un subconjunto cerrado propio. El conjunto de puntos no singulares de una curva plana se denomina lugar singular. □

3.2. Cono tangente a curvas planas

Un polinomio $f\in\mathbb{K}[X,Y]$ puede ser escrito de forma única como la suma finita

$$f=f_0+f_1+f_2+\cdots+f_m+\ldots,$$

donde cada f_m es un polinomio homogéneo de grado m. Al término f_1, que denotaremos por f_l, lo llamaremos forma lineal de f y al sumando homogéneo de f de menor grado, que denotaremos por f_p, lo llamaremos forma principal de f.

Si $P=(0,0)$ es un punto de la curva $C=v(f)$, entonces $f_0=0$. La expresión de f como suma finita sería

$$f = aX + bY + \text{términos de grado superior}$$

y la ecuación del espacio tangente,

$$aX + bY = 0.$$

Definición 3.4. Sea $C = v(f)$ una curva plana. Si $(0,0) \in C$, entonces se define el cono tangente geométrico a C en $(0,0)$ como el conjunto de ceros de f_p. El cono tangente a C en $(0,0)$ es el par $(V(f_p), f_p)$.

Ahora bien, interesa también estudiar una curva en un punto que no sea el origen. En ese caso, bastará con utilizar una transformación afín que lleve el punto a estudiar al origen.

Observación 3.5. Nótese que el cono tangente geométrico en un punto de una curva siempre tiene dimensión 1. Mientras que el espacio tangente nos indica si un punto es singular o no singular, el cono tangente nos da información sobre la naturaleza de la singularidad.

Ejemplo 3.6. Consideremos la curva plana $C = v(f)$ dada por $f(X,Y) = X^3 + X^2 - Y^2$. El espacio tangente a C en $P = (x,y)$ viene dado por la ecuación

$$x(3x+2)(X-x) - 2y(Y-y) = 0.$$

Dado que $x(3x+2) = 0 \iff x = 0$ ó $x = -2/3$ y $-2y = 0 \iff y = 0$ se tiene que $(0,0)$ es el único punto singular de C pues $(-2/3, 0)$ no es un cero de f y por lo tanto no es un punto de la curva. Por tanto, el espacio tangente a C en p es todo el plano. El cono tangente en el $(0,0)$ está definido por $Y^2 - X^2$. Es la unión de las rectas $Y = X$ e $Y = -X$.

3.3. Anillos de valoración discreta

A continuación introduciremos conceptos que nos llevarán a la definición de anillo de valoración discreta. Los anillos de valoración discreta serán anillos locales tales que su ideal maximal es principal. Veremos que los puntos no singulares de una curva tienen asociados anillos locales que son de valoración discreta, esto constituye la razón por la que los estudiaremos de forma más detallada.

Definición 3.7. Sea A un dominio de integridad y sea K su cuerpo de fracciones. Diremos que A es un anillo de valoración de K si , para cada $x \in K \setminus \{0\}$, $x \in A$ ó $x^{-1} \in A$.

Proposición 3.8. *Los anillos de valoración son anillos locales.*

Demostración. Sea A es un anillo de valoración y $\mathfrak{m}$ el conjunto de todos los elementos que no son unidades de A. Sabemos, entonces, que $x \in \mathfrak{m}$ si, y solo si, $x = 0$ ó $x^{-1} \notin A$. Sea $a \in A$ y $x \in \mathfrak{m}$, entonces, $ax \in \mathfrak{m}$ pues, de lo contrario, $(ax)^{-1} \in A$, y, en consecuencia, $x^{-1} = a(ax)^{-1} \in A$. Sean ahora $x, y \in \mathfrak{m} \setminus \{0\}$, entonces, $xy^{-1} \in A$ ó $x^{-1}y \in A$. Si $xy^{-1} \in A$, entonces, $x + y = (1 + xy^{-1})y \in A\mathfrak{m} \subseteq \mathfrak{m}$. Un razonamiento análogo nos lleva a que $x + y \in \mathfrak{m}$ en el caso en el que $x^{-1}y \in A$. Hemos probado por tanto, que $\mathfrak{m}$ es un ideal. Como cada ideal distinto de $\langle 1 \rangle$ de A está formado por elementos que no son unidades, necesariamente ha de estar contenido en $\mathfrak{m}$. Por lo tanto, $\mathfrak{m}$ es el único ideal maximal de A. Luego, A es un anillo local. □

Definición 3.9. Sea $\mathbb{K}$ un cuerpo. Una valoración discreta en $\mathbb{K}$ es una aplicación ν de $\mathbb{K} \setminus \{0\}$ sobre $\mathbb{Z}$ tal que

(i) $\nu(xy) = \nu(x) + \nu(y)$, $\forall x, y \in \mathbb{K}$, es decir, ν es un homomorfismo,

(ii) $\nu(x + y) \geq \text{mín}(\nu(x), \nu(y))$, $\forall x, y \in \mathbb{K}$.

El conjunto formado por el 0 y todos los $x \in K \setminus \{0\}$ tales que $\nu(x) \geq 0$ es un anillo, llamado anillo de valoración de ν. Es un anillo de valoración del cuerpo $\mathbb{K}$.

Observación 3.10. En ocasiones, es conveniente extender ν a todo $\mathbb{K}$ poniendo $\nu(0) = +\infty$.

Definición 3.11. Sea A un dominio de integridad y sea K su cuerpo de fracciones. Diremos que A es un anillo de valoración discreta si existe una valoración discreta ν en $\mathbb{K}$ tal que A es el anillo de valoración de ν.

Observación 3.12. Dado que los anillos de valoración son anillos locales, A es un anillo local y su ideal maximal es el conjunto de todos los $x \in K$ tales que $\nu(x) > 0$.

Otra forma de definir los anillos de valoración discreta puede venir dada de la siguiente manera.

Proposición 3.13. *Sea A un dominio que no es un cuerpo. Entonces equivalen:*

(i) A es noetheriano y local y su ideal maximal es principal.

(ii) Existe un elemento irreducible $t \in A$ tal que todo elemento no nulo $x \in A$ se escribe de forma única como $x = ut^n$, donde u es una unidad en A y n un entero no negativo.

Demostración. Probemos ambas implicaciones:
$(i) \implies (ii)$: Sea $\mathfrak{m} = \langle t \rangle$ el ideal maximal de A.

Veamos primero la unicidad. Para ello, sea $x \in A \setminus \{0\}$. Supongamos $x = ut^n = vt^m$, con n y m enteros no negativos tales que $n \geq m$ y $u, v \in U(A)$, donde $U(A)$ denota el

conjunto de las unidades de A. Entonces, $ut^{n-m} = v \in U(A)$. Por tanto, $n = m$ y $u = v$, luego, $x \in A \setminus \{0\}$ se escribe de forma única como $x = ut^n$, con $u \in U(A)$ y n un entero no negativo.

Veamos, ahora, la existencia. Sea $x \notin U(A)$, entonces $x = x_1 t$, $x_1 \in A$. Si $x_1 \in U(A)$ ya estaría probada. En caso contrario, $x_1 = x_2 t$, $x_2 \in A$. Si $x_2 \in U(A)$ ya estaría probada. En caso contrario, procederíamos de forma análoga. De esta forma, obtendríamos una cadena ascendente infinita de ideales, $\langle x_1 \rangle \subset \langle x_2 \rangle \subset \cdots$, de forma que $x_i = x_{i+1} t$. Como A es noetheriano, verifica la condición de cadena ascendente, y, por lo tanto, $\langle x_n \rangle = \langle x_{n+1} \rangle$, para algún n. Esto quiere decir que $x_{n+1} = v x_n$ con $v \in A$. Entonces se tiene que $x_{n+1} = vt x_{n+1}$, lo que implica que $vt = 1$, es decir, $t \in U(A)$, lo cual constituye una contradicción.
$(ii) \implies (i)$: Claramente, $\mathfrak{m} = \langle t \rangle$ es el conjunto de las no unidades, ya que todo elemento que no es unidad es un múltiplo de una potencia de t. Vemos que los únicos ideales propios de A son los $\langle t^n \rangle$, $n \geq 1$, luego, se tiene el resultado. □

Definición 3.14. Un anillo A satisfaciendo las condiciones de la proposición previa se dice anillo de valoración discreta. Un elemento t como el de (ii) se denomina parámetro de uniformización para A.

3.4. Anillo local en un punto

La relevancia de los anillos de valoración discreta en relación con el estudio de curvas viene dada por los siguientes resultados.

Proposición 3.15. *Sea P un punto de una curva plana C y sea $\mathfrak{m}$ el correspondiente ideal maximal en $A(C)$. Si P es no singular, entonces $dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2) = 1$. En otro caso, $dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2) = 2$.*

Demostración. Supogamos, en primer lugar, que $P = (0,0)$, entonces $\mathfrak{m} = \langle x, y \rangle$ en $A(C) = \mathbb{K}[X,Y]/\langle f(X,Y) \rangle = \mathbb{K}[x,y]$. Notemos que $\mathfrak{m}^2 = \langle x^2, xy, y^2 \rangle$ y que

$$\mathfrak{m}/\mathfrak{m}^2 = \langle X, Y \rangle / \langle \mathfrak{m}^2 + f(X,Y) \rangle = \langle X^2, XY, Y^2, f(X,Y) \rangle.$$

En $\mathfrak{m}/\mathfrak{m}^2$, cada elemento está representado por un polinomio lineal de la forma $cx + dy$, y la única relación es $f_l = 0$. Si $f_l \neq 0$, claramente, $\dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2) = 1$. En otro caso, $\dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2) = 2$. Teniendo en cuenta que $f_l = 0$ es la ecuación del espacio tangente, la proposición queda probada para $P = (0,0)$. Para un punto arbitrario, $P = (a,b)$, valdría el mismo argumento utilizando las variables $X' = X - a$ y $Y' = Y - b$, es decir, llevaríamos el punto al origen y procederíamos del mismo modo. □

Veamos a continuación qué significa que $\dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2) = 1$ para el anillo local en el punto P, $\mathcal{O}_P$. Sea $\mathfrak{n}$ el ideal maximal del anillo local en el punto, es decir, $\mathfrak{n} = \mathfrak{m}\mathcal{O}_P$. La aplicación $\mathfrak{m} \to \mathfrak{n}$ induce un isomorfismo $\mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{n}/\mathfrak{n}^2$, y así:

$$P \text{ no singular} \iff \dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2) = 1 \iff \dim_{\mathbb{K}}(\mathfrak{n}/\mathfrak{n}^2) = 1.$$

El lema de Nakayama [M, Cap. 1, Prop. 1.3] nos dice que la última condición es equivalente a que $\mathfrak{n}$ es un ideal principal. Dado que el $\mathcal{O}_P$ tiene dimensión de Krull 1, que su ideal maximal sea principal significa que es un anillo local regular de dimensión 1, esto es, $\mathcal{O}_P$ es un anillo local noetheriano que tiene la propiedad que el número mínimo de generadores de su ideal maximal es exactamente 1 (pues su dimensión de Krull es 1). Por lo tanto,

$$P \text{ no singular} \iff \mathcal{O}_P \text{ regular.}$$

Con el siguiente resultado veremos que el anillo local de un punto no singular de una curva es, además, un dominio de ideales principales.

Proposición 3.16. *Todo anillo local regular de dimensión uno es un dominio de ideales principales.*

Demostración. Sea A un anillo local regular de dimensión uno y sea $\mathfrak{m} = \langle t \rangle$ su ideal maximal. Por el teorema de la intersección de Krull [M, Cap. 1, Prop. 1.8], sabemos que $\cap_{r \geq 0} \mathfrak{m}^r = \langle 0 \rangle$. Sea $\mathfrak{a}$ un ideal propio no nulo de A. Como A es noetheriano, $\mathfrak{a}$ está finitamente generado, luego existe $r \in \mathbb{N}$ tal que $\mathfrak{a} \subset \mathfrak{m}^r$ pero $\mathfrak{a} \not\subset \mathfrak{m}^{r+1}$. Por lo tanto, existe $a = ct^r \in \mathfrak{a}$ tal que $a \notin \mathfrak{m}^{r+1}$. Esto implica que $c \notin \mathfrak{m}$, luego es una unidad. En consecuencia, $\langle t^r \rangle = \langle a \rangle \subset \mathfrak{a} \subset \langle t^r \rangle$, luego $\langle a \rangle = \mathfrak{a}$. Queda probado entonces que todos los ideales de A son principales.

Veamos ahora que es un dominio de integridad. Hemos supuesto que existe un ideal primo $\mathfrak{p}$ propio contenido en $\mathfrak{m}$. Entonces, $A/\mathfrak{p}$ es un dominio de integridad. Como $t \notin \mathfrak{p}$, no es nilpotente en $A/\mathfrak{p}$, y, en consecuencia tampoco es nilpotente en A. Sean $a, b \in A$. Existen $r, s \in \mathbb{N}$ tales que $a \in \mathfrak{m}^r \setminus \mathfrak{m}^{r+1}$ y $b \in \mathfrak{m}^s \setminus \mathfrak{m}^{s+1}$. Entonces, $a = ut^r$ y $b = vt^s$ con u, v unidades. Así, $ab = uvt^{r+s} \neq 0$. Por tanto, A es un dominio de integridad. □

Se sigue de la teoría elemental de los dominios de ideales principales que para un dominio de ideales principales, A, las siguientes condiciones son equivalentes:

(a) A tiene un único ideal primo no nulo.

(b) A tiene un único elemento primo salvo producto por unidades.

(c) A es local y no es un cuerpo.

Como sabemos que un anillo satisfaciendo éstas condiciones es un anillo de valoración discreta, podemos resumir lo anterior en el siguiente teorema.

Teorema 3.17. *Un punto P de una curva algebraica plana es no singular si, y solo si, $\mathcal{O}_P$ es regular, y por tanto, un anillo de valoración discreta.*

Tenemos, por tanto, lo siguiente: dada una curva, cada punto, P, tiene un anillo local, $\mathcal{O}_P$, que es el anillo de las funciones racionales definidas en el entorno del punto. Estas funciones racionales, serían el equivalente a las funciones meromorfas que se estudian en análisis de variable compleja. Además, si la curva no tiene singularidades este anillo es un anillo de valoración. Entonces se tiene que $x \in \mathcal{O}_P$ ó $x^{-1} \in \mathcal{O}_P$, esto es, $x = ut^n$ ó $x^{-1} = vt^m$. De esta manera, a cada elemento, fijado un punto, le podemos asociar un número entero. Este número es la valoración. Cuándo la valoración es positiva, representa el orden del cero y cuando la valoración es negativa, la función no está definida en el punto. Si pensamos en las funciones meromorfas esto quiere decir que el punto es un polo de la función racional. En este caso, la valoración representaría el orden del polo.

3.5. Valoraciones y puntos

El fin último de esta sección es probar el teorema principal de este trabajo que afirma que los puntos de una curva plana no singular se corresponden a los anillos de valoración discreta contenidos en el cuerpo de funciones racionales de la curva. Para ello, necesitaremos algunos resultados previos.

Proposición 3.18. *Sea $A(C)$ el anillo de coordenadas de una curva afín no singular C y sea $\mathbb{K}(C)$ el cuerpo de funciones racionales de C, que es el cuerpo de fracciones de $A(C)$. Los anillos de valoración no triviales de $\mathbb{K}(C)$ que contienen a $A(C)$ son precisamente los anillos locales $\mathcal{O}_P$ de $P \in C$. Son anillos de valoración discreta.*

Demostración. Por la proposición previa tenemos que los anillos locales en los puntos de nuestra curva C, $\mathcal{O}_P$, son anillos de valoración discreta. Supongamos ahora que $\mathfrak{o}$ es un anillo de valoración discreta de $\mathbb{K}(C)$ no trivial tal que $A(C) \subset \mathfrak{o}$ y sea $\mathfrak{m}$ su ideal maximal. Entonces $\mathfrak{m} \cap A(C)$ es un ideal primo en $A(C)$, veamos que $\mathfrak{m} \cap A(C) \neq 0$. En efecto, si $h \in \mathbb{K}(C)$, podemos escribir $h = f/g$ con $f, g \in A(C)$ y $g \neq 0$. Si $\mathfrak{m} \cap A(C) = 0$, entonces $g \notin \mathfrak{m}$, luego $g^{-1} \in \mathfrak{o}$, y, por tanto, $h \in \mathfrak{o}$. Así, $\mathbb{K}(C) = \mathfrak{o}$, lo cual contradice la no trivialidad de $\mathfrak{o}$. Por lo tanto, $\mathfrak{m} \cap A(C)$ es un ideal primo no nulo en $A(C)$. Dado que los ideales primos de $A(C)$ son el ideal nulo y los maximales, se corresponde con un punto, es decir, $v(\mathfrak{m} \cap A(C)) = P$, esto es, $\mathfrak{m} \cap A(C)$ es el ideal de los polinomios $f \in A(C)$ que se

anulan en P. Veamos que $\mathfrak{o} = \mathcal{O}_P$. Todo elemento de $\mathcal{O}_P$ se puede escribir como f/g donde $f \in A(C) \subseteq \mathfrak{o}$ y $g \in A(C) \setminus \mathfrak{m} \subseteq \mathfrak{o} \setminus \mathfrak{m}$. Luego g es una unidad en $\mathfrak{o}$ y, por tanto, $f/g \in \mathfrak{o}$. Luego, $\mathcal{O}_P \subseteq \mathfrak{o}$. Veamos el otro contenido. Sea $h \in \mathfrak{o}$ y supongamos que $h \notin \mathcal{O}_P$. Entonces, denotando por ν_P la valoración de $\mathcal{O}_P$ y sabiendo que $\mathcal{O}_P = \{\alpha \in \mathbb{K}(C) \,|\, \nu_P(\alpha) \geq 0\}$, se tiene que $\nu_P(h) < 0$. En consecuencia, $\nu_P(h^{-1}) > 0$, y, por tanto, $h^{-1} \in \mathcal{O}_P \subseteq \mathfrak{o}$. Además, $h^{-1} \in \mathfrak{m}_P$, pues el maximal de $\mathcal{O}_P$ es $\mathfrak{m}_P = \{\alpha \in \mathbb{K}(C) \,|\, \nu_P(\alpha) > 0\}$, y por tanto $h^{-1} \in \mathfrak{m}$, siendo $\mathfrak{m}$ el maximal de $\mathfrak{o}$. Pero h^{-1} es inverso de h, luego es una unidad en $\mathfrak{o}$ lo que constituye una contradicción con $h^{-1} \in \mathfrak{m}$, pues $U(\mathfrak{o}) = \mathfrak{o} \setminus \mathfrak{m}$. Por lo tanto, $\mathfrak{o} \subseteq \mathcal{O}_P$. Queda probado así que $\mathfrak{o} = \mathcal{O}_P$. □

Proposición 3.19. *Sea $A = \mathbb{K}[x]$ el anillo de polinomios que es el anillo de coordenadas de la variedad afín $\mathbb{A}^1(\mathbb{K})$, y sea $F = \mathbb{K}(x)$ su cuerpo de fracciones. Existe una biyección entre los puntos de $\mathbb{P}^1(\mathbb{K})$ y el conjunto de anillos de valoración de F que contienen a $\mathbb{K}$. Al punto $P \in \mathbb{A}^1(\mathbb{K})$ le corresponde su anillo local $\mathcal{O}_P$. Al punto del infinito, ∞, le corresponde el anillo de valoración dado por*

$$\mathcal{O}_\infty = \{x^{-r} f(x^{-1})/g(x^{-1}) \in F \,|\, f, g \text{ polinomios }, r \geq 0, f(0), g(0) \neq 0\}.$$

Demostración. $\mathcal{O}_\infty$ es un anillo de valoración discreta con la valoración

$$v_\infty(x^{-r} f(x^{-1})/g(x^{-1})) = r.$$

Tenemos que ver que todos los anillos de valoración $\mathfrak{o}$ de F que contienen a $\mathbb{K}$ son de esta forma. Distinguimos dos posibilidades:

- Si $x \in \mathfrak{o}$, entonces $A \subseteq \mathfrak{o}$ y entonces, por 3.18, $\mathfrak{o} = \mathcal{O}_P$, para algún $P \in \mathbb{A}^1(\mathbb{K})$.

- Si $x \notin \mathfrak{o}$, entonces x^{-1} está en el maximal $\mathfrak{m}$ de $\mathfrak{o}$. Consideramos el cambio en la base de trascendencia $x \mapsto x^{-1}$ de F. Es decir, estamos sustituyendo $\mathbb{K}[x] = A(\mathcal{U}_1)$ por $\mathbb{K}[x^{-1}] = A(\mathcal{U}_0)$, donde $\mathbb{P}^1(\mathbb{K}) = \mathcal{U}_0 \cup \mathcal{U}_1$ y $\mathcal{U}_0 = \{(x : y) \in \mathbb{P}^1(\mathbb{K}) \,|\, x \neq 0\}$, $\mathcal{U}_1 = \{(x : y) \in \mathbb{P}^1(\mathbb{K}) \,|\, y \neq 0\}$.

  Se tiene, entonces, que x está en el maximal $\sigma(\mathfrak{m})$ de $\sigma(\mathfrak{o})$, y, entonces, $A \subseteq \sigma(\mathfrak{o})$. Por 3.18, $\sigma(\mathfrak{o}) = \mathcal{O}_P$, para algún $P \in \mathbb{A}^1(\mathbb{K})$. Pero como x está en el ideal maximal de $\mathcal{O}_P$, se anula en P, y, por tanto, $P = O$, donde O denota el origen de $\mathcal{U}_0$ que se identifica con el punto del infinito de $\mathcal{U}_1$. En consecuencia, $\mathfrak{o} = \mathcal{O}_\infty$.

Hemos visto, por lo tanto, que $\mathfrak{o}$ es de la forma descrita en el enunciado de la proposición. □

Lema 3.20. *Sea $C \subset A$ una extensión de anillos de modo que A sea un C-módulo finito. Entonces, para cada maximal $\mathfrak{m}$ de C existe un número finito de maximales de A que se contraen a C.*

Demostración. Sea $K = \frac{C}{\mathfrak{m}}$ y sea $\mathfrak{m}^e$ el maximal extensión de $\mathfrak{m} \subset A$. Se tiene que $\frac{A}{\mathfrak{m}^e}$ es un K-espacio vectorial de dimensión finita y, por [AM, Cap. 8, Ej. 8.3], posee un número finito de maximales. Pero los maximales de $\frac{A}{\mathfrak{m}^e}$ se corresponden biyectivamente con los maximales de A que se contraen en $\mathfrak{m}$ en C, por tanto concluimos. □

Proposición 3.21. *Sea $\mathbb{K}(C)$ el cuerpo de funciones de una curva algebraica afín C definida sobre $\mathbb{K}$. Sea $f : \overline{C} \longrightarrow \mathbb{P}^1(\mathbb{K})$, donde $\overline{C}$ denota la clausura de C en $\mathbb{P}^2(\mathbb{K})$, un morfismo no constante y $\mathbb{K}(T) \subset \mathbb{K}(C)$ la extensión asociada de cuerpos. Sea $P \in \mathbb{P}^1(\mathbb{K})$ y $\mathcal{O}_P$ su anillo local. Existe un número finito de anillos de valoración discreta de $\mathbb{K}(C)$ que contienen a $\mathcal{O}_P$.*

Demostración. Sea A la clausura íntegra de $\mathcal{O}_P$ en $\mathbb{K}(C)$. A es finito sobre $\mathcal{O}_P$, es decir, entero y finito, de modo que A posee un número finito de maximales, por el Lema anterior. Ahora, la localización de A en uno de sus maximales es un anillo de valoración discreta de $\mathbb{K}(C)$ que contiene a A, luego éstos solo los hay en cantidad finita. □

Teorema 3.22. *Sea $C \subset \mathbb{P}^2(\mathbb{K})$ una curva plana no singular. Los puntos de C están en correspondencia biyectiva con los anillos de valoración discreta de $\mathbb{K}(C)$.*

Demostración. Utilizaremos la notación de 1.5, es decir, denotaremos por $\mathcal{U}_i$ a la imagen de φ_i. De esta forma, $\mathcal{U}_i \cong \mathbb{A}^2(\mathbb{K})$ y $\mathbb{P}^2(\mathbb{K}) = \mathcal{U}_2 \cup \mathcal{U}_1 \cup \mathcal{U}_0$. Haciendo un cambio de coordenadas, podemos suponer que $(1:0:0) \notin C$ pero $\mathbb{P}^2(\mathbb{K}) \setminus \{(1:0:0)\} = \mathcal{U}_2 \cap \mathcal{U}_1$, de modo que $C = (C \cap \mathcal{U}_1) \cup (C \cap \mathcal{U}_2)$, donde para $i = 1, 2$, $C_i = C \cup \mathcal{U}_i$ es una curva afín no singular.

Supongamos que $C = v_+(F(X, Y, Z))$. Entonces, $C_2 = v(F_*(X/Z, Y/Z, 1)) \subset \mathcal{U}_2$ y $C_1 = v(F_*(X/Y, Z/Y, 1)) \subset \mathcal{U}_1$. Sean $x := X/Z, y := Y/Z$ y $x' := X/Y, y' = Z/Y$. De esta forma, $A(C_2) = \frac{\mathbb{K}[x,y]}{\langle F_*(x,y) \rangle}$. Sabemos que $\mathbb{K}(C_2) = \mathbb{K}(C)$ es una extensión de grado de trascendencia 1 sobre $\mathbb{K}$, por tanto, existe $t \in \mathbb{K}(C)$ trascendente sobre $\mathbb{K}$ tal que $\mathbb{K}(t) \subset \mathbb{K}(C)$ es una extensión algebraica. Esta extensión es, además, separable por ser $\mathbb{K}$ algebraicamente cerrado, y, por tanto, $\mathbb{K}(t)$ perfecto.

Sea $\mathfrak{o}$ un anillo de valoración discreta de $\mathbb{K}(C)$. Se tienen dos casos: $t \in \mathfrak{o}$ ó $t \notin \mathfrak{o}$. Obsérvese que t lo podemos elegir en $A(C_2)$ y, así, la aplicación inyectiva canónica, $\mathbb{K}[t] \hookrightarrow A(C_2)$, se corresponde a una aplicación regular $\psi_2 : C_2 \longrightarrow \mathbb{A}^1(\mathbb{K}) = \mathcal{U}_2$.

- Si $t \in \mathfrak{o}$, $\mathfrak{o}' = \mathfrak{o} \cap \mathbb{K}[t]$ es un anillo de valoración discreta de $\mathbb{K}[t]$ que, por 3.19, se corresponde con un punto $P \in \mathcal{U}_2$. Por la proposición anterior, hay un número finito

de puntos de C_2 cuya imagen es P mediante ψ_2. Si $Q \in \psi_2^{-1}(P)$, $\mathcal{O}_Q$ es un anillo de valoración discreta de $\mathbb{K}(C)$ que contiene a $\mathfrak{o}'$, luego existirá un Q tal que $\mathcal{O}_Q = \mathfrak{o}$.

- Si $t \notin \mathfrak{o}$, entonces $t^{-1} \in \mathfrak{o}$. Dado que $C \setminus C_2 \subset \mathcal{U}_1$, se tiene que $t^{-1} \in A(C_1)$ y tenemos una aplicación regular, $\psi_1 : C_1 \longrightarrow \mathbb{A}^1(\mathbb{K})$ de modo que $\mathfrak{o}'' = \mathfrak{o} \cap \mathbb{K}[t^{-1}]$ es el anillo local del origen de $\mathbb{A}^1(\mathbb{K})$. Argumentando como antes, $\mathfrak{o} = \mathcal{O}_Q$ con $Q \in C_1$ tal que $\psi_1(Q)$ es el origen de $\mathbb{A}^1(\mathbb{K})$.

Con esto hemos visto que todos los anillos de valoración discreta de $\mathbb{K}(C)$ se corresponden a puntos de C. □

En conclusión, la idea clásica de Dedekind y Weber que constituye el significado de este teorema es la siguiente: un punto de una curva es un lugar donde las funciones racionales tienen un orden, ya sea de cero o de polo. Si definimos este orden (proporcionando la valoración), definimos el punto.

Bibliografía

[AK] Altman, A., Kleiman, S.: *Geometría algebraica*, Disponible en `http://web.mit.edu/18.705/www/13Ed.pdf`.

[AM] Atiyah, M. F., Macdonald, I. G.: *Introducción al álgebra conmutativa*, Reverté, 1989.

[F] Fulton, W.: *Algebraic curves: an introduction to algebraic geometry*, W.A. Benjamin, 1969.

[H] Hartshorne, R.: *Algebraic geometry*, Springer-Verlag, cop. 1993.

[I] Ivorra Castillo, C.: *Geometría algebraica*, Disponible en `www.uv.es/ivorra/Libros/Geomalg`.

[K] Kunz, E.: *Introduction to commutative algebra and algebraic geometry* , Birkhäuser, cop.1985.

[LVO] Li, H., Van Oystaeyen F.: *A Primer of algebraic geometry : constructive computational methods*, Marcel Dekker, cop. 2000.

[M] Milne, J.: *Algebraic geometry* (v6.01), Disponible en `www.jmilne.org/math/`, 2015.

[P] Perrin, D.: *Algebraic geometry : an introduction*, Springer, 2008.

[PM] Puente Muñoz, M. J. de la: *Curvas algebraicas y planas*, Universidad de Cádiz, 2007.

[R] Reid, M.: *Undergraduate algebraic geometry*, University Press, cop. 1994.

[RG] Richter-Gebert, J.: *Perspectives on projective geometry : a guided tour through real and complex geometry*, Springer, cop. 2011.

[S] Sancho de Salas, P.: *Álgebra conmutativa y geometría algebraica*, Disponible en `matematicas.unex.es/ sancho/GeometriaAlgebraica/libro0.pdf`.

[W] Walker, R.J.: *Algebraic curves*, University Press, 1950.