CAPÍTULO I

Primeros pasos en Geometría Algebraica

En este primer capítulo introduciremos los objetos con los que vamos a trabajar en los siguientes capítulos, que son las curvas algebraicas afines y proyectivas, y veremos algunas de sus propiedades básicas. Hemos decidido empezar por objetos un poco más generales, que son los conjuntos algebraicos afines y proyectivos, porque con poco esfuerzo más podemos obtener resultados suficientemente generales (como el Nullstellensatz (Teorema de los ceros) de Hilbert o la biyección entre conjuntos algebraicos afines y los ideales radicales del anillo de polinomios en n variables con coeficientes en un cuerpo algebraicamente cerrado K), que le darán al lector un poco de visión de futuro si decide después de leer este texto adentrarse en el mundo de la Geometría Algebraica Compleja. Para simplificar la presentación asumiremos a lo largo de este capítulo, y en general a lo largo del libro, que los cuerpos involucrados son de característica cero.

Este capítulo consta de 4 secciones: la primera introduce los conjuntos algebraicos afines y proyectivos, la segunda tiene por objetivo principal estudiar las principales operaciones que se pueden hacer con ideales de anillos de polinomios y con conjuntos algebraicos (destaca la descomposición de conjuntos algebraicos como unión de sus componentes irreducibles), la tercera aborda la demostración del Nullstellensatz de Hilbert e incluye el lema de preparación de Noether y finalmente la cuarta recoge los preliminares acerca de conjuntos algebraicos del plano, que serán de gran utilidad en el resto de los capítulos. En esta última sección nos centramos en algunos resultados relevantes para curvas algebraicas planas, como el lema de Study, que nos permite demostrar que las curvas algebraicas planas tienen una ecuación minimal que genera su ideal ceros.

Esta capítulo se ha escrito asumiendo que el lector tiene suficientes conocimientos de Geometría proyectiva (al menos un curso básico) y Teoría de Anillos. En concreto, suponemos que maneja con soltura los anillos de polino-

mios tanto en una como en varias variables. Además, el lector debería conocer lo que es un cuerpo algebraicamente cerrado y tener un manejo adecuado de la resultante de dos polinomios, así como conocer sus principales propiedades. Como posibles referencias donde encontrar estos contenidos, sugerimos al lector [FG2, FG4].

1. Conjuntos algebraicos afines y proyectivos

El objetivo de esta sección es introducir los conjuntos algebraicos afines y proyectivos. Ello requerirá presentar algunos conceptos y resultados relevantes al alumno como el Teorema de la base de Hilbert, la identidad de Euler, etc.

1.a. Conjuntos algebraicos afines. Uno de nuestros objetivos es estudiar las propiedades de los conjuntos que se pueden describir como "ceros de polinomios", es decir, aquellos que admiten una descripción como el conjunto de puntos de un cierto espacio afín que satisfacen una cantidad finita de ecuaciones polinómicas. Con el fin de evitar "interferencias algebraicas" de los coeficientes de los polinomios involucrados en los resultados, asumiremos que dichos coeficientes pertenecen a un cuerpo K. Veremos un poco más adelante (en el Nullstellensatz de Hilbert) que para obtener resultados plenamente satisfactorios es ventajoso trabajar sobre un cuerpo algebraicamente cerrado. Como para la presentación inicial esto no es necesario, de momento enunciaremos los resultados para un cuerpo arbitrario K (de característica cero).

Dados un cuerpo K y un subconjunto S del anillo de polinomios $K[\mathtt{x}] := K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ se define *el conjunto de ceros* de S en K^n como

$$\mathcal{Z}(S) := \{x \in K^n : \ f(x) = 0 \text{ para todo } f \in S\}.$$

Sea $\mathfrak{a}$ el ideal de $K[\mathtt{x}]$ generado por S. Entonces es inmediato comprobar que $\mathcal{Z}(S) = \mathcal{Z}(\mathfrak{a})$ con lo que en muchas ocasiones nos centramos en los conjuntos de ceros de ideales .

Los subconjuntos de K^n de la forma $\mathcal{Z}(\mathfrak{a})$, donde $\mathfrak{a}$ es un ideal de $K[\mathtt{x}]$, se denominan *subconjuntos algebraicos de* K^n. Si $\mathfrak{a} := \{f_1, \ldots, f_m\}K[\mathtt{x}]$ es un ideal finitamente generado se tiene

$$\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(f_1, \ldots, f_m) := \{x \in K^n : \ f_1(x) = 0, \ldots, f_m(x) = 0\}.$$

En el caso en el que $m = 1$ y $\mathfrak{a} := fK[\mathtt{x}]$ tenemos

$$\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(f) := \{x \in K^n : \ f(x) = 0\} := \{f = 0\}.$$

Dado un subconjunto $M \subset K^n$ se define *el ideal de* M como

$$\mathcal{J}(M) := \{f \in K[\mathtt{x}] : \ f(x) = 0 \text{ para todo } x \in M\}.$$

Nótese que $\mathcal{J}(M)$ es un ideal de $K[\mathtt{x}]$ que tiene la siguiente propiedad adicional: *si* $f^k \in \mathcal{J}(M)$ *entonces* $f(x)^k = 0$ *para cada* $x \in M$ *y, como* K *es un dominio,* $f(x) = 0$*, o sea,* $f \in \mathcal{J}(M)$. A los ideales de $K[\mathtt{x}]$ que cumplen la propiedad anterior se les conoce como *ideales radicales* y serán estudiados en detalle más adelante.

Ejemplos I.1.1 (i) Los subespacios afines de K^n son conjuntos algebraicos afines, incluido el propio K^n.

(ii) Las cuádricas afines de K^n son conjuntos algebraicos afines, incluida la cuádrica vacía. En particular, el conjunto $X := \{\mathtt{y} - \mathtt{x}^2 = 0\}$ es algebraico afín.

(iii) El conjunto $X := \{(\cos(t), \sin(t)) : \ t \in \mathbb{R}\} = \{\mathtt{x}^2 + \mathtt{y}^2 = 1\} \subset \mathbb{R}^2$ es un conjunto algebraico afín.

(iv) El lector puede comprobar que el conjunto $X := \{\mathtt{xy} - 1 = 0, \mathtt{x} > 0\} \subset \mathbb{R}^2$ no es un conjunto algebraico afín.

(v) Si $p := (p_1, \ldots, p_n) \in K^n$, entonces $\{p\} = \mathcal{Z}(\mathtt{x}_1 - p_1, \ldots, \mathtt{x}_n - p_n)$ es un conjunto algebraico afín.

(vi) Si $K = \mathbb{R}$ y $p := (p_1, \ldots, p_n) \in \mathbb{R}^n$, entonces $\{p\} = \mathcal{Z}(\sum_{i=1}^n (\mathtt{x}_i - p_i)^2)$.

1.a.1. Teorema de la base de Hilbert. Desde el punto de vista computacional calcular el lugar de ceros de un ideal supone manejar a priori una familia infinita de polinomios. El teorema de la base de Hilbert simplifica este supuesto reduciendo el problema a manejar una cantidad finita de polinomios. Presentamos una prueba del Teorema de la base de Hilbert que sigue la original debida a Hilbert y que no involucra teoría de módulos. Recordamos que un anillo A es *noetheriano* si todos sus ideales son finitamente generados.

Teorema I.1.2 (Teorema de la base de Hilbert) *Sea* A *un anillo noetheriano. Entonces, el anillo de polinomios* $A[\mathtt{t}]$ *también es noetheriano.*

Demostración. Supongamos, por reducción al absurdo, que existe un ideal $\mathfrak{a}$ de $A[\mathtt{t}]$ que no es finitamente generado. Elegimos un polinomio $f_1 \in \mathfrak{a} \setminus \{0\}$

tal que $\deg(f_1) = \min\{\deg(f) : f \in \mathfrak{a} \setminus \{0\}\}$ y construimos inductivamente polinomios

$$f_{k+1} \in \mathfrak{a} \setminus (f_1, \ldots, f_k)A[\mathtt{t}]$$

cuyo grado es mínimo entre los grados de los polinomios de $\mathfrak{a} \setminus (f_1, \ldots, f_k)A[\mathtt{t}]$.

Sean $d_k := \deg(f_k)$ y a_k el coeficiente director de f_k. Nótese que $d_k \leq d_{k+1}$ si $k \geq 1$. Denotamos $\mathfrak{b}_k := (a_1, \ldots, a_k)A$ y observamos que $\mathfrak{b}_k \subset \mathfrak{b}_{k+1}$ para cada $k \geq 1$. Como A es noetheriano, existe un entero $n \geq 1$ tal que $\mathfrak{b}_n = \mathfrak{b}_{n+\ell}$ para cada $\ell \geq 1$. En particular, existen $b_1, \ldots, b_n \in A$ tales que $a_{n+1} = \sum_{k=1}^{n} a_k b_k$. Entonces, el polinomio

$$g := f_{n+1} - \sum_{k=1}^{n} b_k f_k \mathtt{t}^{d_{n+1}-d_k} \in \mathfrak{a} \setminus (f_1, \ldots, f_n)A[\mathtt{t}] \quad \& \ \deg(g) < \deg(f_{n+1}),$$

lo que contradice la elección de f_{n+1}. Por tanto, todo ideal de $A[\mathtt{t}]$ es finitamente generado, es decir, $A[\mathtt{t}]$ es noetheriano. □

El recíproco del Teorema I.1.2 es cierto, es decir, si el anillo de polinomios $A[\mathtt{t}]$ es noetheriano, entonces A lo es. En efecto, el cociente $A[\mathtt{t}]/(\mathtt{t})$, que es isomorfo al anillo A, es noetheriano.

Corolario I.1.3 *Si K es un cuerpo, el anillo de polinomios $K[\mathtt{x}]$ es noetheriano.*

Demostración. Vamos a proceder por inducción. El único ideal del cuerpo K es el cero, que es finitamente generado. Supongamos el resultado cierto para $A := K[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$. Por el Teorema I.1.2 el anillo $A[\mathtt{x}_n] = K[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}][\mathtt{x}_n] = K[\mathtt{x}]$ es noetheriano. □

De este modo, dado un ideal $\mathfrak{a}$ de $K[\mathtt{x}]$ podemos elegir polinomios $f_1, \ldots, f_m$ tales que $\mathfrak{a} = \{f_1, \ldots, f_m\}K[\mathtt{x}]$ y por tanto $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(f_1, \ldots, f_m)$.

1.b. Polinomios e ideales homogéneos. Como sabemos de la asignatura de Geometría Lineal el espacio proyectivo $K\mathbb{P}^n$ nos proporciona no solo una herramienta adicional para estudiar problemas relativos al espacio afín K^n (mediante la completación proyectiva), sino que permite desarrollar una teoría más general y abordar objetos que tienen un comportamiento más redondo. Algunos ejemplos son: la fórmula de Grassmann, el hecho de que dos rectas del plano proyectivo (no coincidentes) se cortan en un punto, etc. Desde el punto de vista topológico el espacio proyectivo es compacto y por tanto sus subconjuntos cerrados son también compactos (con lo que no les faltan puntos que

pudieran estar en el "infinito"). Recordamos que los puntos del proyectivo $K\mathbb{P}^n$ son clases de equivalencia módulo proporcionalidad (con respecto al cuerpo K). Por ello, para describir subconjuntos de $K\mathbb{P}^n$ necesitamos usar "condiciones" que respeten dicha proporcionalidad. Por ello, para describir conjuntos algebraicos en este ámbito no podemos utilizar polinomios arbitrarios, sino polinomios que respeten esa proporcionalidad (con respecto al cuerpo K). Dichos polinomios son los *polinomios homogéneos*.

1.b.1. Polinomios homogéneos. Un polinomio $f \in K[\mathtt{x}]$ es *homogéneo de grado* d si todos sus monomios no nulos tienen (el mismo) grado d. Denotamos $K_d[\mathtt{x}]$ el conjunto de los polinomios homogéneos de grado d. Con el fin de dotar al conjunto anterior de estructura de K-espacio vectorial consideramos que el polinomio nulo es homogéneo de grado d para cada d. Si f es homogéneo de grado d se tiene la igualdad:

$$f(\mathtt{tx}) = \mathtt{t}^d f(\mathtt{x}) \tag{I.1.1}$$

como polinomios en $K[\mathtt{x}, \mathtt{t}]$. En efecto, cada monomio $g \in K[\mathtt{x}]$ de grado d se escribe como $g := a\mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_n^{\nu_n}$ donde $\nu_1 + \cdots + \nu_n = d$, luego

$$g(\mathtt{tx}) = a(\mathtt{tx}_1)^{\nu_1} \cdots (\mathtt{tx}_n)^{\nu_n} = \mathtt{t}^{\nu_1+\cdots+\nu_n} a\mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_n^{\nu_n} = \mathtt{t}^d g(\mathtt{x}).$$

En consecuencia, si $f = g_1 + \cdots + g_r$ es suma de monomios de grado d se tiene

$$f(\mathtt{tx}) = \sum_{i=1}^{r} g_i(\mathtt{tx}) = \mathtt{t}^d \sum_{i=1}^{r} g_i(\mathtt{x}) = \mathtt{t}^d f(\mathtt{x}).$$

De hecho, el lector puede comprobar que la propiedad anterior caracteriza a los polinomios homogéneos. De esta forma, los polinomios homogéneos son aquellos que preservan la proporcionalidad y nos van a permitir construir los conjuntos algebraicos proyectivos más adelante.

Lema I.1.4 *El producto de dos polinomios homogéneos de grados d y e es un polinomio homogéneo de grado $d + e$.*

Demostración. Si f y g son polinomios homogéneos de grados d y e, respectivamente, su producto $h := fg$ cumple

$$h(\mathtt{tx}) = f(\mathtt{tx})g(\mathtt{tx}) = \mathtt{t}^d f(\mathtt{x})\mathtt{t}^e g(\mathtt{x}) = \mathtt{t}^{d+e} h(\mathtt{x}),$$

con lo que h es homogéneo de grado $d + e$. □

Los polinomios homogéneos podemos describirlos en términos de sus derivadas parciales.

Lema I.1.5 (Identidad de Euler) *Sea $F \in K[\mathtt{x}]$ un polinomio homogénero de grado d. Entonces $d \cdot F = \sum_{i=1}^{n} \frac{\partial F}{\partial \mathtt{x}_i}\mathtt{x}_i$.*

Demostración. Como las derivadas parciales respetan la linealidad, es suficiente con probar el resultado para los monomios de grado d. Así que supondremos que $F := \mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_n^{\nu_n}$ con $\nu_1 + \cdots + \nu_n = d$. Se cumple que

$$\sum_{i=1}^{n} \frac{\partial F}{\partial \mathtt{x}_i}\mathtt{x}_i = \sum_{i=1}^{n} \nu_i \mathtt{x}_1^{\nu_1} \cdots \mathtt{x}_{i-1}^{\nu_{i-1}} \mathtt{x}_i^{\nu_i - 1} \mathtt{x}_{i+1}^{\nu_{i+1}} \cdots \mathtt{x}_n^{\nu_n} \mathtt{x}_i = \sum_{i=1}^{n} \nu_i F = d \cdot F,$$

de donde se concluye el enunciado. □

Definición I.1.6 (Componentes homogéneas) Cada polinomio $f \in K[\mathtt{x}]$ se escribe, de modo único, como suma $f = \sum_{k=0}^{d} f_k$ donde $d = \deg(f)$ y cada f_k es un polinomio homogéneo de grado k. Los polinomios f_k están determinados por f y reciben el nombre de *componentes homogéneas de f*.

La componente f_k es la suma de los monomios de f de grado k. Por tanto,

$$f(\mathtt{tx}) = \sum_{k=0}^{d} f_k(\mathtt{tx}) = \sum_{k=0}^{d} \mathtt{t}^k f_k(\mathtt{x}_1, \ldots, \mathtt{x}_n),$$

que no coincide con $\mathtt{t}^d f(\mathtt{x}_1, \ldots, \mathtt{x}_n) = \mathtt{t}^d \sum_{k=0}^{d} f_k(\mathtt{x}_1, \ldots, \mathtt{x}_n)$ salvo si $f_k = 0$ para $0 \leq k < d$. Así, la igualdad (I.1.1) caracteriza los polinomios homogéneos de grado d.

El concepto de homogeneidad se puede "extender" a los ideales del modo siguiente.

Definición I.1.7 Un ideal $\mathfrak{a} \subset K[\mathtt{x}]$ es *homogéneo* si para cada $f \in \mathfrak{a}$ se cumple que las componentes homogéneas de f pertencen a $\mathfrak{a}$.

Veamos cómo caracterizar los ideales homogéneos, que serán fundamentales para describir los conjuntos algebraicos complejos, en términos de sus generadores.

Lema I.1.8 (Ideales homogéneos) *Un ideal $\mathfrak{a} \subset K[\mathtt{x}]$ es homogéneo si y solo admite un sistema finito de generadores formado por polinomios homogéneos.*

Demostración. Si $\mathfrak{a} \in K[\mathtt{x}]$ es un ideal homogéneo y $f_1, \ldots, f_r \in \mathfrak{a}$ es un sistema finito de generadores de $\mathfrak{a}$, entonces las componentes homogéneas de los polinomios f_i también pertenecen a $\mathfrak{a}$ y constituyen un sistema finito de generadores de $\mathfrak{a}$ formado por polinomios homogéneos.

Supongamos ahora que el ideal $\mathfrak{a}$ esta generado por polinomios homogéneos $g_1, \ldots, g_s$. Si $f \in \mathfrak{a}$, existen polinomios $h_1, \ldots, h_s$ tales que $f = \sum_{i=1}^{s} h_i g_i$. Sean $h_{ij} \in K[\mathtt{x}]$ las componentes homogéneas de h_i. Como consecuencia del Lema I.1.4 los productos $h_{ij}g_i$ son polinomios homogéneos de grados $\deg(h_{ij}) + \deg(g_i)$. Por tanto, las componentes homogéneas de f son sumas (finitas) de productos $h_{ij}g_i$. De este modo, las componentes homogéneas de f pertenen a $\mathfrak{a} = \{g_1, \ldots, g_s\}K[\mathtt{x}]$ y concluimos que $\mathfrak{a}$ es un ideal homogéneo. □

Observación I.1.9 La condición de finitud del sistema de generadores de un ideal homogéneo se puede relajar en el siguiente sentido: *Un ideal $\mathfrak{a} \subset K[\mathtt{x}]$ es homogéneo si y solo admite un sistema de generadores formado por polinomios homogéneos.*

Basta recordar que si tenemos un sistema de generadores S de un ideal $\mathfrak{a}$ de $K[\mathtt{x}]$ (que es un anillo noetheriano), siempre podemos elegir un subconjunto finito $T \subset S$ que genera $\mathfrak{a}$. Para ello, elegimos un sistema de generadores finito S' de $\mathfrak{a}$ y escribimos cada elemento de S' en términos del sistema de generadores de S. Como S' es finito y la representación de cada elemento de S' en términos de los elementos de S solo involucra una cantidad finita de elementos de S, concluimos que existe un subconjunto finito $T \subset S$ que genera $\mathfrak{a}$.

1.c. Conjuntos algebraicos proyectivos. Recordamos que si K es un cuerpo infinito los polinomios $f \in K[\mathtt{x}]$ definen de forma unívoca (vía el homomorfismo evaluación en cada punto de K^n) una función polinómica $\widehat{f} : K^n \to K$. Cuando trabajamos con el espacio proyectivo $K\mathbb{P}^n$ esto ya no es cierto, ni siquiera si trabajamos con polinomios homogéneos $f \in K[\mathtt{x}^*] := K[\mathtt{x}_0, \ldots, \mathtt{x}_n]$ de grado d ya que, como hemos visto $f(\mathtt{t}\mathtt{x}^*) = \mathtt{t}^d f(\mathtt{x}^*)$. De esta forma, los polinomios homogéneos, que describen un conjunto algebraico proyectivo, se utilizaran como indicadores de pertenencia o no al conjunto correspondiente (es decir, el polinomio se anula o no se anula en el punto), pero debemos de olvidar en este caso el concepto de función asociada. Denotamos $x^* := (x_0, \ldots, x_n) \in K^{n+1}$ y los puntos del espacio proyectivo $K\mathbb{P}^n$ como $[x^*] := [x_0 : \cdots : x_n]$.

Definición I.1.10 Un subconjunto $X \subset K\mathbb{P}^n$ es un *conjunto algebraico proyectivo* si existen polinomios homogéneos $F_1, \ldots, F_r \in K[\mathtt{x}]$ tales que

$$X = \mathcal{Z}(F_1, \ldots, F_r) := \{[x^*] \in K\mathbb{P}^n : \ F_1(x^*) = 0, \ldots, F_r(x^*) = 0\}.$$

Dado un ideal homogéneo $\mathfrak{a} \subset K[\mathtt{x}^*]$ definimos

$$\mathcal{Z}(\mathfrak{a}) := \mathcal{Z}(F_1, \ldots, F_r)$$

donde $F_1, \ldots, F_r$ es un sistema de generadores homogéneos de $\mathfrak{a}$ (véase el Lema I.1.8). El lector puede comprobar que la definición anterior no depende del sistema de generadores homogéneos de $\mathfrak{a}$ elegidos.

Definición I.1.11 (Ideal de ceros) Sea $X \subset K\mathbb{P}^n$ un conjunto algebraico proyectivo. El *ideal de ceros* de X es el ideal (homogéneo) $\mathcal{J}(X)$ generado por el conjunto de polinomios homogéneos de $K[\mathtt{x}^*]$ que se anulan sobre todos los puntos de X.

Ejemplos I.1.12 (i) Los subespacios proyectivos y las cuádricas proyectivas de K^n son conjuntos algebraicos proyectivos. En particular, $\varnothing = \mathcal{Z}(\mathtt{x}_0, \ldots, \mathtt{x}_n)$, los puntos de $K\mathbb{P}^n$ y el propio $K\mathbb{P}^n$ son conjuntos algebraicos proyectivos.

(ii) Las uniones finitas de hiperplanos y de cuádricas proyectivas de K^n son conjuntos algebraicos proyectivos.

1.c.1. Completación proyectiva. La completación proyectiva de espacios y subespacios afines es una herramienta muy habitual para abordar problemas de Geometría Afín. Para construirla lo que se hace es "homogeneizar" las ecuaciones (implícitas) afines de los subespacios afines. Veamos cómo se hace en el caso de los conjuntos algebraicos afines. En primer lugar, consideramos la inmersión

$$\varphi : K^n \hookrightarrow K\mathbb{P}^n,\ x := (x_1, \ldots, x_n) \mapsto [1 : x] := [1 : x_1 : \cdots : x_n].$$

Sea $X \subset K^n$ un conjunto algebraico afín y sean $f_1, \ldots, f_r \in \mathcal{J}(X)$ generadores de $\mathcal{J}(X)$. Observamos que

$$X \equiv \varphi(X) = \{[1 : x] \in K\mathbb{P}^n :\ f_1(x) = 0, \ldots, f_r(x) = 0\}$$

y buscamos el menor conjunto algebraico proyectivo de $K\mathbb{P}^n$ que contiene a $\varphi(X)$. Para ello, en primer lugar tenemos que "homogeneizar" polinomios.

Definición I.1.13 (Homogeneizado) Sea $f \in K[\mathtt{x}]$ un polinomio de grado $d \geq 0$. El polinomio $\widehat{f}(\mathtt{x}^*) := \mathtt{x}_0^d f(\frac{\mathtt{x}}{\mathtt{x}_0})$ es el *homogeneizado* de f y cumple que $\widehat{f}(1, \mathtt{x}) = f$.

Lema I.1.14 (Completación proyectiva) *Sea $X \subset K^n$ un conjunto algebraico afín y $S := \{\widehat{f} : \ f \in \mathcal{J}(X)\}$. Sea $\mathfrak{a}$ el ideal de $K[\mathtt{x}^*]$ generado por S. Entonces el menor conjunto algebraico proyectivo de $K\mathbb{P}^n$ que contiene a X es $\widehat{X} := \mathcal{Z}(\mathfrak{a})$.*

Demostración. En primer lugar observamos, dado que $\widehat{f}(1, \mathtt{x}) = f$ para $i = 1, \ldots, r$, que se cumple $X \subset \widehat{X}$. Sea $Y \subset K\mathbb{P}^n$ un conjunto proyectivo que contiene a X y sean $G_1, \ldots, G_s \in K[\mathtt{x}^*]$ tales que $Y = \mathcal{Z}(G_1, \ldots, G_s)$. Definimos $g_j := G_j(1, \mathtt{x})$ y observamos que $g_j(x) = 0$ para todo $x \in X$, con lo que $g_j \in \mathcal{J}(X)$. De esta forma, $G_j = \mathtt{x}_0^{m_j} \widehat{g_j} \in S$ para algún $m_j \geq 0$, con lo que $G_j \in \mathfrak{a}$ y por tanto $\widehat{X} = \mathcal{Z}(\mathfrak{a}) \subset \mathcal{Z}(G_1, \ldots, G_s) = Y$. Concluimos que $\widehat{X}$ es el menor conjunto algebraico proyectivo de $K\mathbb{P}^n$ que contiene a X. □

Al conjunto algebraico proyectivo $\widehat{X}$ lo llamaremos *completación proyectiva de X*.

Observación I.1.15 Contrariamente a lo que uno podría esperar, para construir el completado proyectivo de un conjunto algebraico afín $X \subset K^n$ no es suficiente con elegir un sistema finito de generadores de $\mathcal{J}(X)$, homogeneizarlos y calcular su lugar de ceros. Veamos un par de ejemplos:

(i) Sean $n \geq 2$ y $X := \mathcal{Z}(1+\mathtt{x}_1, 1-\mathtt{x}_1)$. Obsérvese que $X = \varnothing$, $\mathcal{J}(X) = K[\mathtt{x}]$ y $\mathcal{J}(X) = \{1 + \mathtt{x}_1, 1 - \mathtt{x}_1\}K[\mathtt{x}]$. Sin embargo, $Y = \mathcal{Z}(\mathtt{x}_0 + \mathtt{x}_1, \mathtt{x}_0 - \mathtt{x}_1) = \mathcal{Z}(\mathtt{x}_0, \mathtt{x}_1) \neq \varnothing$, pues $n \geq 2$. Concluimos que Y no es la completación proyectiva de X.

(ii) Sean $X := \mathcal{Z}(\mathtt{x}_1+\mathtt{x}_2^2, \mathtt{x}_1-\mathtt{x}_2^2, \mathtt{x}_2)$. Obsérvese que $X = \{(0,0)\}$, $\mathcal{J}(X) = (\mathtt{x}_1, \mathtt{x}_2)K[\mathtt{x}_1, \mathtt{x}_2]$ y $\mathcal{J}(X) = \{\mathtt{x}_1 + \mathtt{x}_2^2, \mathtt{x}_1 - \mathtt{x}_2^2, \mathtt{x}_2\}K[\mathtt{x}_1, \mathtt{x}_2]$. Sin embargo,

$$Y = \mathcal{Z}(\mathtt{x}_0\mathtt{x}_1 + \mathtt{x}_2^2, \mathtt{x}_0\mathtt{x}_1 - \mathtt{x}_2^2, \mathtt{x}_2) = \mathcal{Z}(\mathtt{x}_0\mathtt{x}_1, \mathtt{x}_2) = \{[0:1:0], [1:0:0]\},$$

que no es la completación proyectiva de X.

2. Operaciones con ideales y conjuntos algebraicos

Con el fin de poder hacer una presentación más discursiva presentamos a continuación algunas propiedades de los ideales radicales, de los ideales de ceros y de los conjuntos algebraicos afines.

2.a. Ideales radicales. Recordamos que un ideal $\mathfrak{a} \subset K[\mathtt{x}]$ es *radical* si para todo $f \in K[\mathtt{x}]$ tal que $f^k \in \mathfrak{a}$ para algún $k \geq 1$, se cumple que $f \in \mathfrak{a}$. Si $\mathfrak{a} \subset K[\mathtt{x}]$ es un ideal se define el *radical* $\sqrt{\mathfrak{a}}$ *de* $\mathfrak{a}$ como el menor ideal radical de $K[\mathtt{x}]$ que contiene a $\mathfrak{a}$.

Lema I.2.1 (Radical de un ideal) *Si* $\mathfrak{a} \subset K[\mathtt{x}]$ *es un ideal, entonces*

$$\sqrt{\mathfrak{a}} = \{f \in K[\mathtt{x}] : \ f^k \in \mathfrak{a} \text{ para algún } k \geq 1\}.$$

Demostración. Es claro que $\mathfrak{b} := \{f \in K[\mathtt{x}] : \ f^k \in \mathfrak{a} \text{ para algún } k \geq 1\}$ contiene a $\mathfrak{a}$ y está contenido en todo ideal radical de $K[\mathtt{x}]$ que contiene a $\mathfrak{a}$. Veamos que $\mathfrak{b}$ es un ideal radical de $K[\mathtt{x}]$. Sean $f, g \in \mathfrak{b}$ y sea $k \geq 1$ tal que $f^k, g^k \in \mathfrak{a}$. Entonces

$$(f+g)^{2k} = \sum_{\ell=0} \binom{2k}{\ell} f^{2k} g^{2k-\ell} \in \mathfrak{a},$$

con lo que $f + g \in \mathfrak{b}$. Sea ahora $a \in K[\mathtt{x}]$ y observamos que $(af)^k = a^k f^k \in \mathfrak{a}$, con lo que $af \in \mathfrak{b}$. De este modo, $\mathfrak{b}$ es un ideal de $K[\mathtt{x}]$. Si $h \in K[\mathtt{x}]$ cumple que $h^m \in \mathfrak{b}$, entonces existe $s \geq 1$ tal que $h^{ms} \in \mathfrak{a}$, con lo que $h \in \mathfrak{b}$ y $\mathfrak{b}$ es por tanto un ideal radical. □

El lector puede probar las siguientes propiedades de los ideales radicales y del operador radical $\sqrt{\cdot}$.

Lema I.2.2 (Propiedades) *Sean* $\mathfrak{a}, \mathfrak{b}, \mathfrak{p} \subset K[\mathtt{x}]$ *ideales. Se cumple que:*

(i) $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$.

(ii) *Si* $\mathfrak{a} \subset \mathfrak{b}$, *entonces* $\sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{b}}$.

(iii) $\sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}}$.

(iv) $\sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}} = \sqrt{\mathfrak{a} + \mathfrak{b}}$.

(v) *Si* $\mathfrak{p} \subset K[\mathtt{x}]$ *es un ideal primo, entonces* $\mathfrak{p}$ *es un ideal radical de* $K[\mathtt{x}]$.

Además, los ideales radicales de ideales homogéneos son de nuevo ideales homogéneos.

Lema I.2.3 (Radical de un ideal homogéneo) *Si* $\mathfrak{a} \subset K[\mathtt{x}^*]$ *es un ideal homogéneo, entonces* $\sqrt{\mathfrak{a}}$ *es también un ideal homogéneo de* $K[\mathtt{x}^*]$.

Demostración. Sea $f \in \sqrt{\mathfrak{a}}$ y lo escribimos como $f := f_d + \cdots + f_p$ donde los polinomios f_k son las componentes homogéneas de f para $k = d, \ldots, p$. Existe $m \geq 1$ tal que

$$f^m = f_d^m + \cdots + f_p^m \in \mathfrak{a}.$$

Como $\mathfrak{a}$ es un ideal homogéneo, $f_d^m, f_p^m \in \mathfrak{a}$, luego $f_d, f_p \in \sqrt{\mathfrak{a}}$. Por tanto, $f - f_d - f_p \in \sqrt{\mathfrak{a}}$ y procediendo por inducción sobre el número de componentes homogéneas de f, concluimos que las componentes homogéneas de f están en $\sqrt{\mathfrak{a}}$. Luego $\sqrt{\mathfrak{a}}$ es un ideal homogéneo de $K[\mathtt{x}^*]$. □

2.b. Ideales y conjuntos de ceros. Veamos a continuación en el caso afín algunas propiedades de los ideales de ceros y de los conjuntos algebraicos. Las siguientes propiedades son elementales y pueden ser comprobadas por el lector.

Lema I.2.4 *Sean $S, T \subset K^n$ y $\mathfrak{a}, \mathfrak{b} \subset K[\mathtt{x}]$ ideales. Se cumple que:*

(i) *Si $S \subset T$, entonces $\mathcal{J}(T) \subset \mathcal{J}(S)$.*

(ii) *Si $\mathfrak{a} \subset \mathfrak{b}$, entonces $\mathcal{Z}(\mathfrak{b}) \subset \mathcal{Z}(\mathfrak{a})$.*

(iii) *$\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\sqrt{\mathfrak{a}})$.*

(iv) *$\mathcal{J}(S \cup T) = \mathcal{J}(S) \cap \mathcal{J}(T)$. De hecho, el mismo resultado es cierto para uniones finitas de subconjuntos de K^n.*

(v) *Si $\mathfrak{a} \cdot \mathfrak{b}$ es el ideal de $K[\mathtt{x}]$ generado por los productos ab con $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$, entonces $\mathcal{Z}(\mathfrak{a} \cdot \mathfrak{b}) = \mathcal{Z}(\mathfrak{a} \cap \mathfrak{b}) = \mathcal{Z}(\mathfrak{a}) \cup \mathcal{Z}(\mathfrak{b})$.*

(vi) *$S \subset \mathcal{Z}(\mathcal{J}(S))$ y $\mathcal{J}(\mathcal{Z}(\mathcal{J}(S))) = \mathcal{J}(S)$. Además, S es un conjunto algebraico si $S = \mathcal{Z}(\mathcal{J}(S))$. De hecho, $\mathcal{Z}(\mathcal{J}(S))$ es el mejor conjunto algebraico de K^n que contiene a S.*

(vii) *$\mathfrak{a} \subset \mathcal{J}(\mathcal{Z}(\mathfrak{a}))$ y $\mathcal{Z}(\mathcal{J}(\mathcal{Z}(\mathfrak{a}))) = \mathcal{Z}(\mathfrak{a})$. De hecho, $\mathcal{J}(\mathcal{Z}(\mathfrak{a}))$ es el mayor ideal de $K[\mathtt{x}]$ cuyo conjunto de ceros coincide con $\mathcal{Z}(\mathfrak{a})$.*

(viii) *Si $S \subsetneq T$ son conjuntos algebraicos, entonces $\mathcal{J}(T) \subsetneq \mathcal{J}(S)$.*

A continuación veremos como es el ideal de ceros de los puntos de K^n.

Lema I.2.5 (Ideal maximal asociado a un punto) *Si $p := (p_1, \ldots, p_n) \in K^n$, entonces $\mathfrak{m}_p := \mathcal{J}(\{p\}) = \{\mathtt{x}_1 - p_1, \ldots, \mathtt{x}_n - p_n\}K[\mathtt{x}]$ es un ideal maximal de $K[\mathtt{x}]$ y $K[\mathtt{x}]/\mathfrak{m}_p \cong K$.*

Demostración. Consideramos el homomorfismo evaluación

$$\mathrm{ev}_p : K[\mathtt{x}] \to K,\ f \mapsto f(p),$$

que es suprayectivo. Por tanto su núcleo $\ker(\mathrm{ev}_p) = \mathfrak{m}_p$ es un ideal maximal de $K[\mathtt{x}]$ que contiene a los polinomios $\mathtt{x}_1 - p_1, \ldots, \mathtt{x}_n - p_n \in \mathfrak{m}_p$ y cumple que $K[\mathtt{x}]/\mathfrak{m}_p \cong K$ (por el primer teorema de isomorfía). Si demostramos que $\ker(\mathrm{ev}_p) \subset \{\mathtt{x}_1 - p_1, \ldots, \mathtt{x}_n - p_n\}K[\mathtt{x}]$, concluiremos la demostración del enunciado. Sea $f \in \ker(\mathrm{ev}_p)$ y lo dividimos sucesivamente entre los polinomios $\mathtt{x}_1 - p_1, \ldots, \mathtt{x}_n - p_n$. Obtenemos polinomios $g_k \in K[\mathtt{x}_k, \ldots, \mathtt{x}_n]$ y $a \in K$ tales que

$$f = \sum_{k=1}^{n} (\mathtt{x}_k - p_k) g_k + a.$$

Observamos que $a = f(p) = 0$ porque $f \in \ker(\mathrm{ev}_p)$, con lo que $f \in \{\mathtt{x}_1 - p_1, \ldots, \mathtt{x}_n - p_n\}K[\mathtt{x}]$. □

2.c. Conjuntos algebraicos irreducibles. Una estrategia habitual en Matemáticas consiste en la descomposición de los objetos de una cierta teoría como "yuxtaposición" finita "única" de objetos de esa teoría que ya no pueden descomponerse nuevamente. Por ejemplo el Teorema fundamental de la Aritmética afirma que todo entero positivo se descompone de forma única como producto finito de números primos. Demostraremos a continuación que los conjuntos algebraicos admiten descomposiciones "únicas" como uniones finitas de conjuntos algebraicos *irreducibles*. Denotamos $E := K^n$ o $K\mathbb{P}^n$ para referirnos a ambos espacios indistintamente.

Definición I.2.6 Un conjunto algebraico $X \subset E$ es *reducible* si existen conjuntos algebraicos X_1, X_2 de E no vacíos y estrictamente contenidos en X cuya unión es X. En caso contrario diremos que X es *irreducible*.

A continuación, proporcionamos una caracterización algebraica de los conjuntos irreducibles. Denotamos

$$A(E) = \begin{cases} K[\mathtt{x}] & \text{si } E = K^n, \\ K[\mathtt{x}^*] & \text{si } E = K\mathbb{P}^n. \end{cases}$$

Lema I.2.7 *Un subconjunto algebraico $X \subset E$ es irreducible si y solo si $\mathcal{J}(X)$ es un ideal primo de $A(E)$.*

Demostración. Supongamos primero que X es irreducible y que $\mathcal{J}(X)$ no es un ideal primo. Entonces existen $f_1, f_2 \in A(E) \setminus \mathcal{J}(X)$ tales que $f_1 f_2 \in \mathcal{J}(X)$. Por tanto, $X = (X \cap \mathcal{Z}(f_1)) \cup (X \cap \mathcal{Z}(f_2))$ y $X \cap \mathcal{Z}(f_i) \subsetneq X$ para $i = 1, 2$, lo que implicaría que X es reducible.

Supongamos ahora que $\mathcal{J}(X)$ es un ideal primo de $A(E)$. Si $X \subset E$ es reducible, entonces existen conjuntos algebraicos $X_1, X_2 \subsetneq X$ tales que $X = X_1 \cup X_2$. Como $X_i = \mathcal{Z}(\mathcal{J}(X_i))$ y $X = \mathcal{Z}(\mathcal{J}(X))$ existe $f_i \in \mathcal{J}(X_i) \setminus \mathcal{J}(X)$ para $i = 1, 2$. Por tanto, $f_1 f_2 \in \mathcal{J}(X)$ y este ideal no sería primo. □

A la vista del resultado anterior, presentamos a continuación un criterio acerca de la primalidad de los ideales homogéneos de $K[\mathtt{x}^*]$.

Lema I.2.8 *Sea $\mathfrak{p} \subset K[\mathtt{x}^*]$ un ideal homogéneo. Entonces $\mathfrak{p}$ es un ideal primo de $K[\mathtt{x}^*]$ si y solo si para todo par de polinomios homogéneos $F, G \in K[\mathtt{x}^*] \setminus \mathfrak{p}$ se cumple que $FG \notin \mathfrak{p}$.*

Demostración. La implicación $\Longrightarrow$) es inmediata. Para probar la implicación recíproca consideramos dos polinomios $f, g \in K[\mathtt{x}^*] \setminus \mathfrak{p}$ y escribimos $f = \sum_{i=0}^{d} f_i$ y $g = \sum_{j=0}^{e} g_j$ donde $f_i, g_j \in K[\mathtt{x}^*]$ son las componentes homogéneas de f, g. Sea i_0 el menor índice tal que $f_i \notin \mathfrak{p}$ y j_0 el menor índice tal que $g_j \notin \mathfrak{p}$. La componente homogénea $(i_0 + j_0)$ de fg es $\sum_{k+\ell=i_0+j_0} f_k g_\ell$. Como $\mathfrak{p}$ es un ideal homogéneo, si $fg \in \mathfrak{p}$, entonces $\sum_{k+\ell=i_0+j_0} f_k g_\ell \in \mathfrak{p}$. Como $f_k \in \mathfrak{p}$ para $k < i_0$ y $g_\ell \in \mathfrak{p}$ para $\ell < j_0$, deducimos que

$$f_{i_0} g_{j_0} = \sum_{k+\ell=i_0+j_0} f_k g_\ell - \sum_{k+\ell=i_0+j_0, k\neq i_0} f_k g_\ell \in \mathfrak{p},$$

lo que es una contradicción ya que los polinomios homogéneos $f_{i_0}, g_{j_0} \in K[\mathtt{x}^*] \setminus \mathfrak{p}$. Por tanto, $fg \notin \mathfrak{p}$ y $\mathfrak{p}$ es un ideal primo. □

Lema I.2.9 *Si $X, X_1, X_2 \subset E$ son conjuntos algebraicos tales que X es irreducible y $X \subset X_1 \cup X_2$, entonces $X \subset X_1$ o $X \subset X_2$.*

Demostración. Observamos que $X = (X \cap X_1) \cup (X \cap X_2)$ y como X es irreducible, entonces $X = X \cap X_1$ o $X = X \cap X_2$, con lo que $X \subset X_1$ o $X \subset X_2$. □

Proposición I.2.10 (Componentes irreducibles) *Sea $X \subset E$ un conjunto algebraico. Entonces existen conjuntos algebraicos irreducibles $X_1, \ldots, X_r \subset$*

E tales que $X = \bigcup_{i=1}^{r} X_i$ y $X_i \not\subset X_j$ si $i \neq j$. Además, los conjuntos algebraicos X_i son únicos (salvo reordenación de los índices) y reciben el nombre de componentes irreducibles de X.

Demostración. Existencia. Sea $\mathfrak{F}$ la familia de los subconjuntos algebraicos de E que no se pueden escribir como unión finita de conjuntos algebraicos irreducibles y la ordenamos con la relación de orden (parcial) dada por la inclusión. Veamos que si $\mathfrak{F} \neq \varnothing$, entonces tiene un elemento minimal. En caso contrario existirían conjuntos algebraicos $X_k \in \mathfrak{F}$ tales que $X_{k+1} \subsetneq X_k$ para $k \geq 1$. Por tanto, tenemos $\mathcal{J}(X_k) \subsetneq \mathcal{J}(X_{k+1})$ para $k \geq 1$. El lector puede comprobar que $\mathfrak{a} := \bigcup_{k\geq 1} \mathcal{J}(X_k)$ es un ideal de $K[\mathtt{x}]$ si $E = K^n$ o un ideal homogéneo de $K[\mathtt{x}^*]$ si $E = K\mathbb{P}^n$. Como los anillos de polinomios con coeficientes en un cuerpo son anillos noetherianos el ideal $\mathfrak{a}$ es finitamente generado y por tanto existe $k \geq 1$ tal que $\mathcal{J}(X_k) = \mathcal{J}(X_{k+\ell})$ para cada $\ell \geq 1$. Por tanto, $X_k = X_{k+\ell}$ para cada $\ell \geq 1$, lo que es una contradicción.

Sea Y un elemento minimal de $\mathfrak{F}$. Como Y no se puede escribir como unión finita de conjuntos algebraicos irreducibles, entonces Y es necesariamente reducible. Por tanto, existen conjuntos algebraicos Y_1, Y_2 de E tales que $Y = Y_1 \cup Y_2$ e $Y_i \subsetneq Y$ para $i = 1, 2$. Por la minimalidad de Y deducimos que $Y_i \notin \mathfrak{F}$ para $i = 1, 2$. De este modo, cada Y_i se puede escribir como unión finita de conjuntos algebraicos irreducibles y por tanto también Y se podría escribir como unión finita de conjuntos algebraicos irreducibles, lo que implicaría que $Y \notin \mathfrak{F}$. De esta forma, $\mathfrak{F} = \varnothing$ y todo subconjunto algebraico de E se puede escribir como unión finita de conjuntos algebraicos irreducibles.

Unicidad. Sea $X \subset E$ un conjunto algebraico y supongamos que

$$X = \bigcup_{i=1}^{r} X_i = \bigcup_{j=1}^{s} Y_j$$

donde X_i, Y_j son conjuntos algebraicos irreducibles. Eliminando algunos de los conjuntos algebraicos X_i, Y_j podemos suponer que $X_i \not\subset X_k$ si $i \neq k$ e $Y_j \not\subset Y_\ell$ si $j \neq \ell$. Además, supondremos que $r \leq s$. Como, $X_1 \subset \bigcup_{j=1}^{s} Y_j$ es irreducible, podemos suponer por el Lema I.2.9 (tras reordenar los índices j) que $X_1 \subset Y_1 \subset \bigcup_{i=1}^{r} X_i$. Como $X_i \not\subset X_k$ si $i \neq k$ e Y_1 es irreducible, deducimos por el Lema I.2.9 que $X_1 = Y_1$. Este mismo argumento lo podemos aplicar a cada uno de los X_i y deducimos que tras reordenar los indices j podemos suponer que $X_i = Y_i$ para $i = 1, \ldots, r$. Por tanto, $X = \bigcup_{i=1}^{r} Y_i$ y si $r < s$, entonces $Y_s \subset \bigcup_{i=1}^{r} Y_i$ está contenido en algún Y_i para $i = 1, \ldots, r$ (aplicando nuevamente el Lema I.2.9), lo que es una contradicción. Por tanto, $r = s$ y la unicidad queda probada. □

A partir del resultado anterior y el Lema I.2.5 el lector puede probar el siguiente resultado.

Corolario I.2.11 *Sea $X := \{p_i\}_{i=1}^r \subset E$ un conjunto finito. Entonces las componentes irreducibles de X son $\{p_i\}$ para $i = 1, \ldots, r$.*

En particular, el resultado anterior nos dice que los únicos conjuntos finitos irreducibles son aquellos formados por un único punto.

3. Nullstellensatz de Hilbert

Dedicamos esta sección a enunciar y demostrar el llamado Nullstellensatz (Teorema de los ceros) de Hilbert siguiendo la prueba publicada por E. Arrondo en [A1], que se basa esencialmente en el uso astuto de la resultante de dos polinomios. Antes de presentar el Nullstellensatz de Hilbert vamos a presentar algunos resultados previos que tienen interés por si mismos.

3.a. Lema de preparación de Noether.

El siguiente resultado nos permitirá "recolocar" los conjuntos algebraicos para que admitan "mejores" proyecciones. Recordamos que como K es un cuerpo de característica cero, en particular es un cuerpo infinito.

Lema I.3.1 (Lema de preparación de Noether) *Sea $f \in K[\mathtt{x}_1, \ldots, \mathtt{x}_n]$ un polinomio no nulo de grado d.*

(i) *Si f es homogéneo, existe $(b_1, \ldots, b_{n-1}) \in K^{n-1}$ tal que*

$$f(b_1, \ldots, b_{n-1}, 1) \in K \setminus \{0\}.$$

(ii) *Existe $(b_1, \ldots, b_{n-1}) \in K^{n-1}$ tal que el coeficiente del monomio $\mathtt{x}_n^d$ del polinomio*

$$h(\mathtt{x}_1, \ldots, \mathtt{x}_n) := f(\mathtt{x}_1 + b_1\mathtt{x}_n, \ldots, \mathtt{x}_{n-1} + b_{n-1}\mathtt{x}_n, \mathtt{x}_n)$$

es un elemento no nulo de K.

Demostración. (i) Consideramos el polinomio no nulo $g := \mathtt{x}_n f$. Como K es un cuerpo infinito, la función polinómica asociada a g es no nula y por tanto

existe $a := (a_1, \ldots, a_n) \in K^n$ tal que $g(a) \neq 0$, y por tanto $a_n \neq 0$ y $f(a) \neq 0$. Definimos $b_k := \frac{a_k}{a_n} \in K$ para $1 \leq k \leq n$. Nótese que $b_n = 1$ y, por ser f homogéneo de grado $d := \deg(f)$, se deduce

$$0 \neq f(a) = f(a_n b_1, \ldots, a_n b_n) = a_n^d f(b_1, \ldots, b_{n-1}, 1),$$

luego $f(b_1, \ldots, b_{n-1}, 1) \neq 0$.

(ii) Escribimos $f := \sum_{j=0}^{d} f_j$ donde cada f_j es un polinomio homogéneo de grado j y $f_d \neq 0$. Aplicando a f_d el apartado (i) existe $(b_1, \ldots, b_{n-1}) \in K^{n-1}$ tal que $f_d(b_1, \ldots, b_{n-1}, 1) \neq 0$. Como

$$\begin{aligned} h(\mathtt{x}_1, \ldots, \mathtt{x}_n) &= f(\mathtt{x}_1 + b_1\mathtt{x}_n, \ldots, \mathtt{x}_{n-1} + b_{n-1}\mathtt{x}_n, \mathtt{x}_n) \\ &= \sum_{j=0}^{d} f_j(\mathtt{x}_1 + b_1\mathtt{x}_n, \ldots, \mathtt{x}_{n-1} + b_{n-1}\mathtt{x}_n, \mathtt{x}_n), \end{aligned}$$

el coeficiente en el polinomio h del monomio $\mathtt{x}_n^d$ coincide con el coeficiente de $\mathtt{x}_n^d$ en el polinomio $f_d(\mathtt{x}_1 + b_1\mathtt{x}_n, \ldots, \mathtt{x}_{n-1} + b_{n-1}\mathtt{x}_n, \mathtt{x}_n)$. Pero el monomio en $\mathtt{x}_n^d$ de este polinomio es

$$f_d(b_1\mathtt{x}_n, \ldots, b_{n-1}\mathtt{x}_n, \mathtt{x}_n) = f_d(b_1, \ldots, b_{n-1}, 1)\mathtt{x}_n^d,$$

que es no nulo. □

3.b. Forma débil del Nullstellensatz de Hilbert. Empezamos demostrando que si trabajamos con coeficientes en un cuerpo algebraicamente cerrado, el lugar de ceros de cualquier ideal de $K[\mathtt{x}]$ es no vacío.

Teorema I.3.2 *Sean K un cuerpo algebraicamente cerrado y $\mathfrak{a}$ un ideal del anillo de polinomios $K[\mathtt{x}]$. Entonces, existe $a := (a_1, \ldots, a_n) \in K^n$ tal que $f(a) = 0$ para cada $f \in \mathfrak{a}$.*

Demostración. Probamos el teorema por inducción sobre n. Si $n = 1$ el anillo $K[\mathtt{x}_1]$ es un dominio de ideales principales, luego existe $g \in \mathfrak{a}$ tal que $\mathfrak{a} = gK[\mathtt{x}_1]$. El polinomio g no es constante ya que $\mathfrak{a}$ es un ideal propio, luego por ser K algebraicamente cerrado existe $a \in K$ tal que $g(a) = 0$. Para cada $f \in \mathfrak{a}$ existe $h \in K[\mathtt{x}_1]$ tal que $f = hg$, y por ello $f(a) = h(a)g(a) = 0$, así que el punto a cumple lo requerido.

Supongamos $n > 1$. El resultado es trivial si $\mathfrak{a}$ es el ideal nulo, así que suponemos que no lo es y, aplicando el Lema I.3.1 a un polinomio no nulo de

$\mathfrak{a}$, existe $(b_1, \ldots, b_{n-1}) \in K^{n-1}$ tal que tras un cambio de variables de la forma

$$(\mathtt{x}_1, \ldots, \mathtt{x}_n) \mapsto (\mathtt{y}_1, \ldots, \mathtt{y}_n) := (\mathtt{x}_1 + b_1\mathtt{x}_n, \ldots, \mathtt{x}_{n-1} + b_{n-1}\mathtt{x}_n, \mathtt{x}_n),$$

que no afecta al enunciado, podemos suponer que el ideal $\mathfrak{a}$ contiene un polinomio g de grado d de la forma

$$g := g_0(\mathtt{x}') + g_1(\mathtt{x}')\mathtt{x}_n + \cdots + g_{d-1}(\mathtt{x}')\mathtt{x}_n^{d-1} + \mathtt{x}_n^d,$$

donde $\mathtt{x}' := (\mathtt{x}_1, \ldots, \mathtt{x}_{n-1})$ y cada $g_j \in K[\mathtt{x}'] := K[\mathtt{x}_1, \ldots, \mathtt{x}_{n-1}]$.

El ideal $\mathfrak{a}_1 := \mathfrak{a} \cap K[\mathtt{x}'] \subsetneq K[\mathtt{x}']$ porque $1 \notin \mathfrak{a}$. Por la hipótesis de inducción, existe un punto $a' := (a_1, \ldots, a_{n-1}) \in K^{n-1}$ tal que $f(a') = 0$ para cada $f \in \mathfrak{a}_1$. El punto clave en la prueba es demostrar que

$$\mathfrak{b} := \{f(a', \mathtt{x}_n) : \ f \in \mathfrak{a}\}$$

es un ideal propio de $K[\mathtt{x}_n]$.

Desde luego $\mathfrak{b} \neq \{0\}$, pues $0 \neq g(a', \mathtt{x}_n) \in \mathfrak{b}$. Además, la comprobación de que $\mathfrak{b}$ es ideal es inmediata, luego se trata de probar que $\mathfrak{b} \neq K[\mathtt{x}_n]$. En caso contrario existiría $f \in \mathfrak{a}$ tal que $1 = f(a', \mathtt{x}_n)$. Si $m = \deg(f)$ escribimos

$$f(\mathtt{x}_1, \ldots, \mathtt{x}_n) = f_0(\mathtt{x}') + f_1(\mathtt{x}')\mathtt{x}_n + \cdots + f_m(\mathtt{x}')\mathtt{x}_n^m,$$

donde cada $f_j \in K[\mathtt{x}']$. Como $K[\mathtt{x}']$ es dominio, existen polinomios $p, q \in K[\mathtt{x}'][\mathtt{x}_n]$ tales que $R := \mathrm{Res}_{\mathtt{x}_n}(f, g) = fp + gq \in \mathfrak{a}$. Como, además, $R \in K[\mathtt{x}']$ concluimos que $R \in \mathfrak{a}_1$, y por tanto $R(a') = 0$, ya que todos los polinomios del ideal $\mathfrak{a}_1$ se anulan en el punto a'. Sin embargo, como

$$1 = f(a', \mathtt{x}_n) = f_0(a') + f_1(a')\mathtt{x}_n + \cdots + f_m(a')\mathtt{x}_n^m,$$

se tiene $f_0(a') = 1$ y $f_j(a') = 0$ para $1 \leq j \leq m$. Así, al evaluar $R(a')$ obtenemos

$$R(a') = \det \begin{bmatrix} f_0(a') & f_1(a') & \cdots & f_m(a') & 0 & 0 & \cdots & 0 \\ 0 & f_0(a') & f_1(a') & \cdots & f_m(a') & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & f_0(a') & f_1(a') & f_2(a') & \cdots & f_m(a') \\ g_0(a') & g_1(a') & \cdots & g_{d-1}(a') & 1 & 0 & \cdots & 0 \\ 0 & g_0(a') & g_1(a') & \cdots & g_{d-1}(a') & 1 & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & g_0(a') & g_1(a') & \cdots & 1 \end{bmatrix}$$

$$= \det \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0 \\ g_0(a') & g_1(a') & \cdots & g_{d-1}(a') & 1 & 0 & \cdots & 0 \\ 0 & g_0(a') & g_1(a') & \cdots & g_{d-1}(a') & 1 & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & g_0(a') & g_1(a') & \cdots & 1 \end{bmatrix} = 1,$$

y esto contradice que $R(a') = 0$.

Así, $\mathfrak{b}$ es un ideal propio de $K[\mathtt{x}_n]$, luego es un ideal principal generado por un polinomio $h \in K[\mathtt{x}_n] \setminus K$. Por ser K algebraicamente cerrado existe $a_n \in K$ tal que $h(a_n) = 0$. Como para cada $f \in \mathfrak{a}$ el polinomio $f(a', \mathtt{x}_n) \in \mathfrak{b} = hK[\mathtt{x}_n]$, existe $p \in K[\mathtt{x}_n]$ tal que $f(a', \mathtt{x}_n) = h(\mathtt{x}_n)p(\mathtt{x}_n)$, por lo que el punto $a := (a', a_n) \in K^n$ cumple que $f(a) = f(a', a_n) = h(a_n)p(a_n) = 0$. □

Observación I.3.3 En el teorema anterior la hipótesis de que K sea algebraicamente cerrado es esencial. Si K no es algebraicamente cerrado, existen polinomios no constantes $f \in K[\mathtt{x}_1]$ sin raíces en K, luego no existen puntos $a \in K^n$ en los que se anulen todos los polinomios del ideal $\mathfrak{a}$ de $K[\mathtt{x}]$ generado por f.

3.c. Forma fuerte del Nullstellensatz de Hilbert. A continuación, presentamos para el caso afín el Nullstellensatz de Hilbert.

Teorema I.3.4 (Nullstellensatz de Hilbert) *Dados un cuerpo algebraicamente cerrado K y un ideal $\mathfrak{a}$ de $K[\mathtt{x}]$ se cumple la igualdad $\mathcal{J}\big(\mathcal{Z}(\mathfrak{a})\big) = \sqrt{\mathfrak{a}}$.*

Demostración. La inclusión $\mathfrak{a} \subset \mathcal{J}(\mathcal{Z}(\mathfrak{a}))$ es inmediata. De aquí se deduce el contenido $\sqrt{\mathfrak{a}} \subset \mathcal{J}(\mathcal{Z}(\mathfrak{a}))$ pues sabemos que el ideal $\mathcal{J}(\mathcal{Z}(\mathfrak{a}))$ es radical. Para demostrar la inclusión recíproca empleamos el denominado truco de Rabinowitsch. Aunque no es imprescindible utilizamos, por comodidad, el Teorema de la base de Hilbert, I.1.2, en virtud del cual existen polinomios $f_1, \ldots, f_m \in \mathfrak{a}$ tales que $\mathfrak{a} = (f_1, \ldots, f_m)K[\mathtt{x}]$. Ahora, dado $f \in \mathcal{J}(\mathcal{Z}(\mathfrak{a})) \setminus \{0\}$ consideramos el ideal

$$\mathfrak{b} := \big(f_1, \ldots, f_m, (\mathtt{x}_{n+1}f - 1)\big)K[\mathtt{x}, \mathtt{x}_{n+1}].$$

Obsérvese que el conjunto $\mathcal{Z}(\mathfrak{b})$ de ceros de $\mathfrak{b}$ es vacío, pues si contuviese algún punto $(a, a_{n+1}) \in K^n \times K = K^{n+1}$ tendríamos $f_j(a) = 0$ para $1 \leq j \leq m$

y, además, $a_{n+1}f(a) = 1$. Sin embargo, $f(a) = 0$ ya que $a \in \mathcal{Z}(\mathfrak{a})$, lo que contradice la igualdad $1 = a_{n+1}f(a)$. Por tanto, $\mathcal{Z}(\mathfrak{b}) = \varnothing$ y esto implica, por la forma débil del Nullstellensatz de Hilbert, que el ideal $\mathfrak{b}$ es el anillo total $K[\mathtt{x}, \mathtt{x}_{n+1}]$. Así, existen $h_1, \ldots, h_{m+1} \in K[\mathtt{x}, \mathtt{x}_{n+1}]$ tales que

$$1 = f_1h_1 + \cdots + f_mh_m + (\mathtt{x}_{n+1}f - 1)h_{m+1}. \tag{I.3.2}$$

Denotemos $K(\mathtt{x})$ el cuerpo de fracciones del anillo de polinomios $K[\mathtt{x}]$ y consideramos en $K(\mathtt{x})[\mathtt{x}_{n+1}]$ la evaluación $\mathtt{x}_{n+1} := \frac{1}{f}$, que efectuada en la igualdad (I.3.2) nos proporciona

$$1 = f_1(\mathtt{x})h_1\Big(\mathtt{x}, \frac{1}{f}(\mathtt{x})\Big) + \cdots + f_m(\mathtt{x})h_m\Big(\mathtt{x}, \frac{1}{f}(\mathtt{x})\Big).$$

Multiplicando los dos miembros de esta igualdad por f^k, donde k es suficientemente grande para eliminar los denominadores, obtenemos una expresión $f^k = f_1g_1 + \cdots + f_mg_m$, donde cada $g_j \in K[\mathtt{x}]$, y por tanto $f \in \sqrt{\mathfrak{a}}$. □

Recordamos que $\mathfrak{m}_a$ denota el ideal maximal de $K[\mathtt{x}]$ asociado al punto $a \in K^n$ (véase el Lema I.2.5).

Corolario I.3.5 *Sean K un cuerpo. Se cumple que:*

(i) *Si $\mathfrak{m}$ es un ideal maximal del anillo de polinomios $K[\mathtt{x}]$ y $a \in \mathcal{Z}(\mathfrak{m})$, entonces $\mathfrak{m} = \mathfrak{m}_a$ y $\mathcal{Z}(\mathfrak{m}) = \{a\}$.*

(ii) *Supongamos que K es algebraicamente cerrado. Definimos*

$$\begin{aligned}
\mathfrak{X} &:= \{\textit{conjuntos algebraicos de } K^n\},\\
\mathfrak{Y} &:= \{\textit{conjuntos algebraicos irreducibles de } K^n\},\\
\mathfrak{S} &:= \{\{p\} : \ p \in K^n\},\\
\mathfrak{A} &:= \{\textit{ideales radicales de } K[\mathtt{x}]\},\\
\mathfrak{P} &:= \{\textit{ideales primos de } K[\mathtt{x}]\},\\
\mathfrak{M} &:= \{\textit{ideales maximales de } K[\mathtt{x}]\}.
\end{aligned}$$

Entonces la aplicación $\phi : \mathfrak{X} \to \mathfrak{A},\ X \mapsto \mathcal{J}(X)$ es una biyección cuya inversa $\psi : \mathfrak{A} \to \mathfrak{X},\ \mathfrak{a} \mapsto \mathcal{Z}(\mathfrak{a})$. Además, $\phi(\mathfrak{Y}) = \mathfrak{P}$ y $\phi(\mathfrak{S}) = \mathfrak{M}$.

Demostración. (i) Como $a \in \mathcal{Z}(\mathfrak{m})$ cada f de $\mathfrak{m}$ se anula en a, o sea, $\mathfrak{m} \subset \mathfrak{m}_a$. Así, como $\mathfrak{m}$ es maximal, $\mathfrak{m} = \mathfrak{m}_a$.

(ii) Como consecuencia del Nullstellensatz de Hilbert si $\mathfrak{a}$ es un ideal radical, entonces $(\phi \circ \psi)(\mathfrak{a}) = \mathcal{J}(\mathcal{Z}(\mathfrak{a})) = \mathfrak{a}$. Por otra parte, si X es un conjunto algebraico, $(\psi \circ \phi)(X) = \mathcal{Z}(\mathcal{J}(X)) = X$. Por el Lema I.2.7 sabemos que un conjunto algebraico $X \subset K^n$ es irreducible si y solo si $\mathcal{J}(X)$ es primo, de este modo dado que los ideales primos son radicales deducimos que $\phi(\mathfrak{Y}) = \mathfrak{P}$. Por el Lema I.2.5 y el apartado (i) deducimos $\phi(\mathfrak{S}) = \mathfrak{M}$. □

Observación I.3.6 Si K no es algebraicamente cerrado, la aplicación ψ del Corolario I.3.5 (ii) no es sobreyectiva. En efecto, vimos en I.3.3 que existe un ideal propio $\mathfrak{a}$ de $K[\mathtt{x}]$ tal que $\mathcal{Z}(\mathfrak{a}) = \varnothing$. Sea $\mathfrak{m}$ un ideal maximal de $K[\mathtt{x}]$ que contiene al ideal $\mathfrak{a}$, luego $\mathcal{Z}(\mathfrak{m})$ es vacío, así que $\mathfrak{m} \neq \mathfrak{m}_a$ para cada $a \in K^n$.

En el caso proyectivo el Nullstellensatz de Hilbert adquiere la siguiente forma.

Corolario I.3.7 *Sea $\mathfrak{a} \subset K[\mathtt{x}^*]$ un ideal homogéneo y $X = \mathcal{Z}(\mathfrak{a})$. Se cumple:*

(i) *$X = \varnothing$ si y solo si $\sqrt{\mathfrak{a}}$ contienen al ideal $\mathfrak{m}_0 := \{\mathtt{x}_0, \ldots, \mathtt{x}_n\}K[\mathtt{x}^*]$.*

(ii) *Si $X \neq \varnothing$, entonces $\mathcal{J}(X) = \sqrt{\mathfrak{a}}$.*

Demostración. (i) Sean $\pi : K^{n+1} \setminus \{0\} \to K\mathbb{P}^n$, $x^* \mapsto [x^*]$ y $\widehat{X} = \mathcal{Z}(\mathfrak{a}) \subset K^{n+1}$. Como $X = \pi(\widehat{X})$ se cumple que $X = \varnothing$ si y solo si $\widehat{X} \subset \{0\}$ lo que sucede si y solo si $\mathfrak{m}_0 = \mathcal{J}(\{0\}) \subset \mathcal{J}(\widehat{X})$.

(ii) Como $X \neq \varnothing$, entonces $\widehat{X} = \pi^{-1}(X) \cup \{0\}$ es el lugar de ceros de $\mathfrak{a}$ en K^{n+1}. Por el Nullstellensatz de Hilbert I.3.4 se cumple que $\mathcal{J}(\widehat{X}) = \sqrt{\mathfrak{a}}$, que es por el Lema I.2.3 un ideal homogéneo de $K[\mathtt{x}^*]$. Como $\widehat{X} = \pi^{-1}(X) \cup \{0\}$, deducimos que $\mathcal{J}(X) = \sqrt{\mathfrak{a}}$. □

4. Conjuntos algebraicos del plano

El objetivo de esta sección es determinar cómo son los conjuntos algebraicos de K^2. El lector debe tener en cuenta que hay que distinguir entre los conjuntos de ceros y las ecuaciones polinómicas que los describen. Por ejemplo, $X = \mathcal{Z}(\mathtt{x}_1+\mathtt{x}_2) = \mathcal{Z}((\mathtt{x}_1+\mathtt{x}_2)^3)$, sin embargo, los polinomios que describen a X tienen en cada caso grados diferentes. Nosotros estamos interesados en el estudio de las propiedades de las ecuaciones polinómicas y no solo de los conjuntos que describen. Por tanto, una *curva algebraica (afín)* es un polinomio no nulo

$f \in K[\mathtt{x}_1, \mathtt{x}_2]$ módulo proporcionalidad por elementos de $K \setminus \{0\}$. Eliminamos la proporcionalidad porque las propiedades algebraicas de los polinomios f y λf son las mismas siempre que $\lambda \in K \setminus \{0\}$. Comenzamos analizando cómo son las intersecciones de dos curvas algebraicas que no comparten componentes irreducibles. Recordamos que K es un cuerpo de característica cero y por tanto infinito.

4.a. Forma débil del Teorema de Bézout. A continuación presentamos la forma débil del Teorema de Bézout para curvas algebraicas (afines) (y posteriormente explicaremos lo que ocurre en el caso proyectivo). Este resultado nos dice que dos curvas algebraicas de grados d y e (que no comparte ningún factor irreducible) se cortan a lo sumo en $d \cdot e$ puntos. Este resultado se puede entender como una generalización de algunos ya conocidos por el lector: dos rectas (curvas de grado 1) no coincidentes se cortan en a lo sumo un punto, una cónica no degenerada y una recta se cortan en a lo sumo dos puntos. Pero también del siguiente: *un polinomio $f \in K[\mathtt{x}_1]$ no nulo tiene a lo sumo d raíces en K*. Para ello, consideremos las curvas algebraicas $\mathtt{x}_2 - f(\mathtt{x}_1)$ (curva de grado $\deg(f)$) y $\mathtt{x}_2$ (curva de grado 1). La intersección $\mathcal{Z}(\mathtt{x}_2 - f(\mathtt{x}_1), \mathtt{x}_2)$ tiene tantos elementos como raíces tiene f en K. Si K es algebraicamente cerrado, entonces $\deg(f)$ coincide con el número de raíces de f en K "contadas con su multiplicidad". Este resultado más fuerte se puede también generalizar para curvas algebraicas proyectivas dando lugar a la forma fuerte del Teorema de Bézout, que veremos en el Capítulo III.

Teorema I.4.1 *Sean $f, g \in K[\mathtt{x}_1, \mathtt{x}_2]$ dos polinomios primos entre sí de grados d y e. Entonces $\mathcal{Z}(f, g)$ es un conjunto finito formado por a lo sumo $d \cdot e$ puntos.*

Antes de probar el resultado anterior necesitamos el siguiente resultado acerca de las propiedades de la resultante de dos polinomios de $K[\mathtt{x}]$. Denotamos $\mathtt{x} := (\mathtt{x}_1, \ldots, \mathtt{x}_n)$ y $\mathtt{x}' := (\mathtt{x}_1, \ldots, \mathtt{x}_{n-1})$.

Lema I.4.2 (Grado de la resultante) *Sean $f, g \in K[\mathtt{x}]$ polinomios de grados d y e tales que $f(0, \mathtt{x}_n), g(0, \mathtt{x}_n) \in K[\mathtt{x}_n]$ son también polinomios de grados d y e. Entonces $\mathrm{Res}_{\mathtt{x}_n}(\widehat{f}, \widehat{g})$ es un polinomio homogéneo de grado $d \cdot e$ y $\mathrm{Res}_{\mathtt{x}_n}(f, g) \in K[\mathtt{x}']$ es un polinomio de grado $\leq d \cdot e$.*

Demostración. Escribimos $f := \sum_{k=0}^{d} a_k \mathtt{x}_n^k$ y $g := \sum_{\ell=0}^{e} b_\ell \mathtt{x}_n^\ell$ donde $a_k, b_\ell \in K[\mathtt{x}']$ y $a_d, b_e \in K \setminus \{0\}$. Sean $\widehat{f}, \widehat{g} \in K[\mathtt{x}^*]$ los homogeneizados de f, g. Entonces $\widehat{f} = \sum_{k=0}^{d} a_k^* \mathtt{x}_n^k$ y $\widehat{g} = \sum_{\ell=0}^{e} b_\ell^* \mathtt{x}_n^\ell$ donde $a_k^*, b_\ell^* \in K[\mathtt{x}_0, \mathtt{x}']$ son polinomios

homogéneos de grados $d-k$ y $e-\ell$ respectivamente y $a_d^* = a_d \in K \setminus \{0\}$ y $b_e^* = b_e \in K \setminus \{0\}$. Observamos que $\mathrm{Res}_{\mathtt{x}_n}(\widehat{f},\widehat{g}) \in K[\mathtt{x}_0,\mathtt{x}']$ cumple que $\mathrm{Res}_{\mathtt{x}_n}(f,g) = \mathrm{Res}_{\mathtt{x}_n}(\widehat{f},\widehat{g})(1,\mathtt{x}')$. Así que si demostramos: $\mathrm{Res}_{\mathtt{x}_n}(\widehat{f},\widehat{g})$ *es un polinomio homogéneo de grado* $d\cdot e$, tendremos que $\mathrm{Res}_{\mathtt{x}_n}(f,g) \in K[\mathtt{x}']$ es un polinomio de grado $\leq d\cdot e$. Por definición, tenemos

$$\mathrm{Res}_{\mathtt{x}_n}(\widehat{f},\widehat{g}) := \det \left[\begin{array}{cccccccc} a_0^* & a_1^* & \cdots & a_d^* & 0 & 0 & \cdots & 0 \\ 0 & a_0^* & a_1^* & \cdots & a_d^* & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_0^* & a_1^* & a_2^* & \cdots & a_d^* \\ \hline b_0^* & b_1^* & \cdots & b_{e-1}^* & b_e^* & 0 & \cdots & 0 \\ 0 & b_0^* & b_1^* & \cdots & b_{e-1}^* & b_e^* & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & b_0^* & b_1^* & \cdots & b_e^* \end{array}\right] \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} e \text{ filas} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} d \text{ filas} \end{array}$$

Observamos que

$$\mathrm{Res}_{\mathtt{x}_n}(\widehat{f},\widehat{g})(\mathtt{t}\mathtt{x}_0,\mathtt{t}\mathtt{x}') = \det \left[\begin{array}{cccccccc} \mathtt{t}^d a_0^* & \mathtt{t}^{d-1} a_1^* & \cdots & a_d^* & 0 & 0 & \cdots & 0 \\ 0 & \mathtt{t}^d a_0^* & \mathtt{t}^{d-1} a_1^* & \cdots & a_d^* & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \mathtt{t}^d a_0^* & \mathtt{t}^{d-1} a_1^* & \mathtt{t}^{d-2} a_2^* & \cdots & a_d^* \\ \hline \mathtt{t}^e b_0^* & \mathtt{t}^{e-1} b_1^* & \cdots & \mathtt{t} b_{e-1}^* & b_e^* & 0 & \cdots & 0 \\ 0 & \mathtt{t}^e b_0^* & \mathtt{t}^{e-1} b_1^* & \cdots & \mathtt{t} b_{e-1}^* & b_e^* & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \mathtt{t}^e b_0^* & \mathtt{t}^{e-1} b_1^* & \cdots & b_e^* \end{array}\right]$$

En las e primeras filas multiplicamos la fila i-ésima por $\mathtt{t}^{e-i}$ y en las d siguientes filas multiplicamos la fila i-ésima por $\mathtt{t}^{d+e-i}$. De esta forma obtenemos $\prod_{i=1}^{e} \mathtt{t}^{e-i} \prod_{j=1}^{d} \mathtt{t}^{d-j}\, \mathrm{Res}_{\mathtt{x}_n}(\widehat{f},\widehat{g})(\mathtt{t}\mathtt{x}_0,\mathtt{t}\mathtt{x}')$ que es igual al determinante de la matriz

$$\left[\begin{array}{cccccccc} \mathtt{t}^{d+e-1} a_0^* & \mathtt{t}^{d+e-2} a_1^* & \cdots & \mathtt{t}^{e-1} a_d^* & 0 & 0 & \cdots & 0 \\ 0 & \mathtt{t}^{d+e-2} a_0^* & \mathtt{t}^{d+e-3} a_1^* & \cdots & \mathtt{t}^{e-2} a_d^* & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & \mathtt{t}^d a_0^* & \mathtt{t}^{d-1} a_1^* & \mathtt{t}^{d-2} a_2^* & \cdots & a_d^* \\ \hline \mathtt{t}^{d+e-1} b_0^* & \mathtt{t}^{d+e-2} b_1^* & \cdots & \mathtt{t}^d b_{e-1}^* & \mathtt{t}^{d-1} b_e^* & 0 & \cdots & 0 \\ 0 & \mathtt{t}^{d+e-2} b_0^* & \mathtt{t}^{d+e-3} b_1^* & \cdots & \mathtt{t}^{d-1} b_{e-1}^* & \mathtt{t}^{d-2} b_e^* & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \mathtt{t}^e b_0^* & \mathtt{t}^{e-1} b_1^* & \cdots & b_e^* \end{array}\right].$$

En el determinante anterior podemos extraer $\mathtt{t}^{d+e-j}$ en la columna j-ésima y obtenemos:

$$\prod_{j=1}^{d+e} \mathtt{t}^{d+e-j} \det \left[\begin{array}{cccccccc} a_0^* & a_1^* & \cdots & a_d^* & 0 & 0 & \cdots & 0 \\ 0 & a_0^* & a_1^* & \cdots & a_d^* & 0 & \cdots & 0 \\ \vdots & & \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_0^* & a_1^* & a_2^* & \cdots & a_d^* \\ \hline b_0^* & b_1^* & \cdots & b_{e-1}^* & b_e^* & 0 & \cdots & 0 \\ 0 & b_0^* & b_1^* & \cdots & b_{e-1}^* & b_e^* & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & b_0^* & b_1^* & \cdots & b_e^* \end{array}\right].$$

Por tanto,

$$\prod_{i=1}^{e} \mathtt{t}^{e-i} \prod_{j=1}^{d} \mathtt{t}^{d-j} \operatorname{Res}_{\mathtt{x}_n}(\widehat{f}, \widehat{g})(\mathtt{t}\mathtt{x}_0, \mathtt{t}\mathtt{x}') = \prod_{j=1}^{d+e} \mathtt{t}^{d+e-j} \operatorname{Res}_{\mathtt{x}_n}(\widehat{f}, \widehat{g})(\mathtt{x}_0, \mathtt{x}')$$

y deducimos que $\operatorname{Res}_{\mathtt{x}_n}(\widehat{f}, \widehat{g})$ es un polinomio homogéneo de grado

$$\sum_{j=1}^{d+e}(d+e-j) - \sum_{i=1}^{e}(e-i) - \sum_{j=1}^{d}(d-j) = \frac{(d+e)(d+e-1)}{2} - \frac{d(d-1)}{2} - \frac{e(e-1)}{2} = de,$$

como queríamos demostrar. □

A continuación probamos el Teorema I.4.1.

Demostración del Teorema I.4.1. La prueba consta de dos partes:

Parte 1. Por el Lema de preparación de Noether I.3.1 podemos suponer que $f(0, \mathtt{x}_2)$ es un polinomio de grado d y $g(0, \mathtt{x}_2)$ es un polinomio de grado e. Por el Lema I.4.2 se cumple que $\operatorname{Res}_{\mathtt{x}_2}(f, g) \in K[\mathtt{x}_1]$ es un polinomio no nulo de grado $\leq d \cdot e$. Como f, g no comparten factores irreducibles se cumple que $\operatorname{Res}_{\mathtt{x}_2}(f, g) \neq 0$ y por tanto tiene a lo sumo $d \cdot e$ raíces. Observamos que si $(x, y) \in \mathcal{Z}(f, g)$ entonces los polinomios $f(x, \mathtt{x}_2)$ y $g(x, \mathtt{x}_2)$ de $K[\mathtt{x}_2]$ tienen una raíz común, con lo que $\operatorname{Res}(f(x, \mathtt{x}_2), g(x, \mathtt{x}_2)) = 0$. Como los coeficientes principales de $f, g \in K[\mathtt{x}_1][\mathtt{x}_2]$ (con respecto a x_2) pertenecen a $K \setminus \{0\}$, deducimos que $\operatorname{Res}_{\mathtt{x}_2}(f, g)$ se comporta bien con respecto a la especialización y por tanto

$$\operatorname{Res}_{\mathtt{x}_2}(f, g)(x) = \operatorname{Res}(f(x, \mathtt{x}_2), g(x, \mathtt{x}_2)) = 0.$$

De esta forma, la primera coordenada del punto $(x, y) \in \mathcal{Z}(f, g)$ es una de entre las (a lo sumo) $d \cdot e$ raíces del polinomio $\mathrm{Res}_{\mathtt{x}_2}(f, g)$. Una vez calculadas las posibles primeras coordenadas de los puntos de $\mathcal{Z}(f, g)$, las segundas coordenadas deben satisfacer las ecuaciones $f(x, \mathtt{x}_2) = 0, g(x, \mathtt{x}_2) = 0$, con lo que a lo sumo tenemos mín$\{d^2e, de^2\}$ puntos en $\mathcal{Z}(f, g)$. Esta cota es muy grosera, pero nos sirve para convencernos de que $\mathcal{Z}(f, g)$ es un conjunto finito.

Parte 2. Veamos a continuación cómo mejorar dicha cota. Consideramos vectores directores $v_i := (a_{1i}, a_{i2})$ de todas las rectas que unen parejas de puntos de $\mathcal{Z}(f, g)$ y supongamos que son en total s. Definimos $h_i := a_{i2}\mathtt{x}_1 - a_{i1}\mathtt{x}_2$ para $i = 1, \ldots, s$ y sean f_d y g_e las formas homogéneas de f y g de grados d y e. Consideramos el polinomio homogéneo $F := f_d g_e \prod_{i=1}^{s} h_i$. Por el Lema I.3.1 existe $b \in K$ tal que $F(b, 1) \neq 0$. Por tanto,

(i) Los coeficientes principales de $f' := f(\mathtt{x}_1 + b\mathtt{x}_2, \mathtt{x}_2)$ y $g' := g(\mathtt{x}_1 + b\mathtt{x}_2, \mathtt{x}_2)$ como polinomios de $K[\mathtt{x}_1][\mathtt{x}_2]$ son elementos no nulos de K.

(ii) El vector $(b, 1)$ no es paralelo a ninguno de los vectores v_i ya que $h_i(b, 1) \neq 0$ para $i = 1, \ldots, s$.

Supongamos que existen puntos $(x, y_1), (x, y_2) \in \mathcal{Z}(f', g')$ con $y_1 \neq y_2$. Entonces $(x + by_j, y_j) \in \mathcal{Z}(f, g)$ y un vector director de la recta que los une es $(b, 1)$, lo que contradice (ii). Por tanto, si dos puntos distintos pertenecen a $\mathcal{Z}(f', g')$, entonces sus primeras coordenadas son distintas. Por lo visto en la primera parte las primeras coordenadas de los puntos de $\mathcal{Z}(f', g')$ son raíces de $\mathrm{Res}_{\mathtt{x}_2}(f', g')$, que es un polinomio no nulo de grado $\leq d \cdot e$. Por tanto, el cardinal de $\mathcal{Z}(f', g')$ es $\leq d \cdot e$. □

En el caso proyectivo tenemos un resultado similar a la forma débil del Teorema de Bézout. Una *curva (algebraica proyectiva)* de $K\mathbb{P}^2$ es la clase de equivalencia módulo proporcionalidad por elementos no nulos de K de un polinomio homogéneo no nulo $F \in K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$.

Teorema I.4.3 *Sean $F, G \in K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ dos polinomios homogéneos primos entre sí de grados d y e. Entonces $\mathcal{Z}(F, G)$ es un conjunto finito formado por a lo sumo $d \cdot e$ puntos.*

Demostración. El lector puede comprobar sin demasiado esfuerzo que como F, G son polinomios primos entre sí entonces (sus deshomogeneizados) $f_0 := F(1, \mathtt{x}_1, \mathtt{x}_2)$ y $g_0 := G(1, \mathtt{x}_1, \mathtt{x}_2)$ también son primos entre sí. Por el Teorema I.4.1 sabemos que $\mathcal{Z}(f_0, g_0)$ es un conjunto finito formado por a lo

sumo $\deg(f_0)\deg(g_0) \leq d \cdot e$ elementos. Análogamente ocurre si consideremos la pareja de polinomios $f_1 := F(\mathtt{x}_0, 1, \mathtt{x}_2)$ y $g_1 := G(\mathtt{x}_0, 1, \mathtt{x}_2)$ y la pareja de polinomios $f_2 := F(\mathtt{x}_0, \mathtt{x}_1, 1)$ y $g_2 := G(\mathtt{x}_0, \mathtt{x}_1, 1)$. Usando las tres cartas afines estándar de $K\mathbb{P}^2$, es decir, $\{\mathtt{x}_0 \neq 0\}$, $\{\mathtt{x}_1 \neq 0\}$ y $\{\mathtt{x}_2 \neq 0\}$, deducimos que

$$\mathcal{Z}(F, G) = \bigcup_{i=1}^{3} (\mathcal{Z}(f_i, g_i))$$

es un conjunto finito. Veamos que en realidad $\mathcal{Z}(F, G)$ solo tiene a lo sumo $d \cdot e$ puntos. Para ello, basta con elegir una recta ℓ de $K\mathbb{P}^2$ que no pase por ninguno de los puntos de $\mathcal{Z}(F, G)$ considerar el complemento afín $K\mathbb{P}^n \setminus \ell$ que contiene a todos los puntos de $\mathcal{Z}(F, G)$. Por el Teorema I.4.1 tendremos que el cardinal de $\mathcal{Z}(F, G) = \mathcal{Z}(F, G) \cap (K\mathbb{P}^n \setminus \ell)$ es $\leq d \cdot e$. Veamos cómo elegir la recta ℓ. Para ello, consideramos los puntos $a_i \in \mathcal{Z}(F, G)$ y una recta genérica $h := \mathtt{b}_0\mathtt{x}_0 + \mathtt{b}_1\mathtt{x}_1 + \mathtt{b}_2\mathtt{x}_2$. Consideramos el polinomio homogéneo $H := \prod_i h(a_i) \in K[\mathtt{b}_0, \mathtt{b}_1, \mathtt{b}_2]$. Por el Lema I.3.1 existe $(b_0, b_1) \in K\mathbb{P}^2$ tal que $H(b_0, b_1, 1) \neq 0$ y elegimos la recta $\ell := b_0\mathtt{x}_0 + b_1\mathtt{x}_1 + \mathtt{x}_2$ a la que no pertenece ninguno de los puntos a_i. □

4.b. Conjuntos algebraicos de K^2 y $K\mathbb{P}^2$. A continuación, vamos a describir cómo son todos los ideales primos de $K[\mathtt{x}_1, \mathtt{x}_2]$ (si K es un cuerpo algebraicamente cerrado) y como consecuencia los conjuntos algebraicos de K^2 y $K\mathbb{P}^2$. Al igual que hemos hecho anteriormente escribimos E para referirnos indistintamente a K^2 o $K\mathbb{P}^2$ y denotamos

$$A(E) = \begin{cases} K[\mathtt{x}_1, \mathtt{x}_2] & \text{si } E = K^2, \\ K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2] & \text{si } E = K\mathbb{P}^2. \end{cases}$$

En el caso en el que $E = K\mathbb{P}^2$ los polinomios de $A(E)$ involucrados que elegiremos en los enunciados serán homogéneos.

Lema I.4.4 (de Study) *Sean $f, g \in A(E)$ polinomios tales que f es irreducible y $\mathcal{Z}(f, g)$ es un conjunto infinito. Entonces f divide a g en $A(E)$.*

Demostración. Dado que f es irreducible, entonces f divide a g o f, g son primos entre sí. Por tanto, debemos descartar el segundo caso. Por los Teoremas I.4.1 y I.4.3 si f, g son primos entre sí, tenemos que $\mathcal{Z}(f, g)$ es un conjunto finito, contra nuestra hipótesis. Por tanto, f divide a g. □

En lo sucesivo en esta sección supondremos que K es un cuerpo algebraicamente cerrado.

Corolario I.4.5 *Los ideales primos no nulos de* $K[\mathtt{x}_1, \mathtt{x}_2]$ *son de la forma:*

(i) $fK[\mathtt{x}_1, \mathtt{x}_2]$ *donde* $f \in K[\mathtt{x}_1, \mathtt{x}_2]$ *es un polinomio irreducible.*

(ii) $\mathfrak{m}_p = \{\mathtt{x}_1 - p_1, \mathtt{x}_2 - p_2\}K[\mathtt{x}_1, \mathtt{x}_2]$ *donde* $p := (p_1, p_2) \in K^2$.

Demostración. Sea $\mathfrak{p}$ un ideal primo no nulo de $K[\mathtt{x}_1, \mathtt{x}_2]$. Si $\mathcal{Z}(\mathfrak{p})$ es un conjunto finito, entonces $\mathcal{Z}(\mathfrak{p}) = \{p\}$ donde $p \in K^2$ (dado que los únicos conjuntos irreducibles finitos son los formados por un único punto). En ese caso, por el Nullstellensatz de Hilbert $\mathfrak{p} = \mathcal{J}(\mathcal{Z}(\mathfrak{p})) = \mathfrak{m}_p$. Supongamos entonces que $\mathcal{Z}(\mathfrak{p})$ es un conjunto infinito. Elegimos $f \in \mathfrak{p}\backslash\{0\}$ y escribimos $f = uf_1^{\alpha_1} \cdots f_r^{\alpha_r}$ donde $u \in K \setminus \{0\}$, $f_i \in K[\mathtt{x}_1, \mathtt{x}_2]$ es irreducible y f_i y f_j no son polinomios irreducibles asociados si $i \neq j$. Como $\mathfrak{p}$ es primo, podemos suponer que $f_1 \in \mathfrak{p}$. Si $g \in \mathfrak{p}$, entonces $\mathcal{Z}(\mathfrak{p}) \subset \mathcal{Z}(f_1, g)$ es un conjunto infinito, con lo que por el Lema de Study I.4.4 deducimos que f_1 divide a g. Por tanto, $\mathfrak{p} = f_1 K[\mathtt{x}_1, \mathtt{x}_2]$. □

Observación I.4.6 Si $\mathfrak{p}$ es un ideal primo homogéneo de $K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ tal que $\mathcal{Z}(\mathfrak{p})$ es un conjunto infinito, entonces por el Lema de Study I.4.4 se deduce que $\mathfrak{p}$ es un ideal principal de $K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ generado por un polinomio irreducible homogéneo de $K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$.

Como consecuencia inmediata del Corolario I.4.5 y de la Proposición I.2.10 el lector puede probar el siguiente resultado.

Corolario I.4.7 *Los subconjuntos algebraicos de* K^2 *son las uniones finitas de los siguientes tipos de conjuntos:*

(i) $\varnothing, K^2$.

(ii) $\{p\}$ *donde* $p \in K^2$.

(iii) $\mathcal{Z}(f)$ *donde* $f \in K[\mathtt{x}_1, \mathtt{x}_2]$ *es un polinomio irreducible (curva algebraica afín irreducible).*

Análogamente, como consecuencia inmediata de la Observacion I.4.6 y de la Proposición I.2.10 el lector puede probar el siguiente resultado.

Corolario I.4.8 *Los subconjuntos algebraicos de* $K\mathbb{P}^2$ *son las uniones finitas de los siguientes tipos de conjuntos:*

(i) $\varnothing, K\mathbb{P}^2$.

(ii) $\{p\}$ *donde* $p \in K\mathbb{P}^2$.

(iii) $\mathcal{Z}(F)$ *donde* $F \in K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ *es un polinomio homogéneo irreducible (curva algebraica proyectiva irreducible).*

Si K es un cuerpo algebraicamente cerrado, tenemos el siguiente resultado.

Corolario I.4.9 *Sean* $f \in K[\mathtt{x}_1, \mathtt{x}_2]$ *un polinomio no nulo,* $u \in K \setminus \{0\}$ *y* $f_1, \ldots, f_r \in K[\mathtt{x}_1, \mathtt{x}_2]$ *polinomios irreducibles no asociados dos a dos tales que* $f = uf_1^{\alpha_1} \cdots f_r^{\alpha_r}$ *para ciertos enteros* $\alpha_i \geq 1$. *Entonces* $\mathcal{J}(\mathcal{Z}(f)) = f_1 \cdots f_r K[\mathtt{x}_1, \mathtt{x}_2]$.

Demostración. En primer lugar se cumple por el Lema I.2.4 que

$$\mathcal{J}(\mathcal{Z}(f)) = \mathcal{J}(\mathcal{Z}(f_1^{\alpha_1} \cdots f_r^{\alpha_r})) = \mathcal{J}\Big(\bigcup_{i=1}^{r} \mathcal{Z}(f_i^{\alpha_i})\Big) = \bigcap_{i=1}^{r} \mathcal{J}(\mathcal{Z}(f_i)).$$

Como f_i es un polinomio irreducible, $f_i K[\mathtt{x}_1, \mathtt{x}_2]$ es un ideal primo y por el Nullstellensatz de Hilbert I.3.4 se cumple que $\mathcal{J}(\mathcal{Z}(f_i)) = f_i K[\mathtt{x}_1, \mathtt{x}_2]$. De esta forma,

$$\mathcal{J}(\mathcal{Z}(f)) = \bigcap_{i=1}^{r} f_i K[\mathtt{x}_1, \mathtt{x}_2] = f_1 \cdots f_r K[\mathtt{x}_1, \mathtt{x}_2],$$

con lo que concluye la prueba. □

Por tanto, si X es el lugar de ceros de un polinomio $g \in K[\mathtt{x}_1, \mathtt{x}_2]$ y $f \in K[\mathtt{x}_1, \mathtt{x}_2]$ es un polinomio de grado minimal tal que $\mathcal{Z}(f) = X$, entonces por el resultado anterior $\mathcal{J}(X) = fK[\mathtt{x}_1, \mathtt{x}_2]$. En el caso proyectivo tenemos el siguiente resultado análogo:

Corolario I.4.10 *Sean* $F \in K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ *un polinomio homogéneo no nulo,* $u \in K \setminus \{0\}$ *y* $F_1, \ldots, F_r \in K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ *polinomios homogéneos irreducibles no asociados dos a dos tales que* $F = uF_1^{\alpha_1} \cdots F_r^{\alpha_r}$ *para ciertos enteros* $\alpha_i \geq 1$. *Entonces* $\mathcal{J}(\mathcal{Z}(F)) = F_1 \cdots F_r K[\mathtt{x}_1, \mathtt{x}_2]$.

Demostración. En primer lugar se cumple por el Lema I.2.4 que

$$\mathcal{J}(\mathcal{Z}(F)) = \mathcal{J}(\mathcal{Z}(F_1^{\alpha_1} \cdots F_r^{\alpha_r})) = \mathcal{J}\Big(\bigcup_{i=1}^{r} \mathcal{Z}(F_i^{\alpha_i})\Big) = \bigcap_{i=1}^{r} \mathcal{J}(\mathcal{Z}(F_i)).$$

Como F_i es un polinomio irreducible, $F_iK[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ es un ideal primo. Por el Corolario I.3.7 se cumple $\mathcal{J}(\mathcal{Z}(F_i)) = F_iK[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$. De esta forma,

$$\mathcal{J}(\mathcal{Z}(F)) = \bigcap_{i=1}^{r} F_iK[\mathtt{x}_1, \mathtt{x}_2] = F_1 \cdots F_rK[\mathtt{x}_1, \mathtt{x}_2],$$

con lo que concluye la prueba. □

Por tanto, si X es el lugar de ceros de un polinomio homogéneo no nulo $G \in K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ y $F \in K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ es un polinomio homogéneo de grado minimal tal que $\mathcal{Z}(F) = X$, entonces por el resultado anterior $\mathcal{J}(X) = FK[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$.

4.c. Polinomios irreducibles. Criterios de irreducibilidad. A la vista de los Corolarios I.4.7 y I.4.8 para determinar cuales son todos los subconjuntos algebraicos de K^2 y $K\mathbb{P}^2$ es importante conocer como son las curvas algebraicas irreducibles, que son las clases de equivalencia módulo proporcionalidad de un polinomio irreducible de $K[\mathtt{x}_1, \mathtt{x}_2]$ o de un polinomio homogéneo irreducible de $K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$. Como un polinomio homogéneo de $K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ no divisible entre las variables $\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2$ es irreducible si y solo si su deshomogeneizado con respecto a cualquiera de sus variables es irreducible, nos centraremos en recordar algunos criterios de irreducibilidad para el anillo $K[\mathtt{x}_1, \mathtt{x}_2]$. Dichos criterios nos permitirán en muchos ejemplos garantizar la irreducibilidad de los polinomios involucrados. La mayoría de estos criterios los incluimos sin demostración, que puede ser realizada por el lector o puede encontrarla en [FG2].

Lema I.4.11 (Criterio de la traslación) *Sean $f \in K[\mathtt{x}_1, \mathtt{x}_2]$ y $h \in K[\mathtt{x}_1]$. Entonces f es irreducible si y solo si el polinomio $f(\mathtt{x}_1, \mathtt{x}_2 + h(\mathtt{x}_1)) \in K[\mathtt{x}_1, \mathtt{x}_2]$ es irreducible.*

Lema I.4.12 (Criterio de Eisenstein) *Sea*

$$f := \sum_{k=0}^{d} a_k(\mathtt{x}_1)\mathtt{x}_2^k \in K[\mathtt{x}_1][\mathtt{x}_2]$$

un polinomio de grado d con respecto a $\mathtt{x}_2$ y tal que $\mathrm{m.c.d.}(a_0, \ldots, a_d) = 1$. *Supongamos que existe un polinomio irreducible $p \in K[\mathtt{x}_1]$ tal que p divide a a_k para $k = 0, \ldots, d-1$, p no divide a a_d y p^2 no divide a a_0. Entonces f es irreducible.*

Lema I.4.13 (Criterio de Netto) *Sea* $f := \sum_{k=0}^{2m+1} a_k(\mathtt{x}_1)\mathtt{x}_2^k \in K[\mathtt{x}_1][\mathtt{x}_2]$ *un polinomio de grado impar* $2m+1$ *con respecto a* $\mathtt{x}_2$ *y tal que*

$$\text{m.c.d.}(a_0, \ldots, a_{2m+1}) = 1.$$

Supongamos que existe un polinomio irreducible $p \in K[\mathtt{x}_1]$ *tal que* p^2 *divide a* a_k *para* $k = 0, \ldots, m$, p *divide a* a_k *para* $k = m+1, \ldots, 2m$, p *no divide a* a_{2m+1} *y* p^3 *no divide a* a_0. *Entonces* f *es irreducible.*

Lema I.4.14 (Criterio de Gibson) *Sea* $f \in K[\mathtt{x}_1, \mathtt{x}_2]$ *tal que* $f = f_{d-1} + f_d$ *donde cada* $f_k \in K[\mathtt{x}_1, \mathtt{x}_2]$ *es un polinomio homogéneo no nulo de grado* k *y los polinomios* f_{d-1} *y* f_d *son primos entre sí. Entonces* f *es irreducible.*

Demostración. Supongamos que f es reducible y sean $g, h \in K[\mathtt{x}_1, \mathtt{x}_2]$ dos polinomios de grado ≥ 1 tales que $f = gh$. Escribimos g, h como la suma de sus componentes homogéneas, es decir, $g = \sum_{k=0}^{r} g_k$ y $h = \sum_{\ell=0}^{s} h_\ell$. Tenemos que $r + s = d$ y

$$f = \sum_{m=0}^{r+s} \sum_{k+\ell=m} g_k h_\ell$$

es la descomposición de f como suma de sus componentes homogéneas. Por tanto

$$f_m = \sum_{k+\ell=m} g_k h_\ell = 0$$

para $m = 0, \ldots, r+s-2$. Veamos que: $g_k = 0$ *para* $k = 0, \ldots, r-2$ *y* $h_\ell = 0$ *para* $\ell = 0, \ldots, s-2$.

Sea k_0 el primer índice tal que g_k no es cero y ℓ_0 el primer índice tal que h_ℓ no es cero. Veamos que $k_0 \geq r-1$ y $\ell_0 \geq s-1$. Supongamos que $k_0 \leq r-2$. Entones $k_0 + \ell_0 \leq s + r - 2$ y por tanto

$$0 = f_{k_0+\ell_0} = \sum_{k+\ell=k_0+\ell_0} g_k h_\ell = g_{k_0} h_{\ell_0} + \sum_{0 \leq k < k_0} g_k h_{k_0-k+\ell_0} + \sum_{0 \leq \ell < \ell_0} g_{k_0+\ell_0-\ell} h_\ell$$

con lo que $g_{k_0} h_{\ell_0} = 0$, lo que contradice el hecho de que g_{k_0} y h_{ℓ_0} son no nulos. Por tanto $k_0 \geq r-1$ y de forma análoga $\ell_0 \geq s-1$.

De esta forma, $g = g_{r-1} + g_r$ y $h = h_{s-1} + h_s$ y por tanto $g_{r-1}h_{s-1} = 0$. Podemos suponer que $h_{s-1} = 0$ y entonces $f = g_{r-1}h_s + g_r h_s$, lo que implica que h_s es un factor común de f_{d-1} y f_d, contra nuestras hipótesis. Por tanto, f es irreducible. □

Ejercicios y problemas propuestos

Número I.1 Sean K un cuerpo y consideramos los polinomios

$$f(\mathtt{x},\mathtt{y}) := \mathtt{x}\mathtt{y}^4 + \mathtt{x}^3\mathtt{y}^3 + \mathtt{x}^2(\mathtt{y}^3+1) - 1 \quad \text{y} \quad g(\mathtt{x},\mathtt{y}) := \mathtt{x}^5 + \mathtt{y}(\mathtt{x}^4 + \mathtt{x}^3 + \mathtt{y}(\mathtt{y}+1)\mathtt{x} + \mathtt{y}).$$

Demostrar que f y g son irreducibles en $K[\mathtt{x},\mathtt{y}]$.

Número I.2 Encontrar todos los puntos $(x, y) \in \mathbb{C}^2$ tales que

$$\mathtt{y}^2 + \mathtt{x}^2 - \mathtt{y} - 3\mathtt{x} = 0 \quad \text{e} \quad \mathtt{y}^2 - 6\mathtt{x}\mathtt{y} - \mathtt{x}^2 + 11\mathtt{y} + 7\mathtt{x} - 12 = 0.$$

Número I.3 Sea $p := \mathtt{x}^2\mathtt{y} - 3\mathtt{x}\mathtt{y}^2 + \mathtt{x}^2 - 3\mathtt{x}\mathtt{y}$ y $q := \mathtt{y}\mathtt{x}^3 - 4\mathtt{y}^2 - 3\mathtt{y} + \mathtt{x}^3 + 1$. Comprobar que $\mathrm{Res}_{\mathtt{x}}(p, q) \neq 0$ mientras que $\mathrm{Res}_{\mathtt{y}}(p, q) = 0$. ¿Cómo se puede explicar esto?

Número I.4 Sean $F, G \in K[\mathtt{x}_0, \mathtt{x}_1, \mathtt{x}_2]$ polinomios homogéneos. Demostrar que $\mathrm{Res}_{\mathtt{x}_2}(F, G)$ es un polinomio homogéneo de grado $\deg_{\mathtt{x}_2}(F)\deg(G)+\deg(F)\deg_{\mathtt{x}_2}(G)-\deg_{\mathtt{x}_2}(F)\deg_{\mathtt{x}_2}(G)$. Concluir que $\mathrm{Res}_{\mathtt{x}_2}(F, G)$ tiene grado $\deg(F)\deg(G)$ si y solo si $\deg_{\mathtt{x}_2}(F) = \deg(F)$ o $\deg_{\mathtt{x}_2}(G) = \deg(G)$.

Número I.5 Sea $F \in K[\mathtt{x},\mathtt{y}]$ un polinomio homogéneo de grado n con coeficientes en un cuerpo algebraicamente cerrado K. Demostrar que existen $a \in K\backslash\{0\}$, $r \leq n$ puntos distintos $[a_i : b_i] \in K\mathbb{P}^1$ y enteros positivos $m_i \geq 1$ tales que

$$F = a\prod_{i=1}^{r}(a_i\mathtt{y} - b_i\mathtt{x})^{m_i}$$

Se dice que $[a_i : b_i]$ son las raíces de F y m_i es la multiplicidad de $[a_i : b_i]$ como raíz de F.

Número I.6 Descomponer en factores irreducibles el polinomio $\mathtt{x}^4 + \mathtt{y}^4$ en $\mathbb{Q}[\mathtt{x},\mathtt{y}]$, $\mathbb{R}[\mathtt{x},\mathtt{y}]$ y $\mathbb{C}[\mathtt{x},\mathtt{y}]$.

Número I.7 Sean K un cuerpo algebraicamente cerrado y $f := \mathtt{t}^2+a\mathtt{t}+b$ y $g := \mathtt{t}^2+c\mathtt{t}+d$ dos polinomios de $K[\mathtt{t}]$ sin raíces comunes, tales que $a \neq c$. ¿Cuántos puntos $[\alpha : \beta] \in K\mathbb{P}^1$ cumplen que el polinomio $\alpha f + \beta g$ tiene alguna raíz múltiple?

Número I.8 Sea K un cuerpo. Encontrar un ideal $\mathfrak{a}$ de $K[\mathtt{x},\mathtt{y}]$ que cumpla:

(i) $\mathfrak{a}$ es radical, pero no primo.

(ii) $\mathfrak{a}$ es primo, pero no maximal.

(iii) $\mathfrak{a}$ no es principal.

(iv) $\mathfrak{a}$ no es radical.

Número I.9 Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales homogéneos de $K[\mathtt{x}^*]$. Demostrar que los ideales $\mathfrak{a}+\mathfrak{b}$, $\mathfrak{a}\cdot\mathfrak{b}$, $\mathfrak{a}\cap\mathfrak{b}$ y $\sqrt{\mathfrak{a}}$ son homogéneos.

Número I.10 Demostrar que los divisores de un polinomio homogéneo son necesariamente polinomios homogéneos.

Número I.11 (i) Sea K un cuerpo. Demostrar que existe una topología en K^n, llamada *topología de Zariski*, en la que los subconjuntos cerrados son los subconjuntos algebraicos de K^n. Para cada subconjunto S de K^n, ¿Cuál es su adherencia en esta topología?

(ii) Sean $f := \mathtt{x}^2(1-\mathtt{x})+\mathtt{y}^2$ y $S := \{(x,y)\in\mathbb{R}^2 : \ f(x,y)=0,\, x>0\}$. Calcular la adherencia de S en la topología de Zariski de $\mathbb{R}^2$.

Número I.12 (i) Sea K un cuerpo y $f\in K[\mathtt{x}]$ un polinomio. ¿Es cierto que si el conjunto $\mathcal{Z}(f)$ es un subconjunto algebraico irreducible de K^n, entonces f es irreducible?

(ii) ¿Es cierto que si $f\in\mathbb{R}[\mathtt{x}]$ es un polinomio irreducible, $\mathcal{Z}(f)$ es un conjunto algebraico irreducible de $\mathbb{R}^n$?

Número I.13 Probar que el cuerpo K es infinito si y solo si K^n es un conjunto algebraico irreducible para cada $n\geq 1$.

Número I.14 (i) Sea K un cuerpo. Calcular los subconjuntos algebraicos de K.

(ii) ¿Es $\mathbb{Z}$ un subconjunto algebraico de $\mathbb{R}$? ¿Lo es el intervalo $[0,1)$?

Número I.15 (i) Sean K un cuerpo y $f\in K[\mathtt{x}]$ ¿Es cierto que si $\mathcal{Z}(f)$ es irreducible, entonces f es irreducible?

(ii) ¿Es cierto que si $f\in\mathbb{R}[\mathtt{x}]$ es un polinomio irreducible, entonces $\mathcal{Z}(f)$ es un subconjunto irreducible de $\mathbb{R}^n$?

Número I.16 Supongamos que el cuerpo K no es algebraicamente cerrado. Probar que existe un polinomio homogéneo $f\in K[\mathtt{x},\mathtt{y}]$ cuyo único cero en K^2 es el punto $(0,0)$. ¿Es posible conseguir siempre que dicho polinomio sea además irreducible?

Número I.17 Sea $\pi : K^n \to K^{n-1}$, $(\mathtt{x}_1,\ldots,\mathtt{x}_n)\mapsto(\mathtt{x}_1,\ldots,\mathtt{x}_{n-1})$. Probar que π es una aplicación abierta si en K^n y K^{n-1} consideramos la topología de Zariski.

Número I.18 Sean $X,Y\subset K^n$ dos conjuntos algebraicos. ¿Es cierta la igualdad $\mathcal{J}(X\cap Y)=\mathcal{J}(X)+\mathcal{J}(Y)$?

Número I.19 (i) ¿Es el conjunto $X := \{(x,y)\in\mathbb{R}^2 : \ y=\exp(x)\}$ un subconjunto algebraico de $\mathbb{R}^2$?

(ii) ¿Es el conjunto $X := \{(x,y)\in\mathbb{R}^2 : \ y=\sin(x)\}$ un subconjunto algebraico de $\mathbb{R}^2$?

Número I.20 Encontrar un sistema de generadores del radical del ideal generado en $\mathbb{C}[\mathtt{x},\mathtt{y}]$ por los polinomios $f := \mathtt{x} - \mathtt{y}^2$ y $g := (\mathtt{x}-1)^2 - \mathtt{y}^2 - 1$.

Número I.21 Demostrar que la intersección (arbitraria) de ideales primos es un ideal radical.

Número I.22 Sea $\mathfrak{a}$ el ideal generado en $\mathbb{R}[\mathtt{x},\mathtt{y},\mathtt{z}]$ por los polinomios $f := \mathtt{x}^2 - \mathtt{yz}$ y $g := \mathtt{zx} - \mathtt{x}$. ¿Es $\mathfrak{a}$ un ideal radical? ¿Es $\mathfrak{a}$ un ideal primo? Calcular las componentes irreducibles de $X := \mathcal{Z}(\mathfrak{a})$. ¿Es X conexo con respecto a la topología usual? ¿Es X conexo con respecto a la topología de Zariski? Una de las proyecciones de X sobre los planos coordenados no es un conjunto algebraico. Determinar de cuál se trata.

Número I.23 ¿Son algebraicos los conjuntos $S := \{(uv, u^2, v^2) \in \mathbb{C}^3 : \ (u,v) \in \mathbb{C}^2\}$ y $T := \{(uv, uv^2, v^2) \in \mathbb{C}^3 : \ (u,v) \in \mathbb{C}^2\}$? Calcular los ideales de ceros de S y T y sus adherencias en la topología de Zariski de $\mathbb{C}^3$.