MULTIPLICIDADES DE INTERSECCIÓN

TRABAJO DE FIN DE GRADO

CURSO 2019/20

UNIVERSIDAD COMPLUTENSE
MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

DOBLE GRADO EN MATEMÁTICAS-FÍSICA

José Luis López Núñez

Tutor: Enrique Arrondo Esteban

Madrid, 8 de julio de 2020

Abstract:

In this work we present a proof of Bézout's Theorem for plane projective curves making use of the Hilbert polynomial. Firstly, we introduce the algebraic and geometric notions that are necessary for the development of the work, focusing on the description of the properties of homogeneous ideals in a polynomial ring and their link with projective sets. Secondly, we analyze the Hilbert function for finitely generated graded modules over a polynomial ring and we prove its most relevant properties for our purposes, namely: its additivity for exact sequences and the existence of a polynomial, the Hilbert polynomial, that agrees with the Hilbert function for sufficiently large values of the degree. Finally, we introduce the key notions of dimension and degree of a projective set and their description in terms of the Hilbert polynomial, to conclude with the proof of Bézout's Theorem, where we make use of the tools developed throughout the discussion.

Índice general

Introducción **1**

1. Conceptos previos **3**

2. Descomposición primaria de ideales **8**

3. El polinomio de Hilbert **13**

4. El Teorema de Bézout para curvas planas **18**

Bibliografía **23**

Introducción

Uno de los resultados centrales con el que nos encontramos al iniciarnos en el estudio de la teoría de curvas proyectivas planas es el Teorema de Bézout, que nos da las condiciones bajo las cuales dos curvas planas intersecan en una cantidad finita de puntos, además de cuantificar el número de puntos de dicha intersección de acuerdo a su multiplicidad.

Precisamente en la definición correcta de multiplicidad de intersección de dos curvas en un punto es donde se encuentra la principal dificultad a la hora de demostrar el Teorema de Bézout. La aproximación habitual, y que es la que se lleva a cabo en particular en la asignatura de Curvas Algebraicas, consiste en estudiar las denominadas parametrizaciones formales de las curvas en un punto, lo que lleva de manera natural a la introducción de los anillos de series formales, el anillo de series de Puiseux, los conceptos de rama de una curva en un punto y de multiplicidad de intersección ramas, etc.

Esta aproximación resulta satisfactoria dentro del marco de la teoría de curvas planas, por ser esencialmente autocontenida, al requerir de pocos conocimientos previos sobre álgebra conmutativa. No obstante, y debido precisamente a esto último, cuando se estudia el Teorema de Bézout desde la perspectiva descrita en el párrafo se anterior se pasa por alto la estrecha relación existente entre la geometría y el álgebra, así como la potencia de las herramientas de esta última en su aplicación a la geometría.

El objetivo de este trabajo es presentar una aproximación alternativa a la definición de multiplicidad de intersección de dos curvas en un punto y a la demostración del Teorema de Bézout para curvas planas desde el punto de vista del álgebra conmutativa, haciendo uso, en particular, del polinomio de Hilbert.

Para ello, en primer lugar se revisan algunos resultados conocidos sobre ideales en anillos de polinomios, a saber: el Teorema de los ceros de Hilbert, el concepto de irreducibilidad de un ideal, el Teorema de descomposición primaria de ideales, etc., todo ello adaptado a la clase de ideales relevantes en geometría proyectiva: los ideales homogéneos. Veremos que si bien existe un paralelismo entre las propiedades de los ideales y las de los ideales homogéneos, estos últimos presentan algunas particularidades que los hacen merecedores de un estudio propio.

Una vez hecha esta discusión estaremos en disposición de introducir la función de Hilbert para módulos graduados finitamente generados y de enunciar y demostrar sus principales propiedades, entre las que destaca el hecho de que dicha función de Hilbert venga descrita, esencialmente, por un polinomio, que llamaremos polinomio de Hilbert.

Finalmente, se acometerá la tarea de definir la multiplicidad de intersección de dos curvas en un punto y de demostrar el Teorema de Bézout. Veremos aquí que ciertos conceptos geométricos, como la dimensión y el grado, admiten definiciones muy sencillas en términos del polinomio del Hilbert.

El tratamiento de todos los conceptos y resultados enumerados en los párrafos anteriores se llevará a cabo de la manera más general posible, trabajando en espacios proyectivos de dimensión arbitraria y con conjuntos proyectivos más generales que las curvas planas, si bien haremos referencia a estas continuamente dado que son nuestro objeto de estudio principal. Hacia el final de la discusión, cuando demostremos el Teorema de Bézout, particularizaremos todo lo desarrollado al caso de curvas en el plano proyectivo. Se pretende con esto ilustrar además la naturalidad con que el lenguaje del álgebra conmutativa permite generalizar la geometría en el plano a dimensiones superiores.

La elaboración de este trabajo ha consistido, fundamentalmente, en una tarea de investigación bibliográfica. Nuestra exposición sigue la que se lleva a cabo en [1], que se ha tomado como referencia principal y es de donde se han extraído la mayor parte de las definiciones y resultados. Por otro lado, [2] ha servido como fuente para algunos resultados de carácter puramente algebraico, como es el caso del Teorema de descomposición primaria de ideales. Finalmente, de las referencias [3, 4] se ha seguido la exposición acerca de la función y el polinomio de Hilbert para módulos graduados finitamente generados.

A esta tarea de recopilación de información bibliográfica se ha sumado la elaboración de las demostraciones de todos aquellos resultados que encontramos propuestos como ejercicios a lo largo de la bibliografía pero que no obstante hemos necesitado en nuestra exposición. Tal es el caso, por ejemplo, del Teorema de los ceros de Hilbert proyectivo (que encontramos en [4]), de las caracterizaciones de los ideales homogéneos primos y primarios, y de la mayoría de los resultados presentados en el Capítulo 4 (que podemos encontrar en [1]).

Capítulo 1

Conceptos previos

En este primer capítulo se introducen los conceptos algebraicos necesarios para el desarrollo de la exposición, y además se fijarán las notaciones que usaremos a lo largo de la misma.

De ahora en adelante, denotaremos $S = \mathbb{K}[X_0, ..., X_n]$ el anillo de polinomios en $(n+1)$ variables con coeficientes en el cuerpo $\mathbb{K}$, que supondremos algebraicamente cerrado, mientras que A denotará un anillo arbitrario. Por su parte, $\mathbb{P}^n$ representará el espacio proyectivo n-dimensional sobre $\mathbb{K}$.

Definición 1.1. *Se dice que un anillo A es un anillo graduado si, como grupo aditivo, se puede expresar como suma directa $A = \bigoplus_{l \geqslant 0} A_l$, y además la multiplicación en A es compatible con dicha estructura, en el sentido de que $A_k A_l \subseteq A_{k+l}$.*

A los elementos $a \in A_l$ les llamaremos elementos homogéneos de grado l de A, y A_l constituirá la parte homogénea de grado l de A. De la Definición 1.1 se desprende que cualquier $a \in A$ se escribe, de forma única, como $a = a_r + ... + a_d$, con cada $a_l \in A_l$. Dichos elementos a_l se denominan componentes homogéneas de a.

En nuestro caso, la relevancia de esta definición radica en que S adquiere de forma natural una estructura de anillo graduado tomando como parte homogénea de grado l el conjunto de polinomios homogéneos (en el sentido habitual) de grado l junto con el polinomio nulo.

Como sabemos, una clase distinguida de subconjuntos de un anillo son los ideales. De entre estos, en el estudio de la geometría proyectiva tienen especial relevancia los llamados ideales homogéneos, que definimos a continuación. Más abajo veremos una motivación para introducir estos ideales.

Definición 1.2. *Dado un anillo graduado A, un ideal $\mathfrak{a} \subset A$ se dice homogéneo si se puede expresar como $\mathfrak{a} = \bigoplus_{l \geqslant 0} (\mathfrak{a} \cap A_l)$.*

Nótese que lo anterior es equivalente a decir que si $a = a_r + ... + a_d \in \mathfrak{a}$, con $a_i \in A_i$, entonces $a_i \in \mathfrak{a}$ para cada $i = r, ..., d$. Se desprende de esta observación que un ideal $\mathfrak{a} \subset A$ es homogéneo si y solo si está generado por elementos homogéneos.

Conviene hacer ahora un comentario antes de seguir dando definiciones. Sabemos que cuando un polinomio homogéneo $F \in S$ es evaluado en puntos de $\mathbb{P}^n$ solo tiene sentido decir si dicho polinomio se anula o no en un determinado punto. Sin embargo, nos resultará útil extender esta noción a polinomios arbitrarios: diremos que $F \in S$ se anula en $p \in \mathbb{P}^n$ si y solo si cada una de sus componentes homogéneas se anula en dicho punto.

Con esta aclaración podemos ya definir dos conceptos fundamentales.

Definición 1.3. *Decimos que un subconjunto $X \subset \mathbb{P}^n$ es un conjunto proyectivo si existe un conjunto $T \subset S$ de polinomios homogéneos tales que $X = \{p \in \mathbb{P}^n |\ F(p) = 0\ \forall F \in T\}$. Dado un conjunto $T \subset S$ de polinomios homogéneos, llamamos conjunto proyectivo definido por T al conjunto $V(T) := \{p \in \mathbb{P}^n |\ F(p) = 0\ \forall F \in T\}$.*

En el caso en que $T = \{F\}$, con $F \in S$ un polinomio homogéneo de grado positivo, $V(T)$ se denomina hipersuperficie en $\mathbb{P}^n$. En el caso $n = 2$ dicho conjunto se denomina curva proyectiva plana.

Observación. Es importante notar que para cualquier subconjunto $T \subset S$ de polinomios homogéneos, $V(T) = V(\langle T \rangle)$, siendo $\langle T \rangle$ el ideal generado por T en S. En efecto, $V(\langle T \rangle) \subset V(T)$ pues $T \subset \langle T \rangle$. Pero si un punto anula todos los polinomios de T, en particular anula cada polinomio de la forma $H = G_1F_1 + ... + G_sF_s$, con $G_i \in S$ y $F_i \in T$, dándose así el contenido $V(T) \subset V(\langle T \rangle)$. Por tanto, podemos suponer que todo conjunto proyectivo está definido por un ideal, que es además homogéneo por estar generado por elementos homogéneos (que podremos tomar en cantidad finita, al ser S un anillo noetheriano en virtud del Teorema de la base de Hilbert). Notemos además que, en particular, $V(S) = \emptyset$.

Más aún, dado un ideal homogéneo $\mathfrak{a} \subset S$, se cumple $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$, siendo $\sqrt{\mathfrak{a}}$ el radical de $\mathfrak{a}$, que también es un ideal homogéneo. En efecto, sea $a \in \sqrt{\mathfrak{a}}$, cuya descomposición en componentes homogéneas es $a = a_r + ... + a_d$. Por definición, existe un $n \in \mathbb{N}$ tal que $a^n \in \mathfrak{a}$. La componente homogénea de menor grado de a^n es a_r^n, y puesto que $\mathfrak{a}$ es homogéneo, se cumple que $a_r^n \in \mathfrak{a}$, es decir, $a_r \in \sqrt{\mathfrak{a}}$. Entonces, $a' = a - a_r \in \sqrt{\mathfrak{a}}$, y repitiendo el mismo argumento, llegamos a que $a_i \in \sqrt{\mathfrak{a}}$ para cada $i = r, ..., d$, con lo que $\sqrt{\mathfrak{a}}$ es un ideal homogéneo.

A lo largo de la exposición denotaremos por $(F_1, ..., F_r)$ el ideal generado por los polinomios $F_1, ..., F_r$; usaremos además que si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales homogéneos, también lo son los ideales $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{ab}$ y $\mathfrak{a} \cap \mathfrak{b}$, por estar generados por elementos homogéneos, y que en particular, $V(\mathfrak{a} + \mathfrak{b}) = V(\mathfrak{a}) \cap V(\mathfrak{b})$ y $V(\mathfrak{ab}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.

Un concepto en cierto sentido dual a la Definición 1.3 es el siguiente:

Definición 1.4. *Dado un conjunto proyectivo $X \subset \mathbb{P}^n$, definimos el ideal de X como el conjunto $I(X) := \{F \in S |\ F(p) = 0\ \forall p \in X\}$.*

Que efectivamente $I(X)$ es un ideal de S es claro. Pero además, teniendo en cuenta el comentario inmediatamente anterior a la Definición 1.3, vemos que de hecho se trata de un ideal homogéneo, que es además radical. En particular, $I(\emptyset) = S$.

Nos encontramos así con que al tratar de establecer una relación entre conjuntos proyectivos e ideales en un anillo de polinomios, los ideales homogéneos aparecen de manera natural.

Presentamos ahora una definición que adquirirá gran relevancia más adelante.

Definición 1.5. *Dado un conjunto proyectivo $X \subset \mathbb{P}^n$, definimos el anillo graduado de X (también llamado anillo coordenado homogéneo de X) al anillo cociente $S(X) := S/I(X)$.*

Se cumple lo siguiente

Proposición 1.1. *El anillo $S(X)$ tiene estructura de anillo graduado.*

Demostración. Denotando $I_l := I(X) \cap S_l$, tenemos las descomposiciones $S = \bigoplus_{l\geqslant 0} S_l$ e $I(X) = \bigoplus_{l\geqslant 0} I_l$.

Consideremos los grupos cociente S_l/I_l, con $l \geq 0$ y la operación suma heredada de S_l, que está bien definida por ser I_l un subgrupo normal (aditivo) de S_l. Tomemos la aplicación $\varphi : S \longrightarrow \bigoplus_{l\geqslant 0} S_l/I_l$, que a cada $F = F_r + ... + F_d \in S$ le asigna $(F_r + I_r) + ... + (F_d + I_d)$. Podemos dotar a la suma directa de estructura de anillo definiendo la multiplicación de $F = (F_r+I_r)+...+(F_d+I_d)$ y $G = (G_s+I_s)+...+(G_n+I_n)$, como $FG = \sum_{i,j}(F_iG_j+I_{i+j})$. Nótese que está bien definida por cumplirse $S_iS_j \subseteq S_{i+j}$.

Con estas operaciones, $\bigoplus_{l\geqslant 0} S_l/I_l$ adquiere estructura de anillo graduado y φ es un homomorfismo de anillos, claramente sobreyectivo. Además, dado $F = F_r + ... + F_d \in S$, $\varphi(F) = 0 \Leftrightarrow F_i + I_i = 0\ \forall i = r, ..., d \Leftrightarrow F_i \in I(X)\ \forall i = r, ..., d \Leftrightarrow F \in I(X)$, es decir, $\ker(\varphi) = I(X)$.

Por el Primer Teorema de isomorfía de anillos, $S(X) \cong \bigoplus_{l\geqslant 0} S_l/I_l$. □

Observación (1). Notemos que $S_l/(I(X)\cap S_l)$ y $(S_l+I(X))/I(X)$ son isomorfos como grupos, por lo que los elementos homogéneos de grado l de $S(X)$ podrán identificarse con las clases de equivalencia módulo $I(X)$ de elementos homogéneos de S del mismo grado.

Observación (2). El mismo argumento empleado en la demostración prueba que si A es un anillo graduado y $\mathfrak{a} \subset A$ es un ideal homogéneo, el anillo $A/\mathfrak{a}$ tiene estructura de anillo graduado.

En general, el cálculo de $I(X)$ para conjuntos proyectivos arbitrarios es complicado. Sin embargo, en el caso de hipersuperficies es una tarea trivial. Para ello, haremos uso del Teorema de los ceros de Hilbert (Nullstellensatz) en su versión proyectiva. Antes de dar la demostración, presentamos dos lemas previos. Se supondrá conocido el Teorema de los ceros de Hilbert en su versión usual (afín).

Lema 1.1. *Sea $\mathfrak{a} \subset S$ un ideal homogéneo, y sea $F \in S$ un polinomio homogéneo de grado positivo tal que $F(p) = 0$ para cada $p \in V(\mathfrak{a}) \subset \mathbb{P}^n$. Entonces, existe un $r \in \mathbb{N}$ tal que $F^r \in \mathfrak{a}$.*

Demostración. La demostración pasa por considerar el conjunto de los ceros de los polinomios de $\mathfrak{a}$ en el espacio afín $\mathbb{A}^{n+1}$.

En efecto, denotemos por $V_a(\mathfrak{a}) = \{(a_0, ..., a_n) \in \mathbb{A}^{n+1} |\ G(a_0, ..., a_n) = 0\ \forall G \in \mathfrak{a}\}$, y $\Lambda = \{(ta_0, ..., ta_n) |\ t \in \mathbb{K},\ (a_0 : ... : a_n) \in V(\mathfrak{a})\}$. Puesto que el ideal $\mathfrak{a}$ es homogéneo, un punto $(a_0, ..., a_n) \in \mathbb{A}^{n+1}$ cumple $G(a_0, ..., a_n) = 0$ para cada $G \in \mathfrak{a}$ si y solamente si se anulan en dicho punto todos los polinomios homogéneos de $\mathfrak{a}$, lo que a su vez es equivalente a que $G(ta_0, ..., ta_n) = 0$ para cada $t \in \mathbb{K}$ y cada $G \in \mathfrak{a}$, con lo que o bien $(a_0, ..., a_n) = (0, ..., 0)$ o bien alguna componente es no nula y por tanto $(a_0 : ... : a_n) \in \mathbb{P}^n$ está bien definido y además $(a_0 : ... : a_n) \in V(\mathfrak{a})$.

En definitiva, tenemos que $\Lambda = V_a(\mathfrak{a})$. De esta manera, si $F \in S$ es un polinomio homogéneo tal que $F(a_0 : ... : a_n) = 0$ para cada $(a_0 : ... : a_n) \in V(\mathfrak{a})$, se cumplirá que $F(ta_0, ..., ta_n) = 0$ para cada $t \in \mathbb{K}$ y cada $(a_0 : ... : a_n) \in V(\mathfrak{a})$, con lo que en particular $F(p) = 0$ para cualquier $p \in V_a(\mathfrak{a})$. Aplicando el Teorema de los ceros de Hilbert usual, tenemos que existe un $r \in \mathbb{N}$ tal que $F^r \in \mathfrak{a}$.

□

Lema 1.2. *Sea $\mathfrak{a} \subset S$ un ideal homogéneo, y consideremos el conjunto $V(\mathfrak{a}) \subset \mathbb{P}^n$. Entonces son equivalentes*

1. $V(\mathfrak{a}) = \emptyset$.
2. $\sqrt{\mathfrak{a}} = S$ *o bien* $\sqrt{\mathfrak{a}} = \mathfrak{M}$, *con* $\mathfrak{M} := \bigoplus_{l>0} S_l = (X_0, ..., X_n)$ *(que es un ideal homogéneo).*
3. $S_l \subset \mathfrak{a}$ *para algún* $l > 0$.

Demostración. Probamos las implicaciones cíclicamente:

$1 \Rightarrow 2$: si $V(\mathfrak{a}) = \emptyset$, en particular se anulan sobre dicho conjunto los polinomios $X_0, ..., X_n$. Por el Lema 1.1, existe algún $r \in \mathbb{N}$ tal que $X_0^r, ..., X_n^r \in \mathfrak{a}$, es decir, $\mathfrak{M} \subseteq \sqrt{\mathfrak{a}}$. Como $\mathfrak{M}$ es un ideal maximal de S (nótese que $S/\mathfrak{M} \cong \mathbb{K}$, que es un cuerpo), esto solo es posible si $\sqrt{\mathfrak{a}} = \mathfrak{M}$ o $\sqrt{\mathfrak{a}} = S$.

$2 \Rightarrow 3$: en cualquiera de los dos casos, existe un $r \in \mathbb{N}$ tal que $X_0^r, ..., X_n^r \in \mathfrak{a}$. Tomando $l \in \mathbb{N}$ tal que $l \geqslant (n+1)r$ se cumple que $S_l \subset \mathfrak{a}$; en efecto, basta observar que el conjunto $\{X_0^{i_0} \cdot ... \cdot X_n^{i_n} | i_0 + ... + i_n = l\}$ es una base (sobre $\mathbb{K}$) de los polinomios homogéneos de grado l, y que con esta elección de l, alguna indeterminada tiene exponente mayor o igual que r.

$3 \Rightarrow 1$: en este caso, $X_0^l, ..., X_n^l \in \mathfrak{a}$, y la única $(n+1)$-upla que anula todas estas potencias es $(0, ..., 0)$, que no representa ningún punto en el espacio proyectivo, con lo que $V(\mathfrak{a}) = \emptyset$. □

Por razones que se verán más adelante, a todos aquellos ideales $\mathfrak{a}$ tales que $\sqrt{\mathfrak{a}} = \mathfrak{M}$ les llamaremos ideales $\mathfrak{M}$-primarios.

Teorema 1.1 (de los ceros de Hilbert proyectivo)**.** *Si* $\mathfrak{a} \subset S$ *es un ideal homogéneo que no sea* $\mathfrak{M}$*-primario, entonces* $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

Demostración. En primer lugar notemos que, por definición, siempre se cumple que $\sqrt{\mathfrak{a}} \subset I(V(\mathfrak{a}))$. Veamos pues que $I(V(\mathfrak{a})) \subset \sqrt{\mathfrak{a}}$.

Si $V(\mathfrak{a}) = \emptyset$, por el Lema 1.2 se tiene que $\sqrt{\mathfrak{a}} = S$, con lo que $I(V(\mathfrak{a})) = I(\emptyset) = S = \sqrt{\mathfrak{a}}$.

Supongamos pues que $V(\mathfrak{a}) \neq \emptyset$. Si $F \in S$ es un polinomio homogéneo de grado positivo tal que $F \in I(V(\mathfrak{a}))$, por el Lema 1.1 existe algún $r \in \mathbb{N}$ tal que $F^r \in \mathfrak{a}$, es decir, $F \in \sqrt{\mathfrak{a}}$, con lo que $I(V(\mathfrak{a})) \subset \sqrt{\mathfrak{a}}$. □

Vemos así que el Teorema 1.1 nos da una biyección entre conjuntos proyectivos e ideales homogéneos radicales distintos de $\mathfrak{M}$. Dado que este último no interviene en dicha correspondencia, suele dársele el nombre de *ideal irrelevante*. La razón de tener que excluirle es que, como se vio en el Lema 1.2, en el caso proyectivo podemos obtener el conjunto vacío de dos formas distintas, a diferencia de lo que ocurre en el caso afín.

Como ya adelantamos, el Teorema 1.1 nos permite además calcular el ideal de una hipersuperficie de manera sencilla.

Corolario 1.1. *Sea* $X \subset \mathbb{P}^n$ *una hipersuperficie proyectiva descrita como* $X = V(F)$*, con* $F \in S$ *un polinomio homogéneo de grado positivo. Si la descomposición de* F *en factores irreducibles es* $F = F_1^{s_1} \cdot ... \cdot F_m^{s_m}$*, entonces* $I(X) = (F')$*, con* $F' = F_1 \cdot ... \cdot F_m$.

Demostración. Como F tiene grado positivo, en particular $V(F) \neq \emptyset$, y en virtud del Lema 1.2 el ideal (F) no es $\mathfrak{M}$-primario, luego estamos en las condiciones del Teorema 1.1 y por tanto $I(X) = \sqrt{(F)}$.

Por otro lado, $G \in \sqrt{(F)} \Leftrightarrow$ existe $r \in \mathbb{N}$ tal que $F | G^r \Leftrightarrow F' | G \Leftrightarrow G \in (F')$. Por lo tanto, $I(X) = \sqrt{(F)} = (F')$. □

Observación. En el caso de curvas en $\mathbb{P}^2$, el polinomio F' del Corolario 1.1 es lo que suele denominarse *ecuación minimal* de la curva. Acabamos de probar por tanto que dicha ecuación minimal siempre existe y que es única salvo multiplicación por una constante no nula. Más adelante haremos uso explícito de que el ideal de una curva plana es principal.

Capítulo 2

Descomposición primaria de ideales

Una consecuencia importante del Corolario 1.1 es la siguiente.

Dada una curva proyectiva $C \subset \mathbb{P}^2$ descrita por una ecuación minimal $F = F_1 \cdot ... \cdot F_m$, con los F_i polinomios homogéneos irreducibles distintos, se cumple que $C = C_1 \cup ... \cup C_m$, con $C_i = V(F_i)$. Además, dada la irreducibilidad de los polinomios F_i, tenemos que $I(C) = (F) = (F_1) \cap ... \cap (F_m) = I(C_1) \cap ... \cap I(C_m)$.

Las curvas C_i se denominan *componentes irreducibles* de C. Este nombre viene motivado por lo siguiente.

Definición 2.1. *Un conjunto proyectivo $X \subset \mathbb{P}^n$ se dice que es irreducible si dados dos conjuntos proyectivos $Y_1, Y_2 \subset \mathbb{P}^n$ tales que $X \subset Y_1 \cup Y_2$, se cumple que $X \subset Y_1$ o bien $X \subset Y_2$.*

Es posible caracterizar los conjuntos proyectivos irreducibles en términos de su ideal. Antes de dar dicha caracterización necesitamos enunciar una propiedad de los ideales homogéneos.

Lema 2.1. *Un ideal homogéneo $\mathfrak{a}$ de un anillo graduado A es primo si y solo si para cualesquiera elementos homogéneos $a, b \in A$ tales que $ab \in \mathfrak{a}$, se cumple que $a \in \mathfrak{a}$ o $b \in \mathfrak{a}$.*

Demostración. La condición necesaria es consecuencia de la propia definición de ideal primo, así que probamos solo la condición suficiente.

Sean $a, b \in A$, cuya descomposición en componentes homogéneas es $a = a_0 + ... + a_d$ y $b = b_0 + ... + b_e$, tales que $ab \in \mathfrak{a}$, y supongamos que ninguno de ellos pertece a $\mathfrak{a}$. Puesto que $\mathfrak{a}$ es homogéneo, esto implica que existe alguna componente homogénea de a, digamos a_r, y alguna de b, digamos b_l, tales que $a_r, b_l \notin \mathfrak{a}$. Tomemos a_r y b_l como las componentes de homogéneas de a y b, respectivamente, con grado mínimo entre las que cumplen esta propiedad. Es claro entonces que $ab = (a_0 + ... + a_d)(b_0 + ... + b_e) \in \mathfrak{a} \Leftrightarrow (a_r + ... + a_d)(b_l + ... + b_e) \in \mathfrak{a}$. Ahora bien, la componente homogénea de menor grado de $(a_r + ... + a_d)(b_l + ... + b_e)$ es $a_r b_l$, con lo cual $a_r b_l \in \mathfrak{a}$. Pero la hipótesis sobre $\mathfrak{a}$ implica que bien $a_r \in \mathfrak{a}$ o bien $b_l \in \mathfrak{a}$, lo que contradice la elección de a_r y b_l. En consecuencia, o bien $a \in \mathfrak{a}$ o bien $b \in \mathfrak{a}$, con lo que $\mathfrak{a}$ es primo. □

Ya podemos demostrar la siguiente proposición.

Proposición 2.1. *Un conjunto proyectivo $X \subset \mathbb{P}^n$ es irreducible si y solo si $I(X)$ es un ideal primo.*

Demostración. $\Rightarrow$: Sea X irreducible, y sean $F, G \in S$ polinomios homogéneos tales que $FG \in I(X)$. Entonces, $(FG) \subset I(X)$, lo que implica que $X \subset V(FG) = V(F) \cup V(G)$. Por la irreducibilidad de X, o bien $X \subset V(F)$, con lo que $F \in I(X)$; o bien $X \subset V(G)$ y $G \in I(X)$. Por tanto, $I(X)$ es un ideal primo.

$\Leftarrow$: sean Y_1, Y_2 conjuntos proyectivos tales que $X \subset Y_1 \cup Y_2$. Entonces, $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2) \subset I(X)$, y dado que el ideal $I(X)$ es primo, alguno de los ideales, digamos $I(Y_1)$, verifica que $I(Y_1) \subset I(X)$, con lo que $X \subset Y_1$. Por tanto, X es irreducible. □

Es claro ahora por qué llamábamos a las curvas C_i descritas más arriba *componentes irreducibles de* C: puesto que $I(C_i) = (F_i)$, y F_i es un polinomio irreducible, en virtud de la Proposición 2.1 dichas curvas son conjuntos proyectivos irreducibles en el sentido de la Definición 2.1.

En realidad esta descomposición en conjuntos irreducibles no es exclusiva de las curvas proyectivas planas. Para probarlo con toda generalidad necesitamos introducir primero la *descomposición primaria* de ideales homogéneos. Además, esta herramienta nos permitirá demostrar resultados importantes en secciones posteriores.

Definición 2.2. *Un ideal $\mathfrak{a} \subset A$ se dice primario si para cualesquiera $a, b \in A$ tales que $ab \in \mathfrak{a}$, o bien $a \in \mathfrak{a}$ o bien $b \in \sqrt{\mathfrak{a}}$. Si denotamos $\mathfrak{p} = \sqrt{\mathfrak{a}}$, diremos que $\mathfrak{a}$ es $\mathfrak{p}$-primario.*

Observación (1). Si $\mathfrak{a}$ es primario, el ideal $\mathfrak{p} = \sqrt{\mathfrak{a}}$ es primo. En efecto, si $a, b \in A$ cumplen $ab \in \mathfrak{p}$, entonces existe un $m \in \mathbb{N}$ tal que $a^m b^m \in \mathfrak{a}$, con lo que o bien $a^m \in \mathfrak{a}$ o bien $b^m \in \mathfrak{p}$; pero entonces, por definición, o bien $a \in \mathfrak{p}$ o bien $b \in \mathfrak{p}$, con lo que $\mathfrak{p}$ es un ideal primo.

Observación (2). Que $\mathfrak{p} = \sqrt{\mathfrak{a}}$ sea primo no implica necesariamente que $\mathfrak{a}$ sea primario. Sin embargo, si $\mathfrak{p}$ es maximal (y en particular, primo), entonces sí puede afirmarse que $\mathfrak{a}$ sea primario. En efecto, sean $a, b \in A$ tales que $ab \in \mathfrak{a}$, y supongamos que $b \notin \mathfrak{p}$. Por la maximalidad de $\mathfrak{p}$ se sigue que $A = \mathfrak{p} + (b)$, luego en particular $1 = c + bd$, con $c \in \mathfrak{p}$ y $d \in A$. Sea $m \in \mathbb{N}$ tal que $c^m \in \mathfrak{a}$, y tomemos $1 = c^m + bd'$, para cierto $d' \in A$. Entonces $a = a \cdot 1 = a(c^m + bd') = ac^m + (ab)d' \in \mathfrak{a}$, con lo que $\mathfrak{a}$ es primario. Esto explica que a aquellos ideales cuyo radical es $\mathfrak{M}$ los llamásemos ideales $\mathfrak{M}$-primarios, por serlo en el sentido de la Definición 2.2

Observación (3). Al igual que ocurre con los ideales primos, los ideales homogéneos son primarios si y solamente si cumplen la condición de la Definición 2.2 para elementos homogéneos. De nuevo, la condición necesaria es consecuencia de la definición, así que veamos la condición suficiente. Sean $a, b \in A$, con $a = a_r + ... + a_d$ y $b = b_l + ... + b_e$, tales que $ab \in \mathfrak{a}$, y supongamos que $a \notin \mathfrak{a}$. Veamos que $b \in \sqrt{\mathfrak{a}}$. Sea a_s la componente homogénea de menor grado de A tal que $a_s \notin \mathfrak{a}$. Entonces, $ab \in \mathfrak{a}$ si y solo si $(a_s + ... + a_d)(b_l + ... + b_e) \in \mathfrak{a}$. La componente homogénea de menor grado de $(a_s + ... + a_d)(b_l + ... + b_e)$ es $a_s b_l$, y puesto que $a_s b_l \in \mathfrak{a}$ y $a_s \notin \mathfrak{a}$, entonces $b_l \in \sqrt{\mathfrak{a}}$. En particular, el conjunto $\{m \in \mathbb{N} \mid ab_l^m \in \mathfrak{a}\}$ es no vacío, así que tendrá un elemento mínimo $n \geq 1$. Tomemos $a' = ab_l^{n-1} \notin \mathfrak{a}$. Por la elección de n, tenemos que $a'b \in \mathfrak{a}$, lo cual implica que $a'(b_{l+1} + ... + b_e) \in \mathfrak{a}$. Aplicando entonces el mismo argumento al resto de componentes homogéneas de b concluimos que $b_i \in \sqrt{\mathfrak{a}}$ para cada $i = l, ..., e$, es decir, $b \in \sqrt{\mathfrak{a}}$, con lo que efectivamente $\mathfrak{a}$ es primario.

Observación (4). Si $\mathfrak{a} = \bigcap_{i=1}^r \mathfrak{b}_i$, con los ideales $\mathfrak{b}_i$ $\mathfrak{p}$-primarios, entonces $\mathfrak{a}$ es $\mathfrak{p}$-primario. En efecto, por un lado tenemos que $\sqrt{\mathfrak{a}} = \sqrt{\bigcap_{i=1}^r \mathfrak{b}_i} = \bigcap_{i=1}^r \sqrt{\mathfrak{b}_i} = \mathfrak{p}$. Por otro lado, dados $a, b \in A$ tales que $ab \in \mathfrak{a}$, si $a \notin \mathfrak{a}$ entonces existe algún i tal que $a \notin \mathfrak{b}_i$. Pero entonces $b \in \sqrt{\mathfrak{b}_i} = \mathfrak{p}$ por ser $\mathfrak{b}_i$ un ideal primario, con lo que $b \in \sqrt{\mathfrak{a}}$ y por tanto $\mathfrak{a}$ es $\mathfrak{p}$-primario.

Probaremos a continuación el Teorema de descomposición primaria de ideales homogéneos. Necesitamos antes dos lemas previos.

Definición 2.3. *Un ideal homogéneo $\mathfrak{a} \subset S$ se dice que es irreducible si no puede expresarse como intersección no trivial de ideales homogéneos; es decir, si existen ideales homogéneos $\mathfrak{b}, \mathfrak{c} \subset S$ tales que $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, entonces o bien $\mathfrak{a} = \mathfrak{b}$ o bien $\mathfrak{a} = \mathfrak{c}$.*

Lema 2.2. *Todo ideal homogéneo de S se puede expresar como intersección finita de ideales homogéneos irreducibles.*

Demostración. Sea $\mathfrak{a} \subset S$ un ideal homogéneo, y supongamos que no es intersección finita de ideales homogéneos irreducibles. En particular, el propio $\mathfrak{a}$ no es irreducible, luego existen $\mathfrak{b}_1, \mathfrak{c}_1 \subset S$ ideales homogéneos tales que $\mathfrak{a} = \mathfrak{b}_1 \cap \mathfrak{c}_1$, con $\mathfrak{a} \subsetneq \mathfrak{b}_1$ y $\mathfrak{a} \subsetneq \mathfrak{c}_1$. Por la hipótesis sobre $\mathfrak{a}$, alguno de estos, digamos $\mathfrak{b}_1$, no es intersección finita de ideales homogéneos irreducibles. Aplicando a este el mismo argumento que a $\mathfrak{a}$, encontramos otro ideal homogéneo $\mathfrak{b}_2$ que no es intersección finita de ideales homogéneos irreducibles y tal que $\mathfrak{b}_1 \subsetneq \mathfrak{b}_2$. Procediendo inductivamente se construye una cadena ascendente de ideales tales que $\mathfrak{a} \subsetneq \mathfrak{b}_1 \subsetneq \mathfrak{b}_2 \subsetneq ...$, lo que contradice que S sea noetheriano. □

Lema 2.3. *Si $\mathfrak{a} \subset S$ es un ideal homogéneo irreducible entonces es primario.*

Demostración. Sean $F, G \in S$ polinomios homogéneos tales que $FG \in \mathfrak{a}$, y consideremos los ideales homogéneos $\mathfrak{b}_n = \{H \in S \mid HG^n \in \mathfrak{a}\}$. Para estos ideales, tenemos la cadena $\mathfrak{a} \subset \mathfrak{b}_1 \subset \mathfrak{b}_2 \subset ....$ Como S es noetheriano, la cadena estaciona, luego existe un $n \in \mathbb{N}$ tal que $\mathfrak{b}_n = \mathfrak{b}_m$ si $m \geq n$. Veamos que $\mathfrak{a} = \mathfrak{b}_1 \cap (\mathfrak{a} + (G^n))$. Que $\mathfrak{a} \subset \mathfrak{b}_1 \cap (\mathfrak{a} + (G^n))$ es claro. Para probar el otro contenido tomemos $H \in \mathfrak{b}_1 \cap (\mathfrak{a} + (G^n))$, con lo que $H = H_1 + H_2 G^n$ para ciertos $H_1 \in \mathfrak{a}$ y $H_2 \in S$. Como $H \in \mathfrak{b}_1$, tenemos que $HG = H_1 G + H_2 G^{n+1} \in \mathfrak{a}$. Pero $H_1 G \in \mathfrak{a}$, con lo que $H_2 G^{n+1} \in \mathfrak{a}$; es decir, $H_2 \in \mathfrak{b}_{n+1} = \mathfrak{b}_n$. Esto significa que $H_2 G^n \in \mathfrak{a}$, con lo que $H \in \mathfrak{a}$.

Ahora, como $\mathfrak{a}$ es irreducible, o bien se cumple $\mathfrak{a} = \mathfrak{b}_1$, y en particular $F \in \mathfrak{a}$, o bien $\mathfrak{a} = \mathfrak{a} + (G^n)$, con lo que $G \in \sqrt{\mathfrak{a}}$. Por lo tanto, $\mathfrak{a}$ es primario. □

Teorema 2.1 (de descomposición primaria)**.** *Dado un ideal homogéneo $\mathfrak{a} \subset S$, este puede escribirse como $\mathfrak{a} = \mathfrak{b}_1 \cap ... \cap \mathfrak{b}_r$, donde cada $\mathfrak{b}_i$ es un ideal homogéneo primario. Además, dicha descomposición puede tomarse de forma que los radicales $\sqrt{\mathfrak{b}_i}$ sean todos distintos y $\bigcap_{i \neq j} \mathfrak{b}_j \not\subset \mathfrak{b}_i$ para cada $i = 1, ..., r$. Más aún, los ideales $\mathfrak{b}_i$ cuyo radical sea minimal (bajo la relación de orden dada por la inclusión) en la familia $\{\sqrt{\mathfrak{b}_1}, ..., \sqrt{\mathfrak{b}_r}\}$ aparecen en cualquier descomposición como la descrita en este enunciado.*

Demostración. Por los Lemas 2.2 y 2.3, podemos escribir $\mathfrak{a}$ como intersección finita de ideales homogéneos primarios, $\mathfrak{a} = \mathfrak{b}_1 \cap ... \cap \mathfrak{b}_r$. Eliminando ideales redundantes en esta intersección si es necesario, podemos suponer que se cumple $\bigcap_{i \neq j} \mathfrak{b}_j \not\subset \mathfrak{b}_i$. Además, por la Observación 4 que hicimos tras la Definición 2.2, podemos suponer que los radicales $\sqrt{\mathfrak{b}_i}$ son todos distintos, sin más que agrupar en la intersección aquellos ideales con el mismo radical.

Probemos ahora la segunda parte; sean $\mathfrak{a} = \mathfrak{b}_1 \cap ... \cap \mathfrak{b}_r = \mathfrak{c}_1 \cap ... \cap \mathfrak{c}_s$ dos descomposiciones de $\mathfrak{a}$ en las condiciones del enunciado. Sea $\mathfrak{b}_i$ un ideal cuyo radical es minimal en $\{\sqrt{\mathfrak{b}_1}, ..., \sqrt{\mathfrak{b}_r}\}$. Dado que $\sqrt{\mathfrak{b}_i}$ es primo y los ideales $\sqrt{\mathfrak{b}_j}$ son distintos, el hecho de ser minimal implica que $\bigcap_{j \neq i} \sqrt{\mathfrak{b}_j} \not\subset \sqrt{\mathfrak{b}_i}$, de forma que podemos encontrar $G \in \bigcap_{j \neq i} \sqrt{\mathfrak{b}_j}$ tal

que $G \notin \sqrt{\mathfrak{b}_i}$. Así, $G \notin \sqrt{\mathfrak{a}}$, luego existe $\mathfrak{c}_j$, cuyo radical podemos suponer minimal en el conjunto $\{\sqrt{\mathfrak{c}_1}, ..., \sqrt{\mathfrak{c}_s}\}$, tal que $G \notin \sqrt{\mathfrak{c}_j}$. Veamos que $\mathfrak{b}_i \subset \mathfrak{c}_j$.

En efecto, sea $F \in \mathfrak{b}_i$ y tomemos G en las condiciones anteriores. Entonces, existe $n \in \mathbb{N}$ tal que $FG^n \in \mathfrak{a}$, con lo que en particular $FG^n \in \mathfrak{c}_j$. Puesto que $G \notin \sqrt{\mathfrak{c}_j}$, necesariamente $F \in \mathfrak{c}_j$, con lo que $\mathfrak{b}_i \subset \mathfrak{c}_j$.

Si ahora aplicamos el mismo argumento al ideal $\mathfrak{c}_j$, encontraremos un $\mathfrak{b}_k$ tal que $\mathfrak{c}_j \subset \mathfrak{b}_k$. Tendremos entonces $\mathfrak{b}_i \subset \mathfrak{c}_j \subset \mathfrak{b}_k$, y dado que $\mathfrak{b}_i \not\subset \mathfrak{b}_k$ si $i \neq k$ por hipótesis, ha de cumplirse que $i = k$, con lo que en particular $\mathfrak{b}_i = \mathfrak{c}_j$. □

La descomposición que acabamos de describir recibe el nombre de *descomposición primaria irredundante* del ideal $\mathfrak{a}$, y los ideales $\mathfrak{b}_i$, *componentes primarias* de $\mathfrak{a}$. Las componentes primarias cuyos radicales no sean minimales en el sentido descrito en el enunciado del Teorema 2.1 se denominan *componentes inmersas* de $\mathfrak{a}$. Los radicales de las componentes primarias en una descomposición irredundante los llamaremos *primos asociados* de $\mathfrak{a}$. Si bien las componentes inmersas presentes en una descomposición primaria irredundante concreta no están unívocamente determinadas por $\mathfrak{a}$, es posible demostrar que los primos asociados de $\mathfrak{a}$ sí son independientes de la descomposición primaria particular. La demostración de este hecho puede consultarse en [2].

Comenzábamos el capítulo mencionando la posibilidad de descomponer una curva proyectiva plana en componentes irreducibles. Podemos probar ahora el carácter general de este hecho como una consecuencia del Teorema 2.1.

Corolario 2.1. *Todo conjunto proyectivo $X \subset \mathbb{P}^n$ se descompone de manera única como unión finita de conjuntos irreducibles, $X = Y_1 \cup ... \cup Y_r$, de forma que $Y_i \not\subset Y_j$ si $i \neq j$.*

Demostración. Tomamos una descomposición primaria del ideal de X, $I(X) = \mathfrak{b}_1 \cap ... \cap \mathfrak{b}_r$. Como $I(X)$ es radical, podemos suponer que los $\mathfrak{b}_i$ son ideales primos, sin más que tomar radicales a ambos lados de la igualdad. Si eliminamos de la intersección aquellos ideales que sean redundantes, podemos además asumir que $\mathfrak{b}_i \not\subset \mathfrak{b}_j$ para cada $i \neq j$, con lo que finalmente obtenemos $V(I(X)) = X = V(\mathfrak{b}_1) \cup ... \cup V(\mathfrak{b}_r) = Y_1 \cup ... \cup Y_r$, con $Y_i \not\subset Y_j$ si $i \neq j$. La irreducibilidad de los conjuntos Y_j se sigue de la Proposición 2.1, teniendo en cuenta que en virtud del Teorema 1.1, $I(Y_j) = \sqrt{\mathfrak{b}_j} = \mathfrak{b}_j$, esta última igualdad por ser $\mathfrak{b}_j$ un ideal primo, luego en particular radical (nótese que como hemos supuesto $\mathfrak{b}_i \not\subset \mathfrak{b}_j$ para cada $i \neq j$, ninguno de estos puede ser el ideal irrelevante $\mathfrak{M}$, luego es aplicable el Teorema 1.1).

La unicidad de la descomposición de X se deduce al notar que los ideales primos que intervienen en la descomposición de $I(X)$ son minimales en el sentido del Teorema 2.1, y por tanto, en virtud de dicho teorema, tal descomposición es única. □

Los conjuntos irreducibles Y_i del enunciado reciben el nombre de *componentes irreducibles* de X. Vemos entonces la interpretación geométrica de las componentes primarias no inmersas de un ideal $\mathfrak{a}$: estas dan lugar a las componentes irreducibles de $V(\mathfrak{a})$. Por su parte, las componentes inmersas de $\mathfrak{a}$ darán lugar a conjuntos proyectivos contenidos estrictamente en alguna de las componentes irreducibles de $V(\mathfrak{a})$.

Para terminar este capítulo sobre descomposición primaria de ideales vamos a introducir una noción que deberemos tener en cuenta más adelante.

Definición 2.4. *Dado un ideal homogéneo $\mathfrak{a} \subset S$, llamaremos componente irrelevante de una descomposición primaria irredundante de $\mathfrak{a}$ a la componente $\mathfrak{M}$-primaria (en caso de que exista) de dicha descomposición.*

Observación. Del Teorema 2.1 se desprende que solo puede existir, a lo sumo, una componente irrelevante en una descomposición primaria como la descrita en dicho teorema, dado que los radicales de las componentes primarias han de ser distintos. El nombre de componente irrelevante deriva del hecho de que si $\mathfrak{b}$ es una tal componente irrelevante, entonces $V(\mathfrak{b}) = \emptyset$. Además, en los capítulos siguientes se verá que para nuestros propósitos podremos obviar la existencia de estas componentes irrelevantes en las descomposiciones primarias de ideales.

Definición 2.5. *Dado un ideal homogéneo $\mathfrak{a} \subset S$, definimos la saturación de $\mathfrak{a}$ como el ideal homogéneo $\bar{\mathfrak{a}} = \{F \in S |\ \exists k \in \mathbb{N},\ X_i^k F \in \mathfrak{a},\ \forall i = 0, ..., n\}$. Diremos que $\mathfrak{a}$ es saturado si coincide con su saturación.*

Proposición 2.2. *Sea $\mathfrak{a} \subset S$ un ideal homogéneo, y $\mathfrak{a} = \mathfrak{b}_0 \cap \mathfrak{b}$ una descomposición primaria irredundante suya, con $\mathfrak{b}_0$ la componente irrelevante y $\mathfrak{b}$ la intersección del resto de componentes primarias. Entonces, $\bar{\mathfrak{a}} = \mathfrak{b}$. Además, para $l \in \mathbb{N}$ lo suficientemente grande, $\mathfrak{a} \cap S_l = \bar{\mathfrak{a}} \cap S_l$.*

Demostración. Sea $F \in \mathfrak{b}$. Como $\sqrt{\mathfrak{b}_0} = \mathfrak{M}$, podemos tomar un $k \in \mathbb{N}$ tal que $X_i^k \in \mathfrak{b}_0$ para cada $i = 0, ..., n$. Pero entonces, $X_i^k F \in \mathfrak{b}_0 \cap \mathfrak{b} = \mathfrak{a}$ para cada $i = 0, ..., n$, con lo que, por definición, $F \in \bar{\mathfrak{a}}$; es decir, $\mathfrak{b} \subset \bar{\mathfrak{a}}$. Recíprocamente, sea $F \in \bar{\mathfrak{a}}$, y escribamos $\mathfrak{b} = \mathfrak{b}_1 \cap ... \cap \mathfrak{b}_r$, con los $\mathfrak{b}_i$ el resto de componentes primarias de la descomposición de $\mathfrak{a}$. Como estas no son irrelevantes, para cada $i = 1, ..., r$ debe existir un $j_i \in \{0, ..., n\}$ tal que $X_{j_i} \notin \sqrt{\mathfrak{b}_i}$. Pero, puesto que $X_{j_i}^k F \in \mathfrak{b}_i$ para cierto $k \in \mathbb{N}$ y $\mathfrak{b}_i$ es un ideal primario, debe cumplirse que $F \in \mathfrak{b}_i$, para cada $i = 1, ..., r$. Esto demuestra que $F \in \mathfrak{b}$, con lo que tenemos $\bar{\mathfrak{a}} \subset \mathfrak{b}$, y en consecuencia, se da la igualdad $\bar{\mathfrak{a}} = \mathfrak{b}$.

Para probar la segunda parte del enunciado, tomemos $\{F_1, ..., F_r\}$ un conjunto de generadores homogéneos de $\bar{\mathfrak{a}}$. Dado que tenemos una cantidad finita de generadores, podemos tomar un $k \in \mathbb{N}$ tal que $X_j^k F_i \in \mathfrak{a}$ para cada $i = 1, ..., r$ y cada $j = 0, ..., n$. Por lo tanto, cualquier polinomio homogéneo $G \in S$ de grado al menos $(n+1)k$ cumple $GF_i \in \mathfrak{a}$ para cada $i = 1, ..., r$. En consecuencia, si tenemos un polinomio homogéneo $H = F_1 G_1 + ... + F_r G_r \in \bar{\mathfrak{a}}$ de grado $l \geq l_0 = (n+1)k + \max\{\deg(F_1), ..., \deg(F_r)\}$, necesariamente $H \in \mathfrak{a}$. Tenemos así el contenido $\bar{\mathfrak{a}} \cap S_l \subset \mathfrak{a} \cap S_l$. para cada $l \geq l_0$. Dado que por definición $\mathfrak{a} \subset \bar{\mathfrak{a}}$, tenemos la igualdad del enunciado. □

En el capítulo siguiente se hará patente que, en ciertos aspectos, los ideales homogéneos saturados tienen mejor comportamiento que los no saturados.

Capítulo 3

El polinomio de Hilbert

En este capítulo presentamos la que será la herramienta fundamental a la hora de demostrar el Teorema de Bézout: el polinomio de Hilbert.

Definición 3.1. *Dado un anillo graduado A, diremos que M es un A-módulo graduado si es un módulo sobre A y admite, como grupo, una descomposición $M = \bigoplus_{l\geq 0} M_l$, de forma que $A_k M_l \subset M_{k+l}$.*

Definición 3.2 (Función de Hilbert)**.** *Dado M un S-módulo graduado finitamente generado, llamamos función de Hilbert de M a la aplicación $h_M : \mathbb{N} \to \mathbb{N}$, $l \mapsto \dim_{\mathbb{K}} M_l$.*

Notemos que la función de Hilbert de un S-módulo graduado finitamente generado está bien definida, en el sentido de que $\dim_{\mathbb{K}} M_l < \infty$. En efecto, tomemos $\{m_1, ..., m_r\}$ un conjunto de generadores (que podemos suponer homogéneos) de M como S-módulo. Sea $d_i = \deg(m_i)$. Entonces, para cualquier $l \in \mathbb{N}$, $M_l = m_1 \cdot S_{l-d_1} + ... + m_r \cdot S_{l-d_r}$ (tomamos $S_i = 0$ si $i < 0$). Puesto que cada S_i es un $\mathbb{K}$-espacio vectorial de dimensión finita, lo mismo le ocurre a M_l.

En la Proposición 1.1 se demostró que dado $\mathfrak{a}$ un ideal homogéneo de S, $S/\mathfrak{a}$ tenía estructura de anillo graduado. No obstante, también podemos ver $S/\mathfrak{a}$ como un S-módulo graduado finitamente generado. En este contexto, y cometiendo un abuso de notación, llamaremos función de Hilbert de $\mathfrak{a}$ a la de $S/\mathfrak{a}$ y la denotaremos por $h_{\mathfrak{a}}$. Cabe destacar que en virtud de la definición de $h_{\mathfrak{a}}$ y de la Proposición 2.2 tenemos que la función de Hilbert de un ideal homogéneo y la de su saturación coinciden para $l \in \mathbb{N}$ lo suficientemente grande.

Por su parte, dado un conjunto proyectivo $X \subset \mathbb{P}^n$, llamaremos función de Hilbert de X a la del ideal $I(X)$.

El resto de la sección la dedicaremos a deducir las propiedades de la función de Hilbert que más adelante usaremos para estudiar las intersecciones de curvas proyectivas planas.

La primera de ellas está relacionada con su comportamiento ante *sucesiones exactas*. Vamos a definir este concepto centrándonos en el caso que a nosotros nos ocupa.

Definición 3.3. *Dados los A-módulos graduados M y N, diremos que un A-homomorfismo $f : M \to N$ es graduado si $f : M_l \to N_l$ para cada $l \in \mathbb{N}$.*

Definición 3.4. *Una sucesión de A-módulos y A-homomorfismos $\cdots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to \cdots$ se dice que es exacta si para cada i, $\mathrm{im}(f_i) = \ker(f_{i+1})$. Si además A es un anillo graduado y los M_i son A-módulos graduados, diremos que la sucesión es exacta graduada si es exacta y además los f_i son A-homomorfismos graduados.*

Podemos ya enunciar y demostrar una propiedad importante:

Proposición 3.1. *Dados M, N y P S-módulos graduados y la sucesión exacta graduada $0 \to M \xrightarrow{\varphi_1} N \xrightarrow{\varphi_2} P \to 0$, se cumple que $h_P(l) = h_N(l) - h_M(l)$ para todo $l \in \mathbb{N}$.*

Demostración. Notemos en primer lugar que los homomorfismos φ_1 y φ_2 definen por restricción aplicaciones $\mathbb{K}$-lineales entre los espacios vectoriales sobre $\mathbb{K}$ correspondientes a las partes homogéneas de los módulos involucrados (identificando $S_0 = \mathbb{K}$).

Teniendo esto en cuenta, basta aplicar la fórmula de las dimensiones conocida del álgebra lineal para espacios vectoriales y aplicaciones lineales, junto con la definición de sucesión exacta. Tenemos así la siguiente cadena de igualdades: $h_P(l) = \dim_{\mathbb{K}} P_l = \dim_{\mathbb{K}}(\mathrm{im}(\varphi_2)) = \dim_{\mathbb{K}} N_l - \dim_{\mathbb{K}}(\ker(\varphi_2)) = h_N(l) - \dim_{\mathbb{K}}(\mathrm{im}(\varphi_1)) = h_N(l) - \dim_{\mathbb{K}} M_l = h_N(l) - h_M(l)$. □

A partir de ahora nos referiremos a lo anterior diciendo que la función de Hilbert es *aditiva* para sucesiones exactas.

Más adelante necesitaremos conocer bajo qué condiciones la intersección de dos curvas planas es un número finito de puntos. La función de Hilbert permite caracterizar esta propiedad:

Proposición 3.2. *Un conjunto proyectivo $X \subset \mathbb{P}^n$ es un conjunto de d puntos si y solamente si $h_{I(X)}(l) = d$ para $l \gg 0$.*

Demostración. $\Rightarrow$: tomemos coordenadas homogéneas de manera que $p_1 = (a_{01} : ... : a_{n1})$,..., $p_d = (a_{0d} : ... : a_{nd})$, y fijemos estos representantes para los puntos. Dado $l \in \mathbb{N}$, sea la aplicación $\varphi_l : S_l \longrightarrow \mathbb{K}^d$ tal que $F \mapsto (F(a_{01}, ..., a_{n1}), ..., F(a_{0d}, ..., a_{nd}))$. Por la definición de $I(X)$, claramente $\ker(\varphi_l) = I(X) \cap S_l$. Veamos la sobreyectividad de φ_l.

Puesto que tenemos una cantidad finita de puntos, podemos encontrar, para cada $i = 1, ..., d$, un polinomio homogéneo de grado 1, H_i, de forma que el hiperplano $V(H_i)$ pase por p_i y no contenga a ningún otro punto p_j para $j \neq i$. Tenemos así d polinomios homogéneos $G_i = \prod_{j \neq i} H_j$ de grado $d-1$ que se anulan en cada uno de los puntos de X salvo en p_i. Tomando $l \geqslant d-1$ es posible encontrar un polinomio homogéneo F de grado $l - d + 1 \geqslant 0$ que no se anule en ninguno de los puntos p_i, de forma que podemos construir d polinomios homogéneos de grado l, FG_i, con $i = 1, ..., d$, tales que para cada i, FG_i se anule en cada $p_{j \neq i}$ y sea no nulo en p_i. De esta forma, el conjunto $\{\varphi_l(FG_i),\ i = 1, ..., d\}$ constituye una base de $\mathbb{K}^d$, con lo que φ_l es sobreyectiva. Por el Primer Teorema de isomorfía, $S_l/(I(X) \cap S_l)$ y $\mathbb{K}^d$ son isomorfos como $\mathbb{K}$-espacios vectoriales, y en particular, $h_{I(X)}(l) = d$ para cada $l \geqslant d-1$.

$\Leftarrow$: supongamos que X no fuera finito. En este caso, podemos tomar $d+1$ puntos distintos de X; llamemos $Y \subset X$ a dicho conjunto de puntos. Entonces $I(X) \subset I(Y)$, y de esta forma tenemos un homomorfismo (de grupos abelianos) sobreyectivo $S(X) \longrightarrow S(X)/(I(Y)/I(X)) \cong S(Y)$, $F + I(X) \mapsto F + I(Y)$, que por restricción induce una aplicación $\mathbb{K}$-lineal sobreyectiva de $S(X)_l$ en $S(Y)_l$ para cada $l \in \mathbb{N}$. Pero esto es imposible, pues para $l \gg 0$, $\dim_{\mathbb{K}} S(X)_l = d < \dim_{\mathbb{K}} S(Y)_l = d+1$ (esta última igualdad por la implicación ya probada).

Por tanto, X debe ser un conjunto finito de puntos, y por lo ya probado, la cantidad de tales puntos debe ser igual a d.

□

Observación (1). En ocasiones nos encontraremos con casos en los que un tal conjunto finito de puntos viene descrito como $X = V(\mathfrak{a})$, con $\mathfrak{a}$ un ideal homogéneo no radical. En este caso, la función de Hilbert de $\mathfrak{a}$ seguirá siendo constante para l suficientemente grande, pero dicha constante no será igual, en general, al número de puntos de X, sino que contará estos con una cierta *multiplicidad*. Esta idea la haremos precisa más adelante.

Observación (2). Al probar la implicación a la izquierda hemos supuesto implícitamente que si X no es finito entonces es infinito. Cabría la posibilidad, sin embargo, de que fuera vacío. Esta situación podemos evitarla si en el enunciado de la Proposición 3.2 añadimos que $h_{I(X)}(l)$ además de ser constante para $l \gg 0$ sea no nula, como demuestra la siguiente proposición.

Proposición 3.3. *Dado un ideal homogéneo $\mathfrak{a} \subset S$, $V(\mathfrak{a}) = \emptyset$ si y solo si $h_{\mathfrak{a}}(l) = 0$ para $l \gg 0$.*

Demostración. La condición $h_{\mathfrak{a}}(l) = 0$ para todo $l \in \mathbb{N}$ lo suficientemente grande es equivalente, por definición, a que $S_l \subset \mathfrak{a}$ para todo $l \gg 0$. En virtud del Lema 1.2 esto a su vez equivale a que $V(\mathfrak{a}) = \emptyset$. □

En relación con nuestro estudio de las intersecciones de curvas proyectivas la propiedad quizás más importante de la función de Hilbert de un ideal es que esta viene dada, para valores suficientemente grandes de $l \in \mathbb{N}$, por un polinomio, que llamaremos polinomio de Hilbert de dicho ideal. Para demostrar este hecho necesitamos antes enunciar dos lemas previos.

Lema 3.1. *Dado un ideal homogéneo $\mathfrak{a} \subset S$, este es saturado si y solo si existe una forma lineal $H \in S$ que no pertenezca a ningún primo asociado de $\mathfrak{a}$.*

Demostración. $\Rightarrow$: supongamos que es saturado, y sea $\mathfrak{a} = \mathfrak{b}_1 \cap ... \cap \mathfrak{b}_r$ una descomposición primaria irredundante. Por la Proposición 2.2 tenemos que $\mathfrak{M}$ no es un primo asociado de $\mathfrak{a}$. Por lo tanto, $V(\mathfrak{b}_i) \neq \emptyset$ para cada $i = 1, ..., r$, en virtud del Lema 1.2. Tomemos entonces un punto $p_i \in V(\mathfrak{b}_i)$ para cada $i = 1, ..., r$, y sea H la ecuación de un hiperplano que no contenga a ninguno de dichos puntos, que existe dado que la cantidad de puntos considerada es finita. De aquí se sigue que $H \notin \sqrt{\mathfrak{b}_i}$ para cada $i = 1, ..., r$, es decir, H no pertence a ningún primo asociado de $\mathfrak{a}$.

$\Leftarrow$: dado que cualquier forma lineal pertenece a $\mathfrak{M}$, si existe alguna que no pertenezca a ningún primo asociado de $\mathfrak{a}$ es claro que $\mathfrak{M}$ no puede estar entre dichos primos asociados, lo que de nuevo por la Proposición 2.2 implica que $\mathfrak{a}$ es saturado. □

Antes de enunciar el segundo lema hay que introducir algo de notación. Dado un anillo graduado A y un A-módulo graduado M, denotaremos por $M(-d)$ el A-módulo que coincide, como conjunto, con M, pero cuya parte homogénea de grado l es la parte homogénea de grado $l - d$ de M.

Lema 3.2. *Sean $\mathfrak{a} \subset S$ un ideal homogéneo y F un polinomio homogéneo de grado d que no pertenezca a ningún primo asociado de $\mathfrak{a}$. Entonces, la multiplicación por F induce un homomorfismo graduado inyectivo entre los módulos $(S/\mathfrak{a})(-d)$ y $(S/\mathfrak{a})$. Esto da lugar, en particular, a la sucesión exacta graduada $0 \to (S/\mathfrak{a})(-d) \to (S/\mathfrak{a}) \to S/(\mathfrak{a} + (F)) \to 0$.*

Demostración. Denotemos por $\varphi : (S/\mathfrak{a})(-d) \to (S/\mathfrak{a})$ el homomorfismo dado por $\varphi(G+\mathfrak{a}) = FG + \mathfrak{a}$. Para ver que es inyectivo, basta probar que $\ker(\varphi) = \{0\}$. Dado $G \in (S/\mathfrak{a})(-d)$, $\varphi(G+\mathfrak{a}) = 0 \Leftrightarrow FG \in \mathfrak{a}$. Tomemos una descomposición primaria del ideal, $\mathfrak{a} = \mathfrak{b}_1 \cap ... \cap \mathfrak{b}_r$. En particular, $FG \in \mathfrak{b}_i$ para cada $i = 1, ..., r$. De la hipótesis sobre F y dado que dichos ideales son primarios, necesariamente $G \in \mathfrak{b}_i$ para cada $i = 1, ...r$, con lo que $G \in \mathfrak{a}$, es decir, $G + \mathfrak{a} = 0$. Además, dado $(G + \mathfrak{a}) \in (S/\mathfrak{a})(-d)$ un elemento homogéneo de grado $l \in \mathbb{N}$, tendremos que $(FG+\mathfrak{a}) \in (S/\mathfrak{a})$ es homogéneo de grado l, con lo que φ es un homomorfismo graduado.

Para la segunda parte, observemos primero que la aplicación $\phi : (S/\mathfrak{a}) \to S/(\mathfrak{a} + (F))$, $G + \mathfrak{a} \mapsto G + (\mathfrak{a} + (F))$ es claramente sobreyectiva. Veamos entonces que $\ker(\phi)$=$\mathrm{im}(\varphi)$. En efecto, $\phi(G + (\mathfrak{a} + (F))) = 0 \Leftrightarrow G \in \mathfrak{a} + (F) \Leftrightarrow G = H_1 + FH_2$, con $H_1 \in \mathfrak{a}$ y $H_2 \in S$, $\Leftrightarrow G + \mathfrak{a} = FH_2 + \mathfrak{a} \in \mathrm{im}(\varphi)$. Además, el hecho de que ϕ es un homomorfismo graduado se deduce de la Observación 1 hecha tras la Proposición 1.1.

De todo lo anterior concluimos que, efectivamente, la sucesión del enunciado es una sucesión exacta graduada. □

Observación. Si aplicamos la aditividad de la función de Hilbert para sucesiones exactas a la sucesión que hemos tratado en este lema, deducimos que $h_{\mathfrak{a}+(F)}(l) = h_{\mathfrak{a}}(l) - h_{\mathfrak{a}}(l-d)$ para cada $l \in \mathbb{N}$. Esta relación nos será de gran utilidad en el siguiente capítulo.

Terminamos el capítulo con la demostración del teorema de existencia del polinomio de Hilbert.

Teorema 3.1. *Sea $\mathfrak{a} \subset S$ un ideal homogéneo. Entonces, existe un polinomio $P_{\mathfrak{a}} \in \mathbb{Q}[t]$ tal que $h_{\mathfrak{a}}(l) = P_{\mathfrak{a}}(l)$ para todo $l \in \mathbb{N}$ suficientemente grande.*

Demostración. Procedemos por inducción en el número de indeterminadas del anillo de polinomios S.

Si $n = 0$, estamos en el caso del anillo de polinomios en una indeterminada. Aquí, todo ideal homogéneo tiene la forma $\mathfrak{a} = (0)$ o $\mathfrak{a} = (X_0^k)$ para $k \geq 0$. En el primer caso, $h_{\mathfrak{a}}(l) = 1$ para todo $l \in \mathbb{N}$, mientras que en el segundo caso $h_{\mathfrak{a}}(l) = 0$ para todo $l \geq k$, con lo que existe tal polinomio (y es constante).

Supongamos la afirmación cierta para $n-1$, y sea $\mathfrak{a}$ un ideal homogéneo de $\mathbb{K}[X_0, ..., X_n]$. Por la Proposición 3.3, si $\mathfrak{a}$ es $\mathfrak{M}$-primario entonces $h_{\mathfrak{a}}(l) = 0$ para todo $l \gg 0$ y no hay nada que probar. Además, dado que queremos estudiar la función de Hilbert para $l \in \mathbb{N}$ suficientemente grande, en virtud de la Proposición 2.2 podemos suponer sin pérdida de generalidad que $\mathfrak{a}$ es saturado. Por el Lema 3.1 es posible encontrar una forma lineal H que no pertenezca a ningún primo asociado de $\mathfrak{a}$, de forma que, por el Lema 3.2, tenemos que $h_{\mathfrak{a}+(H)}(l) = h_{\mathfrak{a}}(l) - h_{\mathfrak{a}}(l-1)$. Haciendo un cambio de coordenadas podemos suponer que $H = X_n$, con lo que $\mathbb{K}[X_0, ..., X_n]/(\mathfrak{a} + (X_n)) \cong \mathbb{K}[X_0, ..., X_{n-1}]/(\mathfrak{b})$, con $\mathfrak{b}$ el ideal de $\mathbb{K}[X_0, ..., X_{n-1}]$ que se obtiene al sustituir $X_n = 0$ en los polinomios de $\mathfrak{a}$. En particular, esto nos permite identificar $h_{\mathfrak{a}+(H)}$ con la función de Hilbert de un ideal en $\mathbb{K}[X_0, ..., X_{n-1}]$, lo que por la hipótesis de inducción implica que $h_{\mathfrak{a}+(H)}(l) = P_{\mathfrak{b}}(l)$, con $P_{\mathfrak{b}} \in \mathbb{Q}[t]$, para todo $l \in \mathbb{N}$ lo suficientemente grande.

Hallemos ahora $P_{\mathfrak{a}}$. Para ello, notemos en primer lugar que una base del conjunto de polinomios de grado a lo sumo d con coeficientes en $\mathbb{Q}$ viene dada por $\binom{t}{0}, ..., \binom{t}{d}$ (nótese que $\binom{t}{0} = 1$, $\binom{t}{1} = t$, y podemos así ir expresando inductivamente las potencias t^k en términos de $\binom{t}{j}$ con $j \leq k$). Por tanto, existen $c_0, ..., c_d \in \mathbb{Q}$ tales que $P_{\mathfrak{b}}(t) = c_d\binom{t}{d} + ... + c_1\binom{t}{1} + c_0\binom{t}{0}$.

Puesto que $\binom{t}{k} = \binom{t}{k-1} + \binom{t-1}{k-1}$, es claro que el polinomio $p(t) = c_d\binom{t+1}{d+1} + ... + c_0\binom{t+1}{1}$ satisface $P_{\mathfrak{b}}(t) = p(t) - p(t-1)$.

Denotemos por $r(l) = h_{\mathfrak{a}}(l) - p(l)$. Dado que, como hemos probado ya, $P_{\mathfrak{b}}(l) = h_{\mathfrak{a}}(l) - h_{\mathfrak{a}}(l-1)$ para $l \gg 0$, se sigue que $r(l) - r(l-1) = 0$ para $l \in \mathbb{N}$ suficientemente grande. En consecuencia, $r(l)$ debe ser una constante, digamos r_0, para $l \gg 0$, con lo que $h_{\mathfrak{a}}(l) = p(l) + r_0$ para $l \gg 0$, y por tanto es un polinomio. □

Observación. La existencia del polinomio de Hilbert es cierta también en el caso general de S-módulos graduados finitamente generados, con el cuerpo $\mathbb{K}$ no necesariamente algebraicamente cerrado. La demostración de este resultado puede encontrarse en [1, 4].

Capítulo 4

El Teorema de Bézout para curvas planas

Con todo lo que hemos desarrollado hasta ahora tenemos las herramientas necesarias para probar el teorema central de este trabajo, el Teorema de Bézout para curvas proyectivas planas.

En primer lugar debemos introducir dos atributos de los conjuntos proyectivos, la *dimensión* y el *grado*, que admiten definiciones sencillas en términos del polinomio de Hilbert.

Definición 4.1. *Dado un conjunto proyectivo $X \subset \mathbb{P}^n$ se define su dimensión como el grado del polinomio de Hilbert del ideal $I(X)$.*

Para interpretar geométricamente esta definición debemos primero ver que es consistente con la noción de dimensión habitual que tenemos para subespacios lineales, definidos como los ceros de un conjunto finito de polinomios homogéneos de grado 1. Sabemos que si $\Lambda \subset \mathbb{P}^n$ es un subespacio lineal definido por las ecuaciones lineales independientes (en el sentido del álgebra lineal) $H_1 = ... = H_r = 0$, con $r \leq n$ y $H_i \in S$ polinomios homogéneos grado 1, se define la dimensión de Λ como $\dim(\Lambda) = n - r$ (notemos que estamos excluyendo el conjunto vacío, que también se considera un subespacio lineal de $\mathbb{P}^n$ para el que, por definición, $\dim(\emptyset) = -1$). Mediante un cambio adecuado de coordenadas, podemos suponer que $H_1 = X_{n-r+1}, ..., H_r = X_n$. Dado que $\mathbb{K}[X_0, ..., X_n]/(H_1, ..., H_r) \cong \mathbb{K}[X_0, ..., X_{n-r}]$, obtenemos que el ideal $(H_1, ..., H_r)$ es primo, luego en particular radical, y dado que $V(H_1, ..., H_r) = \Lambda$, del Teorema 1.1 se sigue que $I(\Lambda) = (H_1, ..., H_r)$.

Por otro lado, notemos que el conjunto $\{X_0^{i_0} \cdot ... \cdot X_{n-r}^{i_{n-r}} \mid i_0 + ... + i_{n-r} = l\}$ constituye una base de la parte homogénea de grado l de $\mathbb{K}[X_0, ..., X_{n-r}]$ vista como $\mathbb{K}$-espacio vectorial. Los elementos de esta base están en biyección con las combinaciones con repetición de $n - r + 1$ elementos tomados de l en l, con lo que la dimensión de dicha parte homogénea es $\binom{n-r+l}{n-r}$. Entonces tendremos que, por definición, $h_{I(\Lambda)}(l) = \binom{n-r+l}{n-r} = \frac{1}{(n-r)!} l^{n-r} + ...$, con lo que $\deg(P_{I(\Lambda)}) = n - r$, y ambas definiciones coinciden.

Tras esta discusión podemos enunciar una proposición que dará sentido geométrico a la dimensión, y que en particular, nos dirá que para calcular la dimensión de un conjunto proyectivo X podemos usar cualquier ideal que defina dicho conjunto.

Proposición 4.1. *Dado un conjunto proyectivo $X \subset \mathbb{P}^n$ definido como $X = V(\mathfrak{a})$, con $\mathfrak{a} \subset S$ un ideal homogéneo no $\mathfrak{M}$-primario, se cumple que $\deg(P_{\mathfrak{a}})$ es el máximo $r \in \mathbb{N}$ tal que cualquier subespacio lineal de $\mathbb{P}^n$ de codimensión r corta a X.*

Demostración. En primer lugar, notemos que en virtud del Lema 1.2, $X \neq \emptyset$, con lo que $\deg(P_{\mathfrak{a}}) \geq 0$ en virtud de la Proposición 3.3. Tomemos un subespacio lineal de codimensión $s \leq r = \deg(P_{\mathfrak{a}})$, que por la discusión que hemos hecho antes, vendrá dado por $V(H_1, ..., H_s)$, con los H_i polinomios homogéneos de grado 1.

De la misma manera a como hicimos en el Lema 3.2 podemos probar que la multiplicación por H_1 induce una sucesión exacta graduada $(S/\mathfrak{a})(-1) \xrightarrow{\varphi_1} (S/\mathfrak{a}) \xrightarrow{\varphi_2} (S/(\mathfrak{a} + (H_1)) \to 0$ (nótese que en este caso la multiplicación por H_1 no tiene por qué ser inyectiva).

Por la fórmula de las dimensiones del álgebra lineal para espacios vectoriales tenemos que, para todo $l \in \mathbb{N}$ suficientemente grande, $P_{\mathfrak{a}+(H_1)}(l) = P_{\mathfrak{a}}(l) - P_{\mathfrak{a}}(l-1) + \dim(\ker(\varphi_1)) \geq P_{\mathfrak{a}}(l) - P_{\mathfrak{a}}(l-1)$. Puesto que el grado del polinomio $P_{\mathfrak{a}}(l) - P_{\mathfrak{a}}(l-1)$ es $r-1$, el de $P_{\mathfrak{a}+(H_1)}(l)$ debe ser al menos $r-1$ (notemos que el coeficiente director de $P_{\mathfrak{a}}(l) - P_{\mathfrak{a}}(l-1)$ es positivo, por serlo el del polinomio $P_{\mathfrak{a}}(l)$).

Reiterando este proceso con los restantes H_i obtenemos que el polinomio de Hilbert del ideal $\mathfrak{a} + (H_1, ..., H_s)$ tiene grado al menos $r - s \geq 0$. Pero dado que $V(\mathfrak{a} + (H_1, ..., H_s)) = X \cap V(H_1, ..., H_s)$, de la Proposición 3.3 deducimos que dicha intersección es no vacía.

Para terminar la demostración vamos a construir un subespacio lineal de codimensión $r+1$ que no corte a X. Dado que $\mathfrak{a}$ no es $\mathfrak{M}$-primario, deberá tener algún primo asociado no irrelevante, y en virtud de la Proposición 2.2 y el Lema 3.1 podemos tomar un polinomio homogéneo de grado 1, H_1, que no esté en ningún primo asociado de la saturación de $\mathfrak{a}$. Por el Lema 3.2, y teniendo en cuenta que los polinomios de Hilbert de un ideal y de su saturación coinciden, tenemos que $P_{\mathfrak{a}+(H_1)}(l) = P_{\mathfrak{a}}(l) - P_{\mathfrak{a}}(l-1)$, que tiene grado $r-1$. Podemos ahora reiterar este proceso hasta obtener, finalmente, $r+1$ formas lineales $H_1, ..., H_{r+1}$ tales que el polinomio de Hilbert de $\mathfrak{a} + (H_1, ..., H_{r+1})$ sea nulo. Esto, de nuevo por la Proposición 3.3, implica que $X \cap V(H_1, ..., H_{r+1}) = \emptyset$, y hemos terminado. □

Observación. El hecho de que dos conjuntos proyectivos se corten o no es independiente de los ideales usados para describir dichos conjuntos. Por tanto, la proposición anterior nos dice en particular que si dos ideales homogéneos no $\mathfrak{M}$-primarios, $\mathfrak{a}$ y $\mathfrak{b}$, son tales que $V(\mathfrak{a}) = V(\mathfrak{b})$, entonces $\deg(P_{\mathfrak{a}})$=$\deg(P_{\mathfrak{b}})$.

Como anunciamos al comienzo del capítulo, la siguiente noción que debemos estudiar es la de grado de un conjunto proyectivo.

Definición 4.2. *Dado un conjunto proyectivo $X \subset \mathbb{P}^n$ de dimensión r se define su grado como* $\deg(X) = ar!$*, donde a es el coeficiente director del polinomio de Hilbert de X.*

La interpretación geométrica del grado es como sigue. Al igual que hicimos en la demostración de la Proposición 4.1, vamos a ir cortando X con hiperplanos generales, es decir, tales que el hiperplano $V(H_i)$ no contenga ninguna componente irreducible de $X \cap V(H_1, ..., H_{i-1})$. En estas condiciones, si $P_{I(X)}(l) = al^r + ...$, entonces en virtud del Lema 3.2 tenemos que $P_{I(X)+(H_1)}(l) = P_{I(X)}(l) - P_{I(X)}(l-1) = arl^{r-1} + ...$ Procediendo inductivamente de esta forma, llegamos finalmente a que $P_{I(X)+(H_1,...,H_r)}(l) = ar! = \deg(X)$, es decir, $X \cap V(H_1, ..., H_r)$ es un conjunto finito de puntos. Como señalamos en la Observación 1 que sucede a la Proposición 3.2, tenemos por tanto que $\deg(X)$ es el número de puntos de intersección de X con r hiperplanos generales, contados con una cierta *multiplicidad* que definiremos en este capítulo.

Vamos a probar ahora un lema que será fundamental a la hora de demostrar el Teorema de Bézout.

Lema 4.1. *Sea $X = V(F) \subset \mathbb{P}^n$, con $F \in S$ un polinomio homogéneo de grado $d > 0$, tal que $I(X) = (F)$. Entonces* $\dim(X) = n - 1$ *y* $\deg(X) = d$.

Demostración. Sea la sucesión exacta graduada $0 \to S(-d) \xrightarrow{\varphi_1} S \to S/(F) \to 0$, donde φ_1 es la aplicación inducida por la multiplicación por F. Teniendo en cuenta, como ya hemos justificado antes, que $\dim_{\mathbb{K}} S_l = \binom{n+l}{n}$, la aditividad de la función de Hilbert para sucesiones exactas implica que $P_{I(X)}(l) = \binom{n+l}{n} - \binom{n+l-d}{n} = \frac{d}{(n-1)!} l^{n-1} + ...$ Atendiendo a las definiciones de dimensión y grado se deduce de aquí que $\dim(X) = n - 1$ y $\deg(X) = d$, respectivamente. □

Particularizando al caso de $\mathbb{P}^2$, este lema nos dice que las curvas planas tienen dimensión 1 y grado igual al grado de cualquier ecuación minimal suya.

Con lo desarrollado hasta ahora podemos enunciar una versión débil del Teorema de Bézout.

Teorema 4.1 (débil de Bézout)**.** *Sean $C, D \subset \mathbb{P}^2$ dos curvas sin componentes irreducibles comunes. Sean $F, G \in \mathbb{K}[X_0, X_1, X_2]$ ecuaciones minimales de C y D, respectivamente. Entonces $C \cap D$ consiste en, a lo sumo,* $\deg(F) \cdot \deg(G)$ *puntos.*

Demostración. Sabemos de la discusión al comienzo del Capítulo 2 que si las descomposiciones en factores irreducibles de las ecuaciones minimales son $F = F_1 \cdot ... \cdot F_r$ y $G = G_1 \cdot ... \cdot G_s$, respectivamente, entonces la descomposición de C y D en componentes irreducibles es $C = V(F_1) \cup ... \cup V(F_r)$ y $D = V(G_1) \cup ... \cup V(G_s)$. Por tanto, la condición de que C y D no compartan componentes irreducibles es equivalente a que F y G sean primos entre sí. En particular, G no pertenece a ningún primo asociado del ideal (F). El Lema 3.2 nos dice entonces que $P_{(F,G)}(l) = P_{(F)}(l) - P_{(F)}(l - \deg(G))$.

Vimos ya que $\dim(C)=1$ y que $\deg(C)=\deg(F)$, con lo que $P_{(F)}(l) = \deg(F)l + b$, para cierto $b \in \mathbb{Q}$. Pero entonces, lo anterior implica que $P_{(F,G)}(l) = \deg(F) \cdot \deg(G)$, de donde se deduce que $C \cap D$ es un conjunto finito de puntos, dado que $P_{I(C \cap D)}(l)$ será también constante en virtud de la Observación tras la Proposición 4.1.

Además, puesto que $(F, G) \subset I(C \cap D)$ tenemos una aplicación sobreyectiva natural $\mathbb{K}[X_0, X_1, X_2]/(F, G) \to \mathbb{K}[X_0, X_1, X_2]/(I(C \cap D))$, $H + (F, G) \mapsto H + I(C \cap D)$, que induce por restricción una aplicación lineal sobreyectiva de $\mathbb{K}$-espacios vectoriales, con lo que $P_{I(C \cap D)}(l) \leq \deg(F) \cdot \deg(G)$. Tenemos así que el número de puntos de $C \cap D$, que es $P_{I(C \cap D)}(l)$ por la Proposición 3.2, es a lo sumo $\deg(F) \cdot \deg(G)$. □

Para enunciar y demostrar el Teorema de Bézout necesitamos finalmente introducir la noción de *multiplicidad de intersección*.

Definición 4.3. *Sean $X, Y \subset \mathbb{P}^n$ dos conjuntos proyectivos, y sea $p \in X \cap Y$ un punto que supondremos una componente irreducible de $X \cap Y$. Se define la multiplicidad de intersección de X e Y en p como el valor del polinomio de Hilbert de la componente $I(p)$-primaria de $I(X) + I(Y)$, donde $I(p)$ denota el ideal de p.*

Observación. La multiplicidad de intersección en un punto p está bien definida, pues la hipótesis de que p sea una componente irreducible de $X \cap Y$ implica que la componente $I(p)$-primaria correspondiente es independiente de la descomposición primaria particular de $I(X) + I(Y)$, al ser entonces $I(p)$ un primo asociado minimal de este ideal.

Lema 4.2. *Dados ideales homogéneos $\mathfrak{a}, \mathfrak{b} \subset S$, existe una sucesión exacta graduada $0 \to S/(\mathfrak{a} \cap \mathfrak{b}) \xrightarrow{\varphi_1} S/\mathfrak{a} \oplus S/\mathfrak{b} \xrightarrow{\varphi_2} S/(\mathfrak{a}+\mathfrak{b}) \to 0$.*

Demostración. Definamos las aplicaciones $\varphi_1(F+(\mathfrak{a}\cap\mathfrak{b})) = (F+\mathfrak{a}, F+\mathfrak{b})$, y $\varphi_2(F+\mathfrak{a}, G+\mathfrak{b}) = (F-G)+(\mathfrak{a}+\mathfrak{b})$. Veamos que con estos homomorfismos la sucesión es exacta.

En primer lugar, $\varphi_1(F+(\mathfrak{a}\cap\mathfrak{b})) = (F+\mathfrak{a}, F+\mathfrak{b}) = (0,0) \Leftrightarrow F \in \mathfrak{a}$ y $F \in \mathfrak{b}$, es decir, $F+(\mathfrak{a}\cap\mathfrak{b}) = 0$, con lo que $\ker(\varphi_1) = \{0\}$ y φ_1 es inyectiva.

Por otro lado, $\varphi_2(F+\mathfrak{a}, G+\mathfrak{b}) = (F-G)+(\mathfrak{a}+\mathfrak{b}) = 0 \Leftrightarrow F-G \in (\mathfrak{a}+\mathfrak{b})$, es decir, $F-G = H_1+H_2$, con $H_1 \in \mathfrak{a}$ y $H_2 \in \mathfrak{b}$; en particular, $F+\mathfrak{a} = (F-H_1)+\mathfrak{a}$ y $G+\mathfrak{b} = (F-H_1-H_2)+\mathfrak{b} = (F-H_1)+\mathfrak{b}$, con lo que $(F+\mathfrak{a}, G+\mathfrak{b}) = (F-H_1+\mathfrak{a}, F-H_1+\mathfrak{b})$ y por tanto $\ker(\varphi_2) \subset \mathrm{im}(\varphi_1)$. El otro contenido es evidente, así que $\ker(\varphi_2) = \mathrm{im}(\varphi_1)$.

Para terminar, basta probar que φ_2 es sobreyectiva; en efecto, dado $F+(\mathfrak{a}+\mathfrak{b})$, tomando $(F+\mathfrak{a}, G+\mathfrak{b})$, con $G \in \mathfrak{b}$, se cumple que $\varphi_2(F+\mathfrak{a}, G+\mathfrak{b}) = F+(\mathfrak{a}+\mathfrak{b})$.

Luego efectivamente la sucesión es exacta. □

Observación. La aditividad de la función de Hilbert para sucesiones exactas aplicada a la sucesión del Lema 4.2, nos permite deducir que dados los ideales homogéneos $\mathfrak{a}, \mathfrak{b} \subset S$, se verifica $h_{\mathfrak{a}+\mathfrak{b}}(l) = h_{\mathfrak{a}}(l) + h_{\mathfrak{b}}(l) - h_{\mathfrak{a}\cap\mathfrak{b}}(l)$ para cada $l \in \mathbb{N}$.

Ya podemos probar el Teorema de Bézout para curvas planas.

Teorema 4.2 (Bézout)**.** *Sean $C, D \subset \mathbb{P}^2$ dos curvas sin componentes irreducibles comunes, y sean $F, G \in \mathbb{K}[X_0, X_1, X_2]$ ecuaciones minimales de C y D, respectivamente. Entonces $C \cap D$ consiste en $\deg(F)\cdot\deg(G)$ puntos, contados con multiplicidad.*

Demostración. Ya sabemos del Teorema 4.1 que F y G son primos entre sí y que $C \cap D$ es un número finito de puntos, $\{p_1, ..., p_r\}$, con $p_i \neq p_j$ si $i \neq j$. Podemos escribir por tanto $(F,G) = \mathfrak{b}_1 \cap ... \cap \mathfrak{b}_s \cap \mathfrak{a}_1 \cap ... \cap \mathfrak{a}_r$, donde los $\mathfrak{a}_i$ son las componentes no inmersas de (F,G), que son ideales $I(p_i)$-primarios; de haber alguna componente inmersa, su radical debería contener estrictamente algún $I(p_i)$, lo que significa que el conjunto proyectivo al que da lugar debe estar estrictamente contenido en $\{p_i\}$, con lo que necesariamente es $\emptyset$. Como sabemos, esto implica que $s = 1$ y que $\mathfrak{b}_1$ es la componente irrelevante de la descomposición.

Tenemos por tanto que $P_{(F,G)}(l) = P_{\mathfrak{a}_1\cap...\cap\mathfrak{a}_r}(l)$. Probemos, por inducción, que $P_{\mathfrak{a}_1\cap...\cap\mathfrak{a}_r}(l) = P_{\mathfrak{a}_1}(l) + ... + P_{\mathfrak{a}_r}(l)$. Para $r = 2$ tenemos que, en virtud del Lema 4.2 y de la aditividad de la función de Hilbert, $P_{\mathfrak{a}_1\cap\mathfrak{a}_2}(l) = P_{\mathfrak{a}_1}(l) + P_{\mathfrak{a}_2}(l) - P_{\mathfrak{a}_1+\mathfrak{a}_2}(l)$. Pero $V(\mathfrak{a}_1+\mathfrak{a}_2) = \{p_1\} \cap \{p_2\} = \emptyset$, con lo que $P_{\mathfrak{a}_1+\mathfrak{a}_2}(l) = 0$, y $P_{\mathfrak{a}_1\cap\mathfrak{a}_2}(l) = P_{\mathfrak{a}_1}(l) + P_{\mathfrak{a}_2}(l)$.

Supongamos ahora que el resultado es cierto hasta $r-1$. De nuevo por el Lema 4.2 tenemos $P_{\mathfrak{a}_1\cap...\cap\mathfrak{a}_r}(l) = P_{\mathfrak{a}_1\cap...\cap\mathfrak{a}_{r-1}}(l) + P_{\mathfrak{a}_r}(l) - P_{(\mathfrak{a}_1\cap...\cap\mathfrak{a}_{r-1})+\mathfrak{a}_r}(l)$, y además $P_{(\mathfrak{a}_1\cap...\cap\mathfrak{a}_{r-1})+\mathfrak{a}_r}(l) = 0$, puesto que $V((\mathfrak{a}_1 \cap ... \cap \mathfrak{a}_{r-1}) + \mathfrak{a}_r) = \emptyset$, con lo que aplicando la hipótesis de inducción, $P_{\mathfrak{a}_1\cap...\cap\mathfrak{a}_r}(l) = P_{\mathfrak{a}_1}(l) + ... + P_{\mathfrak{a}_r}(l)$.

Teniendo en cuenta que, por definición, $m_i = P_{\mathfrak{a}_i}(l)$ es la multiplicidad de intersección de C y D en p_i, y que ya vimos (en la demostración del Teorema 4.1) que $P_{(F,G)}(l) = \deg(F)\cdot\deg(G)$, tenemos finalmente que $\deg(F)\cdot\deg(G) = m_1 + ... + m_r$. □

Observación. Aunque para obtener el resultado anterior no hemos necesitado saberlo, en el caso de dos polinomios $F, G \in \mathbb{K}[X_0, X_1, X_2]$ homogéneos primos entre sí es posible demostrar que el ideal (F,G) es saturado, con lo que nos habríamos ahorrado discutir la posible presencia de una componente irrelevante en la descomposición primaria de dicho ideal. La demostración podemos encontrarla en [1].

Cabe destacar que es posible generalizar el Teorema de Bézout a dimensiones superiores y para intersecciones entre conjuntos proyectivos más generales que las curvas planas. Un tratamiento sistemático de dichas generalizaciones se escapa de los objetivos de este trabajo, donde el interés principal está puesto sobre el Teorema de Bézout para curvas proyectivas planas. No obstante, por completitud, vamos a presentar una generalización inmediata de dicho teorema.

Notemos que el Teorema 4.2 nos da esencialmente las condiciones para que dos hipersuperficies en $\mathbb{P}^2$ tengan por intersección una cantidad finita de puntos, además de decirnos de cuántos puntos consta dicha intersección, contados con su multiplicidad. La generalización más natural que podemos plantear entonces es el caso de n hipersuperficies en $\mathbb{P}^n$.

Teorema 4.3. *Sean $X_1, ..., X_n \subset \mathbb{P}^n$ hipersuperficies tales que $I(X_i) = (F_i)$, con* $\deg(F_i)$=d_i. *Supongamos además que, para cada $i = 2, ..., n$, F_i no pertenece a ningún primo asociado relevante del ideal $(F_1, ..., F_{i-1})$. Entonces $X_1 \cap ... \cap X_n$ consiste en $d_1 \cdot ... \cdot d_n$ puntos, contados con multiplicidad.*

Demostración. Dado que vamos a estudiar la función de Hilbert para $l \gg 0$, podemos suponer sin pérdida de generalidad que los ideales $(F_1, ..., F_{i-1})$, con $i = 2, ..., n$, son saturados, y tendríamos entonces que F_i no pertenece a ningún primo asociado de $(F_1, ..., F_{i-1})$.

Sea el polinomio de Hilbert de X_1, $P_{(F_1)}(l) = \frac{d_1}{(n-1)!} l^{n-1} + ...$ Podemos aplicar el Lema 3.2 al polinomio F_2 y concluir entonces que $P_{(F_1,F_2)}(l) = P_{F_1}(l) - P_{(F_1)}(l - d_2) = \frac{d_1 d_2}{(n-2)!} l^{n-2} + ...$ Aplicando así el Lema 3.2 inductivamente $n-1$ veces llegamos a que $P_{(F_1,...,F_n)}(l) = d_1 \cdot ... \cdot d_n$. Esto demuestra que $X_1 \cap ... \cap X_n$ es una cantidad finita de puntos, $\{p_1, ..., p_r\}$. De esta manera, tenemos una descomposición primaria de la forma $(F_1, ..., F_n) = \mathfrak{b} \cap \mathfrak{a}_1 \cap ... \cap \mathfrak{a}_r$, donde $\mathfrak{b}$ es la componente irrelevante de la descomposición (si existiera), y $\mathfrak{a}_i$ son las componentes $I(p_i)$-primarias. El mismo argumento que usamos en la demostración del Teorema 4.2 nos permite escribir entonces $P_{(F_1,...,F_n)}(l) = d_1 \cdot ... \cdot d_n = P_{\mathfrak{a}_1 \cap ... \cap \mathfrak{a}_r}(l) = P_{\mathfrak{a}_1}(l) + ... + P_{\mathfrak{a}_r}(l) = m_1 + ... + m_r$, con m_i la multiplicidad de intersección en p_i. □

Observación. En el caso $n > 2$ no podemos suponer únicamente que los polinomios $F_1, ..., F_n$ que definen las hipersuperficies sean coprimos dos a dos (como sí ocurría para $n = 2$). Podemos tomar como ejemplo la intersección de tres subespacios lineales distintos de dimensión 2 en $\mathbb{P}^3$; las formas lineales que los definen son polinomios coprimos dos a dos, pero si tomamos estos hiperplanos de forma que pertenezcan al mismo haz, la intersección de los tres es un subespacio lineal de dimensión 1, que no es un conjunto finito de puntos. A un conjunto de polinomios $\{F_1, ..., F_n\}$ tales que F_i no pertenece a ningún primo asociado de $(F_1, ..., F_{i-1})$ para cada $i = 2, ..., n$ se le denomina sucesión regular.

El hecho de que los polinomios F_i que definen las hipersuperficies constituyan una sucesión regular no es una condición banal. Se puede demostrar que un conjunto de polinomios homogéneos $\{F_1, ..., F_r\}$ en $\mathbb{K}[X_0, ..., X_n]$ constituye una sucesión regular si y solo si $\dim(X) = n - r$, con $X = V(F_1, ..., F_r)$. En particular, si queremos que la intersección de n hipersuperficies en $\mathbb{P}^n$ sea una cantidad finita de puntos, los polinomios que las definen deben satisfacer la condición impuesta en el enunciado del Teorema 4.3.

La demostración de este hecho requiere del uso de las llamadas *resoluciones libres* de módulos graduados, construcción que está más allá del alcance de este trabajo. Un tratamiento de dichas resoluciones libres y la demostración del resultado enunciado en el párrafo anterior podemos encontrarla en las referencias [1, 3].

Bibliografía

[1] Arrondo, E. *Introduction to projective varieties*.

[2] Atiyah, M.F., Macdonald, I.G. *Introduction to Commutative Algebra*. Addison-Welsey, 1969.

[3] Harris, J. *Algebraic Geometry. A First Course*. Springer, 1992.

[4] Hartshorne, R. *Algebraic Geometry*. Springer, 1977.