LA NOCIÓN DE MULTIPLICIDAD DE INTERSECCIÓN EN GEOMETRÍA ALGEBRAICA

TRABAJO DE FIN DE GRADO

CURSO 2021/22

UNIVERSIDAD COMPLUTENSE MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS

DOBLE GRADO EN MATEMÁTICAS Y FÍSICA

Diego Trujillo Carcelero

Tutor: Enrique Arrondo Esteban

Madrid, 5 de julio de 2022

Resumen:

En la asignatura de Curvas Algebraicas impartida en esta facultad se desarrolla toda la teoría de curvas planas proyectivas mediante técnicas elementales, lo que hace que dicha asignatura sea en esencia autocontenida. Como consecuencia, las demostraciones de los teoremas importantes como el Teorema de Bézout acaban siendo largas y en ocasiones poco directas. Otra aproximación a las curvas planas se puede llevar a cabo mediante la Geometría Algebraica. Si bien esta otra aproximación requiere de conocimientos previos relativos al Álgebra Conmutativa y a los conjuntos proyectivos, las demostraciones resultan mucho más cortas y conceptualmente más sencillas.

Una de las herramientas fundamentales utilizadas en Geometría Algebraica Proyectiva para el estudio de curvas planas es el polinomio de Hilbert. En términos de este polinomio se puede definir una multiplicidad de intersección de dos curvas en un punto dado, con la cual podemos desarrollar todo el estudio de intersección de curvas planas proyectivas y demostrar los principales teoremas de la teoría.

El resultado más importante de este trabajo es comprobar que dicha definición de multiplicidad coincide con la vista en la asignatura de Curvas Algebraicas. Además, para comprobar el buen funcionamiento de la definición, se demuestra (utilizando el polinomio de Hilbert) el Teorema fuerte de los ceros de Hilbert y el Teorema de Bézout, tanto en su versión débil como fuerte.

Abstract:

In the course of Algebraic Curves of this School, the whole theory of projective plane curves is developed through elementary techniques, which makes this course essentially self-contained. As a consequence, proofs of important theorems like Bézout's Theorem end up being long and complex. Another approach to plane curves can be developed through Algebraic Geometry. Although this other approach requires previous knowledge of Commutative Algebra and projective sets, the proofs are much shorter and conceptually simpler.

One of the fundamental tools used in Projective Algebraic Geometry while studying plane curves is the Hilbert's polynomial. In terms of these polynomials, we can define an intersection multiplicity of two curves at a given point. With this definition we can develop the whole study of intersection of proyective plane curves and we can prove the main results of the theory.

The most important result of this essay is to verify that this definition of intersection multiplicity coincides with the one seen in the course of Algebraic Curves. In addition, in order to check the significance of this definition, we prove Hilbert's Nullstellensatz and Bézout's Theorem using Hilbert's polynomial.

Índice general

Capítulo 0

Introducción y objetivos

La Geometría Algebraica es la rama de las matemáticas que estudia los objetos geométricos definidos sobre un espacio afín o proyectivo a partir de herramientas puramente algebraicas. Por ejemplo, dado un cuerpo algebraicamente cerrado $\mathbb{K}$, es bien sabido de Álgebra Conmutativa que existe un diccionario álgebra-geometría que nos permite caracterizar las variedades afines sobre un $\mathbb{K}$-espacio afín a través de ideales radicales del anillo de polinomios con coeficientes en $\mathbb{K}$. Se puede hacer un desarrollo análogo para el caso de las variedades sobre $\mathbb{K}$-espacios proyectivos, aunque como veremos en este texto, debemos trabajar con el concepto de ideal homogéneo.

Una de las herramientas más potentes de la Geometría Algebraica Proyectiva es el polinomio de Hilbert, el cual permite caracterizar numerosas propiedades de las variedades o conjuntos proyectivos. En particular, nos permite demostrar el Teorema fuerte de los ceros de Hilbert y el Teorema de Bézout. A través del polinomio de Hilbert podemos desarrollar toda la teoría de curvas planas vista en la asignatura de Curvas Algebraicas. Uno de los objetivos principales de este trabajo es comprobar que ambas teorías son equivalentes; esto último lo veremos comprobando que la definición de multiplicidad de intersección de dos curvas planas en un punto p dada por el polinomio de Hilbert coincide con la definición dada a partir de las parametrizaciones de las ramas de una curva. Si bien este resultado es de sobra conocido, al no encontrar referencia alguna donde se demuestre, en este texto presentamos una prueba totalmente original.

En el Capítulo 1 del trabajo recordamos los conceptos algebraicos necesarios para el desarrollo de la teoría. En particular, definimos anillo graduado, ideal homogéneo y concretaremos estos conceptos al anillo de polinomios en varias variables. Además, damos la definición de ideal primario y probaremos el Teorema de descomposición primaria de ideales para el caso homogéneo. Concluimos el capítulo hablando de la saturación de un ideal y dando unos pocos resultados clásicos relacionados con las sucesiones exactas.

En el Capítulo 2 aplicamos todos los conceptos algebraicos del Capítulo 1 al estudio de conjuntos proyectivos. Introducimos el diccionario álgebra-geometría para el caso proyectivo y demostramos el Teorema débil de los ceros de Hilbert. Finalmente, probamos que todo conjunto proyectivo admite una descomposición en conjuntos proyectivos irreducibles.

En el Capítulo 3 desarrollamos toda la teoría necesaria para construir la función de Hilbert de un módulo graduado y su polinomio de Hilbert. Introducimos la función de Hilbert de un ideal homogéneo y estudiamos la caracterización de conjuntos proyectivos finitos o vacíos a través de

su polinomio de Hilbert. Completamos el capítulo demostrando el Teorema fuerte de los ceros de Hilbert utilizando dicho polinomio.

En el Capítulo 4 aparece el principal resultado del texto. Ya sobre $\mathbb{P}^2$ y después de introducir las dos definiciones de multiplicidad de intersección con las que vamos a trabajar, comprobamos que sendas definiciones son equivalentes, probando así que ambas aproximaciones a las curvas planas (la vista en Curvas Algebraicas y la que utiliza el polinomio de Hilbert) coinciden.

El Capitulo 5 y último del trabajo está dedicado a definir la dimensión y grado de un conjunto proyectivo a través del polinomio de Hilbert y a concretar toda la teoría vista hasta este punto para el caso del plano proyectivo. Destacamos como resultado principal la demostración del Teorema de Bézout para curvas planas haciendo uso de técnicas englobadas en la Geometría Algebraica Proyectiva.

Siempre que se pueda se trabajará de la forma más general posible. Así, solamente concretamos la teoría al plano proyectivo cuando demostramos el Teorema de Bézout y cuando tratamos las definiciones de multiplicidad de intersección. Si bien existe una versión general del Teorema de Bézout, no es el objetivo de este trabajo, por lo que no se incluye en el texto.

Capítulo 1

Conceptos algebraicos previos

1.1. Anillos graduados

En esta primera sección asentamos las bases algebraicas necesarias para el desarrollo del trabajo, haciendo especial hincapié en los anillos graduados y los ideales homogéneos. En particular, el anillo graduado que nos interesará será el anillo de polinomios.

Definición 1.1 (Anillo graduado) *Un anillo graduado es un anillo $\mathcal{R}$ tal que, como grupo aditivo, se puede descomponer como suma directa $\mathcal{R} = \bigoplus_{d\geq 0} \mathcal{R}_d$ de tal forma que el producto en $\mathcal{R}$ es compatible con dicha descomposición; es decir, si $a \in \mathcal{R}_e$ y $b \in \mathcal{R}_f$ entonces $ab \in \mathcal{R}_{e+f}$.*

A cada $\mathcal{R}_d$ se le denota *parte homogénea de $\mathcal{R}$ de grado d*, y a los elementos pertenecientes a $\mathcal{R}_d$ se les denomina *elementos homogéneos de grado d*. Es claro que debido a la descomposición en suma directa, todo elemento de $\mathcal{R}$ se podrá escribir como $a = a_r + ... + a_s$ donde $a_i \in \mathcal{R}_i$ no nulos. A los elementos a_i se les conoce como *componentes homogéneas de a*.

El anillo graduado con el que trabajaremos a lo largo del documento es el anillo de polinomios $\mathcal{S} := \mathbb{K}[X_1, ..., X_n]$, donde $\mathbb{K}$ denota un cuerpo algebraicamente cerrado. $\mathcal{S}$ tiene estructura de anillo graduado si tomamos $\mathcal{S}_d$ como el conjunto de polinomios homogéneos de grado d.

Definición 1.2 (Ideal homogéneo) *Un ideal homogéneo de un anillo graduado $\mathcal{R}$ es un ideal $\mathfrak{a} \subset \mathcal{R}$ tal que para todo $a \in \mathfrak{a}$ se tiene que todas sus componentes homogéneas están en $\mathfrak{a}$. Nótese que esto es equivalente a decir que $\mathfrak{a}$ es homogéneo si admite una descomposición de la forma $\mathfrak{a} = \bigoplus_{d\geq 0}(\mathfrak{a} \cap \mathcal{R}_d)$.*

Esta definición de ideal homogéneo a su vez es equivalente a afirmar que un ideal es homogéneo si y solo si está generado por elementos homogéneos.

Lema 1.3 *Un ideal $\mathfrak{a}$ de un anillo graduado $\mathcal{R}$ es un ideal homogéneo si y solo si está generado por elementos homogéneos.*

Demostración: Si $\mathfrak{a}$ es un ideal homogéneo, entonces $\mathfrak{a} = \bigoplus_{d\geq 0}(\mathfrak{a} \cap \mathcal{R}_d)$ y directamente se tiene que que $\mathfrak{a}$ está generado por $\bigcup_{d\geq 0}(\mathfrak{a} \cap \mathcal{R}_d)$.

Recíprocamente, si tenemos que $\mathfrak{a} = \langle \bigcup_{d\in D} H_d \mid D \subseteq \mathbb{N} \text{ y } H_d \subseteq \mathcal{R}_d \rangle$ entonces un elemento de $a \in \mathfrak{a}$ se puede escribir como $a = \sum_{d\in D} \sum_{i=1}^{r_d} g^{di} a_d^i$ donde $g^{di} \in \mathcal{R}$, $a_d^i \in H_d$. Nótse que permitimos que algunos de los g^{di} sean nulos, pues solo consideramos combinaciones finitas. Descomponiendo los g^{di} en sus componentes homogéneas y teniendo en cuenta la compatibilidad del producto con la estructura de anillo graduado de $\mathcal{R}$, concluimos que $a \in \bigoplus_{d\geq 0}(\mathfrak{a} \cap \mathcal{R}_d)$, por lo que tenemos los siguientes contenidos:

$$\bigoplus_{d\geq 0}(\mathfrak{a} \cap \mathcal{R}_d) \subseteq \mathfrak{a} \subseteq \bigoplus_{d\geq 0}(\mathfrak{a} \cap \mathcal{R}_d)$$

donde el primer contenido es trivial. Los contenidos entonces son igualdades y concluimos así que $\mathfrak{a}$ es un ideal homogéneo.

■

Una construcción importante es la del cociente $\mathcal{R}/\mathfrak{a}$ cuando $\mathcal{R}$ es un anillo graduado y $\mathfrak{a}$ es un ideal homogéneo. Tenemos entonces la siguiente proposición [5].

Proposición 1.4 *Si $\mathcal{R}$ es un anillo graduado y $\mathfrak{a} \subset \mathcal{R}$ es un ideal homogéneo entonces $\mathcal{R}/\mathfrak{a}$ tiene estructura de anillo graduado.*

Demostración: Si llamamos $\mathfrak{a}_d := \mathfrak{a} \cap \mathcal{R}_d$ es claro que siempre podemos definir el grupo aditivo $\mathcal{R}_d/\mathfrak{a}_d$, puesto que $\mathfrak{a}_d \lhd \mathcal{R}_d$ como grupos. Así, la suma directa $\bigoplus_{d\geq 0} \mathcal{R}_d/\mathfrak{a}_d$ tiene estructura de anillo definiendo la suma componente a componente y el producto como $[(a_r + \mathfrak{a}_r) + ... + (a_s + \mathfrak{a}_s)][(b_p + \mathfrak{a}_p) + ... + (b_q + \mathfrak{a}_q)] := \sum_{i,j}(a_i b_j + \mathfrak{a}_{i+j})$, la cual está bien definida por ser $\mathcal{R}$ un anillo graduado. Es más, la suma directa adquiere estructura de anillo graduado de esta forma. Sea la aplicación $\phi : \mathcal{R} \to \bigoplus_{d\geq 0} \mathcal{R}_d/\mathfrak{a}_d$ que manda cada $a = a_r + ... + a_s \mapsto (a_r + \mathfrak{a}_r) + ... + (a_s + \mathfrak{a}_s)$. Dicha aplicación es un claro epimorfismo, y además su núcleo es $\mathfrak{a}$, puesto que $\phi(a) = 0 \Leftrightarrow a_i \in \mathfrak{a}_i \Leftrightarrow a \in \mathfrak{a}$.

Por el Primer Teorema de Isomorfía de anillos concluimos que $\mathcal{R}/\mathfrak{a} \cong \bigoplus_{d\geq 0} \mathcal{R}_d/\mathfrak{a}_d$.

■

1.2. Descomposición primaria de ideales

En esta sección introducimos la noción de ideal primario y de descomposición primaria de ideales homogéneos, la cual será fundamental a la hora de definir la multiplicidad de intersección de curvas planas. Comenzamos introduciendo el concepto de *ideal primario* para el caso general de un anillo $\mathcal{R}$ y posteriormente probamos la existencia de la descomposición primaria de ideales homogéneos para el anillo de polinomios $\mathcal{S}$. En pocas palabras, comprobamos que todas estas herramientas algebraicas funcionan igual que en el caso general, pero añadiendo el apellido "homogéneo". Concluimos la sección definiendo el concepto de *saturación de un ideal*.

Definición 1.5 (Ideal primario) *Dado un ideal $\mathfrak{a}$ de un anillo $\mathcal{R}$, decimos que es primario si para cada par de elementos $a, b \in \mathcal{R}$ tales que $ab \in \mathfrak{a}$, o bien $a \in \mathfrak{a}$ o bien $b \in \sqrt{\mathfrak{a}}$. Si denotamos $\mathfrak{p} := \sqrt{\mathfrak{a}}$, entonces se dice que $\mathfrak{a}$ es un ideal $\mathfrak{p}$-primario.*

Nótese que hemos denotado $\mathfrak{p}$ a $\sqrt{\mathfrak{a}}$ puesto que los radicales de ideales son ideales primos. Una propiedad importante de los ideales primarios es la siguiente:

Lema 1.6 *Si* $\mathfrak{a} = \cap_{i=1}^{r} \mathfrak{b}_i$ *tales que* $\mathfrak{b}_i$ *son ideales* $\mathfrak{p}$*-rimarios, entonces* $\mathfrak{a}$ *es* $\mathfrak{p}$*-primario.*

Demostración: Por un lado, por las propiedades de los radicales de ideales (véase [3]), $\sqrt{\mathfrak{a}} = \sqrt{\cap_{i=1}^{r} \mathfrak{b}_i} = \cap_{i=1}^{r} \sqrt{\mathfrak{b}_i} = \cap_{i=1}^{r} \mathfrak{p} = \mathfrak{p}$. Además, si tomamos $a, b \in \mathcal{R}$ tal que $ab \in \mathfrak{a}$, si $a \notin \mathfrak{a}$ entonces existe algún i tal que $a \notin \mathfrak{b}_i$. Pero en ese caso $b \in \sqrt{\mathfrak{b}_i} = \mathfrak{p} = \sqrt{\mathfrak{a}}$, por lo que $\mathfrak{a}$ es $\mathfrak{p}$-primario.

■

Los ideales homogéneos se comportan bien con respecto a la definición de ideal primario de la siguiente manera [5].

Lema 1.7 *Sea* $\mathcal{R}$ *un anillo graduado y* $\mathfrak{a}$ *un ideal homogéneo. Dicho ideal es primario si y solo si para cualesquiera elementos homogéneos* $a, b \in \mathcal{R}$ *tales que* $ab \in \mathfrak{a}$ *se tiene que o bien* $a \in \mathfrak{a}$ *o bien* $b \in \sqrt{\mathfrak{a}}$*.*

Demostración: Por un lado la implicación [$\Rightarrow$] se tiene directamente por la definición de ideal primario. Para ver la otra implicación, tomamos $a, b \in \mathcal{R}$ y escribimos sus componentes homogéneas $a = a_r + ... + a_s$ y $b = b_p + ... + b_q$. Supongamos que $ab \in \mathfrak{a}$ y que $a \notin \mathfrak{a}$. Entonces existe alguna componente homogénea a_i que no está en $\mathfrak{a}$. Sea a_d la componente homogénea de menor grado tal que $a_d \notin \mathfrak{a}$. Como $ab \in \mathfrak{a}$, esto implica que $(a_d + ... + a_s)(b_p + ... + b_q) \in \mathfrak{a}$, al igual que todas sus componentes homogéneas. La componente homogénea de menor grado de dicho producto es $a_d b_p$, y como $a_d b_p \in \mathfrak{a}$ y $a_d \notin \mathfrak{a}$, entonces $b_p \in \sqrt{\mathfrak{a}}$ por hipótesis. Consecuentemente, el conjunto $\{n \in \mathbb{N} \mid ab_p^n \in \mathfrak{a}\}$ es no vacío, así que tendrá un elemento mínimo $m \geq 1$. Denotemos $a' = ab_p^{m-1} \notin \mathfrak{a}$. Por construcción, $a'b \in \mathfrak{a}$, lo que implica que $a'(b_{p+1} + ... + b_q) \in \mathfrak{a}$. Volvemos a aplicar el mismo argumento sobre a' y $(b_{p+1} + ... + b_q)$ para concluir que $b_i \in \sqrt{\mathfrak{a}}$ para todo $i = p, ..., q$, con lo que $b \in \sqrt{\mathfrak{a}}$ y por tanto $\mathfrak{a}$ es primario.

■

Una demostración similar permite caracterizar a los ideales homogéneos primos; un ideal homogéneo $\mathfrak{a}$ de un anillo graduado $\mathcal{R}$ es primo si y solo si para cada par de elementos homogéneos $a, b \in \mathcal{R}$ tal que $ab \in \mathfrak{a}$ se tiene que o bien $a \in \mathfrak{a}$ o bien $b \in \mathfrak{a}$. Otro concepto importante es el de ideal homogéneo irreducible:

Definición 1.8 (Ideal homogéneo irreducible) *Un ideal homogéneo* $\mathfrak{a}$ *de un anillo graduado* $\mathcal{R}$ *es irreducible si no puede expresarse como intersección no trivial de dos ideales homogéneos.*

Para el caso concreto del anillos graduados noetherianos tenemos siempre que todo ideal homogéneo admite una descomposición en ideales primarios. En este trabajo especificamos el resultado para el anillo de polinomios $\mathcal{S}$, aunque la misma demostración vale para un anillo graduado noetheriano general. Recordemos que un anillo $\mathcal{R}$ se dice que es noetheriano si cumple una de estas tres propiedades [3]:

1. Todo conjunto no vacío de ideales de $\mathcal{R}$ tiene un elemento maximal.
2. Toda cadena ascendente de ideales en $\mathcal{R}$ estaciona.
3. Todo ideal de $\mathcal{R}$ es finitamente generado.

Para evitar confusiones denotamos a los ideales de $\mathcal{S}$ con letras latinas $I, J, ...$ Antes de probar el resultado, necesitamos dos lemas previos. Todo este desarrollo se puede encontrar en [2].

Lema 1.9 *Todo ideal homogéneo de $\mathcal{S}$ se puede escribir como intersección finita de ideales homogéneos irreducibles.*

Demostración: Usaremos fuertemente que $\mathcal{S}$ es noetheriano. Sea $I \subset \mathcal{S}$ un ideal homogéneo y supongamos que no es intersección finita de ideales homogéneos irreducibles. En particular, I no es irreducible, luego existen $I_1, J_1 \subset \mathcal{S}$ ideales homogéneos tales que $I = I_1 \cap J_1$ e $I \subset I_1$, $I \subset J_1$ (nótese los contenidos estrictos). Por hipótesis sobre I, alguno de los dos ideales no es intersección finita de ideales homogéneos irreducibles. Sea I_1 dicho ideal. Volvemos a aplicar el mismo argumento a I_1 y recursivamente encontraremos una cadena $I \subset I_1 \subset I_2 ...$ que no estaciona, lo que entra en contradicción con que $\mathcal{S}$ sea noetheriano.

■

Lema 1.10 *Si I es un ideal homogéneo irreducible, entonces es primario.*

Demostración: Sea I un ideal homogéneo irreducible, y supongamos que tenemos dos elementos homogéneos $F, G \in \mathcal{S}$ tales que $FG \in I$. Para cada m consideramos el ideal $I_m := \{H \in \mathcal{S} \mid HF^m \in I\}$. Dado que tenemos una cadena $I \subset I_1 \subset I_2 ...$ y $\mathcal{S}$ es noetheriano, existe un n tal que $I_n = I_{n+1}$. Afirmamos entonces que $I = (\langle F^n \rangle + I) \cap I_1$. El contenido $[\subseteq]$ es trivial. Para ver $[\supseteq]$, tomamos $H \in (\langle F^n \rangle + I) \cap I_1$. en particular, $HF \in I$ y además $H = AF^n + B$ con $A \in \mathcal{S}$ y $B \in I$. Si multiplicamos la última igualdad por F tenemos que $AF^{n+1} = HF - BF \in I$. Así, $A \in I_{n+1} = I_n$, por lo que $AF^n \in I$ y por tanto $H = AF^n + B \in I$.

La descomposición $I = (\langle F^n \rangle + I) \cap I_1$ junto con la hipótesis de irreducibilidad implica que o bien $I = \langle F^n \rangle + I$ (con lo que $F^n \in I$ y por tanto $F \in \sqrt{I}$) o bien $I = I_1$ (y por tanto $G \in I$, puesto que por hipótesis $G \in I_1$). Por el Lema 1.7 concluimos que I es primario.

■

Finalmente probamos el Teorema de descomposición primaria de ideales homogéneos.

Teorema 1.11 (De descomposición primaria) *Todo ideal homogéneo I de $\mathcal{S}$ puede ser escrito como $I = I_1 \cap ... \cap I_s$ donde cada I_i es primario, los radicales $\sqrt{I_i}$ son distintos entre sí e $I_i \not\supset \cap_{i \neq j} I_j$. Además, los ideales primarios de la descomposición cuyo radical sea minimal en el conjunto $\{\sqrt{I_1}, ..., \sqrt{I_s}\}$ están unívocamente determinados por I, de tal forma que aparecen en toda descomposición como la descrita.*

Demostración: Es claro de los Lemas 1.9 y 1.10 que I puede ser escrito como una intersección finita de ideales primarios. Eliminando de la descomposición aquellos ideales primarios que contengan a la intersección de los otros podemos suponer que $I_i \not\supset \cap_{i \neq j} I_j$. Además, por el Lema 1.6, podemos asumir que todos los radicales de los ideales primarios de la descomposición son distintos. Solo nos falta probar la unicidad.

Supongamos que tenemos dos descomposiciones $I = I_1 \cap ... \cap I_s$ e $I = I'_1 \cap ... \cap I'_r$ como las del enunciado. Supongamos que $\sqrt{I_\ell}$ es mínima entre $\{\sqrt{I_1}, ..., \sqrt{I_s}\}$. Entonces, como $I_\ell \not\supset \cap_{\ell \neq j} I_j$, se tiene que $\sqrt{I_\ell} \not\supset \cap_{\ell \neq j} \sqrt{I_j}$. Así, podemos tomar $F \in \cap_{\ell \neq j} \sqrt{I_j}$ que no pertenezca a $\sqrt{I_\ell}$. Como $F \notin \sqrt{I} = \cap_i \sqrt{I'_i}$ podemos encontrar k tal que $F \notin \sqrt{I'_k}$ y podemos elegir dicho $\sqrt{I'_k}$ minimal entre $\{\sqrt{I'_1}, ..., \sqrt{I'_r}\}$. Veamos que $I_\ell \subset I'_k$. En efecto, tomamos $G \in I_\ell$. Como existe m tal que $F^m \in \cap_{\ell \neq j} I_j$ entonces $F^m G$ pertenece a $I = I'_1 \cap ... \cap I'_r$, y en particular $F^m G \in I'_k$. Pero $F^m \notin I'_k$ y

por tanto $G \in I'_k$ por ser I'_k primario. Tenemos así la inclusión $I_\ell \subseteq I'_k$. La otra inclusión se prueba de forma simétrica por minimalidad, lo que implica que $I_\ell = I'_k$ tal y como queríamos probar.

■

Este tipo de descomposición primaria se denomina *descomposición primaria irredundante de* I. Los radicales de las componentes primarias se denominan *primos asociados de* I y las componentes primarias cuyos radicales no son minimales se denominan *componentes inmersas de* I.

Definición 1.12 (Componentes irrelevante) *Dado un ideal homogéneo* $I \subset \mathcal{S}$*, se denomina componente irrelevante de una descomposición primaria irredundante de* I *a la componente* $\langle X_1, ..., X_n\rangle$*-primaria de dicha descomposición (en caso de que exista). Al ideal* $\mathfrak{M} := \langle X_1, ..., X_n\rangle$ *se le suele denominar ideal irrelevante en ciertos contextos.*

Hay que notar que en una descomposición irredundante hay, a lo sumo, una componente irrelevante. Dicho nombre tendrá sentido cuando hablemos de las variedades proyectivas en el siguiente capítulo.

Definición 1.13 (Saturación de un ideal) *Dado un ideal homogéneo* $I \subset \mathcal{S}$ *definimos la saturación de* I *como el ideal homogéneo* $\mathrm{Sat}(I) := \{F \in \mathcal{S} \mid \exists\, k \in \mathbb{N} \text{ tal que } X_i^k F \in I \ \forall\ i = 0, ..., n\}$. *Un ideal homogéneo es saturado si coincide con su saturación.*

La clave de la saturación de un ideal es que nos permite eliminar las contribuciones de las componentes irrelevantes al ideal, tal y como se muestra en la siguiente proposición:

Proposición 1.14 *Sea* $I \subset \mathcal{S}$ *un ideal homogéneo y* J *la intersección de las componentes no irrelevantes de una descomposición primaria irredundante de* I*. Entonces se cumplen las siguientes afirmaciones:*

1. $\mathrm{Sat}(I) = J$
2. *Para* $\ell \in \mathbb{N}$ *lo suficientemente grande se tiene que* $I \cap \mathcal{S}_\ell = \mathrm{Sat}(I) \cap \mathcal{S}_\ell$.

Demostración: (1.) Tomamos $F \in J$. Si la descomposición primaria no tiene componente irrelevante, entonces $F \in J = I \subset \mathrm{Sat}(I)$ y no hay nada que probar. Si por el contrario sí que tenemos componente irrelevante, entonces la denotamos por I_0 de tal forma que $I = I_0 \cap J$. Como $\sqrt{I_0} = \mathfrak{M}$, existe $k \in \mathbb{N}$ tal que $X_j^k \in I_0$ para todo $j = 1, ..., n$. Pero entonces $X_j^k F \in I_0 J \subseteq I_0 \cap J = I$. Así, $F \in \mathrm{Sat}(I)$. Para probar el otro contenido, tomamos $F \in \mathrm{Sat}(I)$ y escribimos $J = I_1 \cap ... \cap I_r$ donde I_i son las componentes primarias no irrelevantes de la descomposición irredundante de I. Como los I_i no son irrelevantes, existe $X_{j_i} \notin \sqrt{I_i}$. Pero como $X_{j_i}^k F \in I \subset I_i$ e I_i es primario, entonces $F \in I_i$ para $i = 1, ..., r$, por lo que $F \in J$.

(2.) Tomamos $\{F_1, ..., F_r\}$ una familia de generadores homogéneos de $\mathrm{Sat}(I)$ (siempre lo podemos hacer por ser $\mathcal{S}$ noetheriano y por ser $\mathrm{Sat}(I)$ un ideal homogéneo) Así, existe $k \in \mathbb{N}$ tal que $X_j^k F_i \in I$ para todo $j = 1, .., n$ e $i = 1, ..., r$. Por tanto, cualquier polinomio homogéneo G de grado al menos $(n+1)k$ cumple que $GF_i \in I$ para cada $i = 1, ..., r$. Consecuentemente, si tenemos un polinomio homogéneo $H = F_1G_1 + ... + F_rG_r \in \mathrm{Sat}(I)$ de grado $\ell \geq \ell_0 = (n+1)k + \max\{\deg(F_1), ..., \deg(F_r)\}$ necesariamente $H \in I$. Hemos probado que $I \cap \mathcal{S}_\ell \supseteq \mathrm{Sat}(I) \cap \mathcal{S}_\ell$. Como $I \subseteq \mathrm{Sat}(I)$ se tiene siempre, tenemos la igualdad. ■

Para finalizar la sección enunciamos y demostramos el siguiente lema [2], en el cual estudiamos cuándo un ideal generado por dos polinomios es saturado en el caso bidimensional. Este lema nos facilitará las demostraciones en los siguientes capítulos cuando trabajemos con curvas planas.

Lema 1.15 *Sean $F, G \in \mathbb{K}[X_0, X_1, X_2]$ dos polinomios homogéneos coprimos de grado positivo. Entonces el ideal $I = \langle F, G\rangle$ es saturado.*

Demostración: Puesto que $I_\ell = \mathrm{Sat}(I)_\ell$ para $\ell \gg 0$ por la Proposición 1.14, es suficiente probar la igualdad $I_{\ell-1} = \mathrm{Sat}(I)_{\ell-1}$ para un ℓ tal que $I_\ell = \mathrm{Sat}(I)_\ell$. Sea $H \in \mathrm{Sat}(I)_{\ell-1}$. Queremos ver que $H \in \langle F, G\rangle$. Dado que $X_i H \in \mathrm{Sat}(I)_\ell = I_\ell$, podemos escribir

$$\begin{cases} X_0H = A_0F + B_0G \\ X_1H = A_1F + B_1G \\ X_2H = A_2F + B_2G \end{cases} \tag{1.1}$$

donde $A_i, B_i \in \mathbb{K}[X_0, X_1, X_2]$. Si eliminamos H de las igualdades:

$$\begin{cases} X_1(A_0F + B_0G) = X_0(A_1F + B_1G) \\ X_2(A_0F + B_0G) = X_0(A_2F + B_2G) \\ X_2(A_1F + B_1G) = X_1(A_2F + B_2G) \end{cases}$$

Podemos reordenar entonces las igualdades anteriores:

$$\begin{cases} F(A_0X_1 - A_1X_0) = G(B_1X_0 - B_0X_1) \\ F(A_0X_2 - A_2X_0) = G(B_2X_0 - B_0X_2) \\ F(A_1X_2 - A_2X_1) = G(B_2X_1 - B_1X_2) \end{cases}$$

La coprimalidad de F, G implica la existencia de polinomios C_0, C_1, C_2 tales que

$$\begin{cases} A_0X_1 - A_1X_0 = C_2G & B_1X_0 - B_0X_1 = C_2F \\ A_0X_2 - A_2X_0 = C_1G & B_2X_0 - B_0X_2 = C_1F \\ A_1X_2 - A_2X_1 = C_0G & B_2X_1 - B_1X_2 = C_0F \end{cases} \tag{1.2}$$

y además $C_0X_0 - C_1X_1 + C_2X_2 = 0$. De esta última igualdad se deriva que $C_0X_0 \in \langle X_1, X_2\rangle$. Como $\langle X_1, X_2\rangle$ es primo y $X_0 \notin \langle X_1, X_2\rangle$, entonces $C_0 \in \langle X_1, X_2\rangle$, por lo que existen D_2, D_1 tales que:

$$C_0 = D_2X_1 - D_1X_2$$

Consecuentemente, tenemos que $(D_2X_1 - D_1X_2)X_0 - C_1X_1 + C_2X_2 = 0$ que reorganizando se escribe como $(D_2X_0 - C_1)X_1 = (D_1X_0 - C_2)X_2$. La coprimalidad de X_1 y X_2 implica entonces la existencia de D_0 tal que:

$$\begin{cases} D_2X_0 - C_1 = D_0X_2 \Rightarrow C_1 = D_2X_0 - D_0X_2 \\ D_1X_0 - C_2 = D_0X_1 \Rightarrow C_2 = D_1X_0 - D_0X_1 \end{cases}$$

Sustituyendo en la primera fila de (1.2):

$$A_0X_1 - A_1X_0 = (D_1X_0 - D_0X_1)G$$

$$B_1X_0 - B_0X_1 = (D_1X_0 - D_0X_1)F$$

Moviendo los términos con X_0 a un lado y los términos con X_1 al otro, dado que X_0 no divide a X_1 podemos asumir la existencia de A, B tales que:

$$A_0 + D_0G = AX_0 \qquad B_0 - D_0F = BX_0$$

Y sustituyendo en la primera fila de (1.1):

$$X_0H = (AX_0 - D_0G)F + (BX_0 + D_0F)G = AFX_0 + BGX_0$$

Por lo que $H = AF + BG$ y por tanto $H \in \langle F, G\rangle$.

■

1.3. Sucesiones graduadas

Para el correcto desarrollo del Capítulo 4 es recomendable mencionar ciertos resultados clásicos relacionados con sucesiones graduadas.

Lema 1.16 *Sea $\mathcal{R}$ un anillo conmutativo y $\mathcal{M}$, $\mathcal{N}$ dos $\mathcal{R}$-módulos con $h : \mathcal{M} \to \mathcal{N}$ un morfismo entre ellos. Entonces la sucesión*

$$0 \to \ker(h) \overset{i}{\hookrightarrow} \mathcal{M} \overset{h}{\longrightarrow} \mathcal{N} \overset{p}{\longrightarrow} \operatorname{coker}(h) \to 0$$

es exacta.

Demostración: Es una comprobación directa teniendo en cuenta que $\operatorname{coker}(h) = \mathcal{N}/\operatorname{im}(h)$ y que la inclusión i es un monomorfismo y el cociente p es un epimorfismo.

■

Lema 1.17 *Si tenemos la siguiente sucesión exacta de espacios vectoriales de dimensión finita:*

$$0 \to V_1 \to V_2 \to ... \to V_r \to 0$$

entonces se cumple que $\sum_{i=1}^{r}(-1)^i \dim V_i = 0$.

Demostración: Si denotamos h_i a los morfismos que van de V_i a V_{i+1}, entonces por el Teorema de Rango-Nulidad de Álgebra Lineal y la exactitud de la sucesión:

$$\dim V_i = \dim \ker(h_i) + \dim \operatorname{im}(h_i) = \dim \ker(h_i) + \dim \ker(h_{i+1})$$

de esta forma, si aplicamos la exactitud de la sucesión

$$\sum_{i=1}^{r}(-1)^i \dim V_i = \sum_{i=1}^{r}(-1)^i \dim \ker(h_i) + \sum_{i=1}^{r}(-1)^i \dim \ker(h_{i+1}) =$$

$$= (-1)\dim \ker(h_1) + \sum_{i=1}^{r-1}[(-1)^{i+1} + (-1)^i]\dim \ker(h_{i+1}) + (-1)^r \dim \ker(h_{r+1}) = 0$$

■

Finalmente enunciamos también el conocido como Lema de la serpiente, que se puede ver en [3].

Lema 1.18 (De la serpiente) *Consideremos el siguiente diagrama, donde todos los objetos son módulos sobre un anillo $\mathcal{R}$:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{M} & \xrightarrow{h_1} & \mathcal{N} & \xrightarrow{h_2} & \mathcal{P} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & \mathcal{M}' & \xrightarrow{h_1'} & \mathcal{N}' & \xrightarrow{h_2'} & \mathcal{P}' & \longrightarrow & 0 \end{array}$$

de tal forma que las dos filas son exactas y los cuadrados son conmutativos (i.e. $\beta \circ h_1 = h_1' \circ \alpha$ *y* $\gamma \circ h_2 = h_2' \circ \beta$*) Entonces la sucesión siguiente*

$$0 \to \ker(\alpha) \to \ker(\beta) \to \ker(\gamma) \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta) \to \operatorname{coker}(\gamma) \to 0$$

está bien definida y es exacta.

Completamos aquí nuestro repaso de álgebra conmutativa necesario para desarrollar el resto del trabajo. En el próximo capítulo definiremos las variedades proyectivas y sus relaciones con los ideales homogéneos de $\mathcal{S}$.

Capítulo 2

Conjuntos proyectivos y sus ideales

A lo largo de este capítulo y para lo que queda de trabajo vamos a trabajar siempre con el anillo graduado $\mathcal{S} = \mathbb{K}[X_0, ..., X_n]$ donde $\mathbb{K}$ es un cuerpo algebraicamente cerrado. Además, denotamos $\mathbb{P}^n$ al espacio proyectivo de dimensión n formado por las rectas sobre el espacio vectorial $\mathbb{K}^{n+1}$. Los puntos de $\mathbb{P}^n$ los escribimos como $p = [p_0 : ... : p_n]$ con alguno de los p_i no nulos.

Recordemos que los únicos polinomios $F \in \mathcal{S}$ para los cuales tiene sentido definir el conjunto de puntos proyectivos p tales que $F(p) = 0$ son los polinomios homogéneos, tal y como se vio en la asignatura de Curvas Algebraicas [1]. Esto fomenta la siguiente definición:

Definición 2.1 (Conjunto proyectivo) *Un conjunto proyectivo $X \subset \mathbb{P}^n$ es un subconjunto del espacio proyectivo para el cual existe una familia de polinomios homogéneos $\{F_j\}_{j \in J}$ tal que $X = \{p \in \mathbb{P}^n \mid F_j(p) = 0 \; \forall \; j \in J\}$.*

Además, por motivos prácticos, diremos que $F \in \mathcal{S}$ arbitrario se anula en $p \in \mathbb{P}^n$ si $F_i(p) = 0$ donde $F = F_r + ... + F_s$ y los F_i son las componentes homogéneas de grado i de F. Podemos definir entonces el siguiente concepto:

Definición 2.2 (Conjunto proyectivo de una familia de polinomios) *Dado un subconjunto $T \subset \mathcal{S}$, definimos el conjunto proyectivo dado por T como $V(T) = \{p \in \mathbb{P}^n \mid F(p) = 0 \; \forall \; F \in T\}$. Nótese que $V(T)$ es un conjunto proyectivo puesto que se define como los puntos donde se anulan las componentes homogéneas de los polinomios de T.*

Hay que notar que $V(T) = V(\langle T \rangle)$, donde $\langle T \rangle$ es el ideal generado por T. Es más, como podemos ver T como un subconjunto de polinomios homogéneos, $\langle T \rangle$ es un ideal homogéneo y además finitamente generado por ser $\mathcal{S}$ un anillo noetheriano. Por tanto, en la práctica siempre trabajaremos con $V(\langle F_1, ..., F_r \rangle) = V(F_1, ..., F_r)$ donde los F_i son polinomios homogéneos. Tenemos también la definición dual:

Definición 2.3 (Ideal de un conjunto proyectivo) *Dado un conjunto proyectivo X, definimos el ideal homogéneo de X como $I(X) = \{F \in \mathcal{S} \mid F(p) = 0 \; \forall \; p \in X\}$. Está claro que*

$I(X)$ es un ideal de $\mathcal{S}$ y que además es homogéneo por el comentario posterior a la Definición 2.1.

Hay que notar que $I(X)$ es siempre un ideal radical. En efecto, si $F \in \sqrt{I(X)}$, entonces $F^a(p) = 0$ para todo $p \in X$ y para cierto $a \in \mathbb{N}$. Pero entonces, por ser $\mathbb{K}$ un cuerpo, $F(p) = 0$ y por tanto $F \in I(X)$. Para completar esta parte de definiciones, definimos el anillo graduado de un conjunto proyectivo:

Definición 2.4 (Anillo graduado de un conjunto proyectivo) *Dado un conjunto proyectivo X, definimos el anillo graduado de X como el anillo $\mathcal{S}(X) := \mathcal{S}/I(X)$. Es graduado por la Proposición 1.4, ya que el ideal $I(X)$ es homogéneo.*

Es claro que hay una firme relación entre ideales homogéneos y conjuntos proyectivos. En una situación ideal, nos gustaría que hubiera una biyección entre estos dos conceptos:

$$\text{¿ Ideales homogéneos de } \mathcal{S} \iff \text{Conjuntos proyectivos de } \mathbb{P}^n \text{ ?}$$

Así, si partimos de un conjunto proyectivo X, debería satisfacerse que $V(I(X)) = X$. Y de la misma forma, si partimos de un ideal homogéneo J debería satisfacerse $I(V(J)) = J$. Si bien la primera afirmación sí que es cierta y es una simple comprobación rutinaria, la segunda no siempre se cumple (solo se tiene asegurado el contenido $J \subseteq I(V(J))$). Por ejemplo, si consideramos $J = \langle X_1^2, ..., X_n^2 \rangle$, es claro que $V(J) = (1 : 0 : ... : 0)$, pero $I(V(J)) = \langle X_1, ..., X_n \rangle \neq J$. Para que nuestro diccionario álgebra-geometría funcione correctamente, debemos considerar ideales homogéneos radicales de $\mathcal{S}$, puesto que el *Teorema de los ceros de Hilbert proyectivo* afirma que $I(V(J)) = \sqrt{J}$ (siempre y cuando $V(J)$ no sea el conjunto vacío). Así, la correspondencia real:

$$\textbf{Ideales homogéneos radicales de } \mathcal{S} \iff \textbf{Conjuntos proyectivos de } \mathbb{P}^n$$

Observación 2.5 *La presencia de ideales radicales no debe asustarnos, pues es la generalización del concepto de ecuación minimal para el caso de curvas planas en $\mathbb{P}^2$. De esta forma, si $C = V(F)$ es una curva plana proyectiva, F es una ecuación minimal suya si y solo si $I(C) = \langle F \rangle$.*

Para el caso proyectivo, que es el que nos concierne, no es válida la demostración estándar del Teorema de los ceros de Hilbert, ya que, a diferencia del espacio afín, el conjunto vacío en el espacio proyectivo se logra de dos formas distintas: $V(\mathcal{S}) = V(\mathfrak{M}) = \emptyset$ donde recordemos que $\mathfrak{M} := \langle X_0, ..., X_n \rangle$ es el conocido como ideal irrelevante. Por ello, ahora vamos a dar una versión débil del Teorema de los ceros de Hilbert [2] y, tras desarrollar el polinomio de Hilbert, daremos la demostración completa.

Teorema 2.6 (Débil de los ceros de Hilbert) *Sea I un ideal homogéneo de $\mathcal{S} = \mathbb{K}[X_0, ..., X_n]$ con $\mathbb{K}$ algebraicamente cerrado. Entonces $V(I) = \emptyset$ si y solo si $\mathfrak{M} \subseteq \sqrt{I}$ (i.e. $\sqrt{I} = \mathfrak{M}$ o $\sqrt{I} = \mathcal{S}$)*

Demostración: La implicación [$\Leftarrow$] es directa, puesto que si $\mathfrak{M} \subseteq \sqrt{I}$, entonces $X_i^{r_i} \in I$ para todo $i = 0, ..., n$ y para ciertos $r_i \in \mathbb{N}$, lo que implica directamente que $V(I) = \emptyset$. Probemos ahora [$\Rightarrow$] por inducción en el número de variables n. Si $n = 0$, supongamos que $\mathfrak{M} \not\subset \sqrt{I}$. Entonces $X_0^d \notin I$ para todo $d \geq 1$. Como I es homogéneo, entonces $I = \langle 0 \rangle$, por lo que $V(I) = \mathbb{P}^0 \neq \emptyset$.

Consideremos ahora $n > 0$ y supongamos que $\mathfrak{M} \not\subset \sqrt{I}$. Consecuentemente, $X_i^d \notin I$ para todo $d \in \mathbb{N}$ y para cierto $i \in \{0, ..., n\}$ el cual podemos suponer que es $i = 0$ sin pérdida de generalidad. Sea $I' = I \cap \mathbb{K}[X_0, ..., X_{n-1}]$ otro ideal, también homogéneo. Por hipótesis de inducción, como $X_0^d \notin I'$, entonces existe $(a_0, ..., a_{n-1}) \in \mathbb{K}^n \setminus (0, ..., 0)$ tal que $F(a_0, ..., a_{n-1}) = 0$ para todo $F \in I'$. Consideramos ahora el ideal $J = \{F(a_0, ..., a_{n-1}, X_n) \mid F \in I\}$, el cual no es necesariamente homogéneo.

Veamos que $J \neq \mathbb{K}[X_n]$. En caso contrario, existiría $F \in I$ tal que $F(a_0, ..., a_{n-1}, X_n) = 1$. Entonces, podríamos escribir $F = A_0 + A_1X_n + ... + A_dX_n^d$ con $A_i \in \mathbb{K}[X_0, ..., X_{n-1}]$ y tal que $A_1(a_0, ..., a_{n-1}) = ... = A_d(a_0, ..., a_{n-1}) = 0$ pero $A_0(a_0, ..., a_{n-1}) \neq 0$. Además, siempre podemos asumir que $(0 : ... : 0 : 1) \notin V(I)$ (si estuviera entonces no habría nada que probar), lo que nos permite encontrar un polinomio homogéneo $G \in I$ mónico en la variable X_n, i.e. $G = B_0 + B_1X_n + ... + B_{e-1}X_n^{e-1} + X_n^e$ con los $B_j \in \mathbb{K}[X_0, ..., X_{n-1}]$.

Si calculamos ahora la resultante de F, G con respecto a X_n, entonces (véase [4]) $res_{X_n}(F, G) \in \langle F, G\rangle \subseteq I'$. Atendiendo a la forma explícita de determinante de la resultante, se puede ver que cuando evaluamos $res_{X_n}(F, G)(a_0, ..., a_{n-1})$ obtenemos el determinante de una matriz triangular con diagonal todo $1's$, por lo que $res_{X_n}(F, G)(a_0, ..., a_{n-1}) = 1$, lo que contradice que $(a_0, ..., a_{n-1}) \in I'$. Es por ello por lo que $J \neq \mathbb{K}[X_n]$. Por ser J un ideal propio de $\mathbb{K}[X_n]$ y ser éste un DIP, existe $H \in \mathbb{K}[X_n]$ tal que $J = \langle H\rangle$. Al ser $\mathbb{K}$ algebraicamente cerrado, existe $a_n \in \mathbb{K}$ tal que $H(a_n) = 0$, por lo que $(a_0, ..., a_n) \in V(I)$, lo que completa la prueba.

■

2.1. Descomposición en conjuntos proyectivos irreducibles

Un tipo de conjunto proyectivo de gran importancia son los conjuntos proyectivos irreducibles, puesto que el Teorema de Bezóut y las definiciones de multiplicidad de intersección de curvas proyectivas planas van a requerir que dichas curvas sean irreducibles.

Definición 2.7 (Conjunto proyectivo irreducible) *Un conjunto proyectivo no vacío $X \subseteq \mathbb{P}^n$ se dice que es irreducible si dados dos conjuntos proyectivos $X_1, X_2 \subseteq \mathbb{P}^n$ tales que $X \subseteq X_1 \cup X_2$ se tiene que $X \subseteq X_1$ o $X \subseteq X_2$.*

Una propiedad muy buena de los conjuntos proyectivos irreducibles es que se pueden caracterizar a través de ideales homogéneos primos [5].

Proposición 2.8 *Un conjunto proyectivo X no vacío es irreducible si y solo si su ideal homogéneo $I(X)$ es un ideal primo.*

Demostración: Supongamos que X es irreducible. Tomamos dos polinomios $F, G \in \mathcal{S}$ tales que $FG \in I(X) \neq \mathcal{S}$ (esto último se tiene por ser X no vacío). Claramente $X \subseteq V(F) \cup V(G)$, por lo que por irreducibilidad $X \subseteq V(F)$ o $X \subseteq V(G)$, lo que es equivalente a que $F \in I(X)$ o $G \in I(X)$, lo que prueba que $I(X)$ es primo.

Recíprocamente, supongamos que $I(X)$ es primo y sea $X \subseteq X_1 \cup X_2$ tal que $X \not\subset X_1$ y $X \not\subset X_2$. Entonces $I(X_1) \not\subset I(X)$ ni $I(X_2) \not\subset I(X)$, por lo que podemos encontrar dos polinomios $F \in I(X_1)$,

$G \in I(X_2)$ tales que $F, G \notin I(X)$ pero que $FG \in I(X_1 \cup X_2) \subset I(X)$, lo que contradice la primalidad de $I(X)$.

■

El resultado fundamental de esta sección afirma que *todo conjunto proyectivo admite una descomposición en conjuntos proyectivos irreducibles.* Para probar esta afirmación, utilizaremos el Teorema 1.11 de descomposición primaria de ideales homogéneos [2], aunque una demostración algo más directa se puede lograr siguiendo los pasos del Lema 1.9.

Teorema 2.9 *Todo conjunto proyectivo $X \subseteq \mathbb{P}^n$ se puede descomponer de forma única como unión finita de conjuntos irreducibles, i.e. $X = X_1 \cup ... \cup X_r$ tales que $X_i \not\subset X_j$ si $i \neq j$.*

Demostración: Por el Teorema 1.11, $I(X)$ admite una descomposición primaria. Sea $I(X) = I_1 \cap ... \cap I_s$ dicha descomposición. Puesto que $I(X)$ es radical, podemos tomar radicales en la descomposición y por tanto suponer que $I_1, ..., I_s$ son radicales y por ello primos (los radicales de ideales primarios son ideales primos [3]). Eliminamos ideales redundantes para asumir $I_j \not\subset I_i$ para $i \neq j$. De esta forma, tomando $X_i := V(I_i)$ tenemos la descomposición buscada. En efecto, es claro que $X = V(I(X))) = V(I_1 \cap ... \cap I_s) = V(I_1) \cup ... \cup V(I_s) = X_1 \cup ... \cup X_s$ y que $X_j \not\subset X_i$ si $i \neq j$. Para ver la irreducibilidad de los X_i, dado que $I_i \subseteq I(V(I_i)) = I(X_i)$, entonces cada I_i satisface que $I(X_1) \cap ... \cap I(X_s) \subseteq I_i$, por lo que por primalidad existe X_j tal que $I(X_j) \subseteq I_i$. Pero $I_j \subseteq I(X_j)$, así que $i = j$ e $I(X_i) = I_i$, lo que hace que los X_i sean irreducibles.

Falta por ver la unicidad de la descomposición. Si $X = X_1' \cup ... \cup X_r'$ es otra descomposición en componentes irreducibles, $I(X) = I(X_1') \cap ... \cap I(X_r')$ es otra descomposición primaria de $I(X)$. Pero como todas las componentes primarias son primas y distintas entre sí, son minimales y por tanto la unicidad de los ideales contradice la existencia de dos descomposiciones distintas.

■

Hay que notar que, para probar que los X_i son irreducibles se podría haber aplicado el Teorema fuerte de los ceros de Hilbert, pero dado que no lo hemos demostrado aún, hemos decidido escribir una demostración que usa argumentos más básicos. Será en el siguiente capítulo cuando introduzcamos la herramienta fundamental de este trabajo: el polinomio de Hilbert.

Capítulo 3

El polinomio de Hilbert

3.1. Módulos graduados y sucesiones exactas graduadas

En esta sección introducimos brevemente el concepto de módulo graduado antes de estudiar la función de Hilbert y su relación con los conjutos proyectivos.

Definición 3.1 (Módulo graduado) *Si $\mathcal{R}$ es un anillo graduado, decimos que $\mathcal{M}$ es un $\mathcal{R}$-módulo graduado si es un módulo sobre $\mathcal{R}$ y si, como grupo aditivo, admite una descomposición del tipo $\mathcal{M} = \bigoplus_{\ell \geq 0} \mathcal{M}_\ell$, de tal forma que $\mathcal{R}_k \mathcal{M}_l \subseteq \mathcal{M}_{k+l}$. A cada $\mathcal{M}_\ell$ se le denota parte homogénea de grado ℓ de $\mathcal{M}$.*

Es sobre los $\mathcal{S}$-módulos graduados sobre los que tiene sentido definir la función de Hilbert.

Definición 3.2 (Función de Hilbert) *Dado un $\mathcal{S}$-módulo graduado $\mathcal{M}$, la función de Hilbert de $\mathcal{M}$ es la aplicación $h_I : \mathbb{N} \to \mathbb{N}$ definida como $h_I(\ell) = \dim_{\mathbb{K}} \mathcal{M}_\ell$.*

Nótese que esta definición tiene sentido puesto que cada $\mathcal{M}_\ell$ no deja de ser un espacio vectorial sobre $\mathbb{K}$. Así, si dicho módulo es finitamente generado, es fácil comprobar que $\dim_{\mathbb{K}} \mathcal{M}_\ell < \infty$.

Definición 3.3 (Morfismo graduado) *Sean $\mathcal{M}$, $\mathcal{N}$ dos $\mathcal{R}$-módulos graduados con $\mathcal{R}$ un anillo graduado. Un $\mathcal{R}$-morfismo graduado entre $\mathcal{M}$ y $\mathcal{N}$ es un $\mathcal{R}$-morfismo $f : \mathcal{M} \to \mathcal{N}$ tal que para todo ℓ se tiene $f|_{\mathcal{M}_\ell} : \mathcal{M}_\ell \to \mathcal{N}_\ell$*

De la misma forma, también hay una definición *graduada* para el caso de las sucesiones exactas:

Definición 3.4 (Sucesión exacta graduada) *Dado un anillo graduado $\mathcal{R}$, una sucesión de $\mathcal{R}$-módulos graduados $\mathcal{M}_i$ y una sucesión de $\mathcal{R}$-morfismos graduados $f_i : \mathcal{M}_{i-1} \to \mathcal{M}_i$, decimos que la sucesión*

$$\ldots \xrightarrow{f_{i-1}} \mathcal{M}_{i-1} \xrightarrow{f_i} \mathcal{M}_i \xrightarrow{f_{i+1}} \mathcal{M}_{i+i} \xrightarrow{f_{i+2}} \ldots$$

es exacta graduada si $\operatorname{im}(f_i) = \ker(f_{i+1})$ para todo i.

En particular, la función de Hilbert tiene un buen comportamiento sobre las sucesiones exactas graduadas cortas de $\mathcal{S}$-módulos graduados [5]:

Proposición 3.5 *Dados $\mathcal{M}$, $\mathcal{N}$, $\mathcal{P}$ tres $\mathcal{S}$-módulos graduados y una sucesión exacta graduada*

$$0 \xrightarrow{\phi_0} \mathcal{M} \xrightarrow{\phi_1} \mathcal{N} \xrightarrow{\phi_2} \mathcal{P} \xrightarrow{\phi_3} 0$$

se tiene siempre que $h_{\mathcal{P}}(\ell) = h_{\mathcal{N}}(\ell) - h_{\mathcal{M}}(\ell)$ para todo $\ell \in \mathbb{N}$ (en el caso en el que las funciones tomen valores finitos).

Demostración: Puesto que los morfismos ϕ_1 y ϕ_2 no dejan de ser aplicaciones lineales si vemos las partes homogéneas de los módulos como $\mathbb{K}$-espacios vectoriales, la fórmula no deja de ser la vista en Álgebra Lineal aplicada a las restricciones de las aplicaciones lineales sobre las partes homogéneas de grado ℓ de los módulos (Teorema del Rango-Nulidad).

$$\begin{aligned} h_{\mathcal{P}}(\ell) = \dim_{\mathbb{K}} \ker(\phi_3|_{\mathcal{P}\ell}) = \dim_{\mathbb{K}} \operatorname{im}(\phi_2|_{\mathcal{N}\ell}) = \dim_{\mathbb{K}} \mathcal{N}_\ell - \dim_{\mathbb{K}} \ker(\phi_2|_{\mathcal{N}\ell}) = \\ = h_{\mathcal{N}}(\ell) - \dim_{\mathbb{K}} \operatorname{im}(\phi_1|_{\mathcal{M}\ell}) = h_{\mathcal{N}}(\ell) - \dim_{\mathbb{K}} \mathcal{M}_\ell = h_{\mathcal{N}}(\ell) - h_{\mathcal{M}}(\ell) \end{aligned}$$

donde se ha utilizado fuertemente la exactitud de la sucesión en todos sus puntos. Además, $\ker(\phi_3|_{\mathcal{P}_\ell}) = \mathcal{P}_\ell$ por definición del morfismo ϕ_3 y $0 = \operatorname{im}(\phi_0) = \ker(\phi_1)$, lo que hace que ϕ_1 sea un monomorfismo.

■

3.2. La función de Hilbert de un conjunto proyectivo

Puesto que nuestro objetivo es estudiar conjuntos proyectivos, nos va interesar el estudio de la función de Hibert para los $\mathcal{S}$-módulos graduados $\mathcal{S}/I$ donde I es un ideal homogéneo. Recordemos que dicho cociente tiene estructura de anillo graduado por la Proposición 1.4, y en particular tiene estructura de módulo graduado.

Llamamos *función de Hilbert del ideal homogéneo I* a la aplicación $h_I : \mathbb{N} \to \mathbb{N}$ definida como $h_I(\ell) := \dim_{\mathbb{K}}(\mathcal{S}/I)_\ell$. Nótese que la función de Hilbert de I coincide con la de $\mathcal{S}/I$, pero por abuso de notación solamente haremos referencia al ideal homogéneo. De forma similar, definimos la *función de Hilbert del conjunto proyectivo X* a la aplicación $h_X(\ell) := h_{I(X)}(\ell)$. Veamos en primer lugar algunas propiedades importantes de la función de Hilbert en relación con los conjuntos proyectivos [2].

Lema 3.6 *Sean I_1, I_2 dos ideales homogéneos de $\mathcal{S}$. Entonces existe una sucesión exacta graduada*

$$0 \longrightarrow \mathcal{S}/(I_1 \cap I_2) \xrightarrow{\phi_1} \mathcal{S}/I_1 \oplus \mathcal{S}/I_2 \xrightarrow{\phi_2} \mathcal{S}/(I_1 + I_2) \longrightarrow 0$$

En particular, aplicando la Proposición 3.5, se tiene que:

$$h_{I_1 \cap I_2}(\ell) = h_{I_1}(\ell) + h_{I_2}(\ell) - h_{I_2 + I_2}(\ell)$$

para todo $\ell \in \mathbb{N}$.

Demostración: En primer lugar definimos las aplicaciones ϕ_1 y ϕ_2 y posteriormente haremos las comprobaciones necesarias.

$$\phi_1 : \mathcal{S}/(I_1 \cap I_2) \to \mathcal{S}/I_1 \oplus \mathcal{S}/I_2 \qquad F + I_1 \cap I_2 \mapsto (F + I_1, F + I_2)$$

$$\phi_2 : \mathcal{S}/I_1 \oplus \mathcal{S}/I_2 \to \mathcal{S}/(I_1 + I_2) \qquad (F + I_1, G + I_2) \mapsto (F - G) + I_1 + I_2$$

Es claro que estas aplicaciones constituyen una sucesión de módulos puesto que $\phi_2 \circ \phi_1 = 0$. Comprobemos que dicha sucesión es exacta. En primer lugar, ϕ_1 es monomorfismo. En efecto, tenemos las siguientes equivalencias:

$$F + I_1 \cap I_2 \in \ker(\phi_1) \Leftrightarrow \phi_1(F + I_1 \cap I_2) = 0 \Leftrightarrow (F + I_1, F + I_2) = 0 \Leftrightarrow$$
$$\Leftrightarrow F \in I_1 \, , F \in I_2 \Leftrightarrow F \in I_1 \cap I_2 \Leftrightarrow F + I_1 \cap I_2 = 0$$

Por otro lado, ϕ_2 es epimorfismo puesto que, dada la clase $F + I_1 + I_2$, es claro que es imagen de $(F + I_1, G + I_2)$ con $G \in I_2$.

Finalmente, comprobemos que $\ker(\phi_2) = \text{im}(\phi_1)$. Por la definición de sucesión siempre se tiene que $\ker(\phi_2) \supseteq \text{im}(\phi_1)$. Para el otro contenido, si $(F + I_1, G + I_2) \in \ker(\phi_2)$, $\phi_2(F + I_1, G + I_2) = (F - G) + I_1 + I_2 = 0$ o lo que es lo mismo, $F - G \in I_1 + I_2$, por lo que $F - G = H_1 + H_2$ con $H_1 \in I_1$ y $H_2 \in I_2$. Pero entonces $F + I_1 = (F - H_1) + I_1$ y $G + I_2 = (F - H_1 - H_2) + I_2 = (F - H_1) + I_2$, y así $(F + I_1, G + I_2) = (F - H_1 + I_1, F - H_1 + I_2) \in \text{im}(\phi_1)$.

■

La función de Hilbert evaluada en $\ell \gg 0$ es especialmente útil para caracterizar conjuntos proyectivos vacíos y finitos, tal y como muestran las tres siguientes proposiciones:

Proposición 3.7 (Caracterización del conjunto vacío) *Dado un ideal homogéneo I de $\mathcal{S}$, se tiene que $h_I(\ell) = 0$ para $\ell \gg 0$ si y solo si $V(I) = \emptyset$.*

Demostración: Por el Teorema débil de los ceros de Hilbert (Teorema 2.6), $V(I) = \emptyset$ si y solo si $\mathfrak{M} \subseteq \sqrt{I}$, o lo que es lo mismo, $X_i^{d_i} \in I$ para todo $i = 0, .., n$ y para ciertos $d_i \geq 0$. En ese caso, existe un $r \in \mathbb{N}$ tal que $X_i^r \in I$ para todo i. Tomando $\ell \in \mathbb{N}$ tal que $\ell \geq (n+1)r$ entonces $\mathcal{S}_\ell \in I$ puesto que una base de $\mathcal{S}_\ell$ es $\{X_0^{i_0} \cdot ... \cdot X_n^{i_n} \mid i_0 + ... + i_n = \ell\}$ y por tanto, por la elección de ℓ, siempre habrá algún $i_j > r$. Consecuentemente, $h_I(\ell) = \dim_{\mathbb{K}}(\mathcal{S}/I)_\ell = \dim_{\mathbb{K}} \mathcal{S}_\ell / I_\ell = 0$. Recíprocamente, si $h_I(\ell) = 0$ para $\ell \gg 0$, entonces $\mathcal{S}_\ell \subseteq I_\ell \subseteq I$. En particular, $X_i^\ell \in I$ para todo $i = 0, ..., n$, lo que implica que $\mathfrak{M} \subseteq \sqrt{I}$ y, otra vez por el Teorema débil de los ceros de Hilbert, $V(I) = \emptyset$.

■

Proposición 3.8 (Caracterización de conjuntos proyectivos finitos) *Sea X un conjunto de d puntos en $\mathbb{P}^n$. Entonces $h_X(\ell) = d$ si $\ell \geq d - 1$. Recíprocamente, si X es un conjunto proyectivo tal que $h_X(\ell) = d$ para valores suficientemente grandes de ℓ, entonces X es un conjunto de d puntos.*

Demostración: Sean $p_1 = (a_{10} : ... : a_{1n})$, ..., $p_d = (a_{d0} : ... : a_{dn})$ los puntos en cuestión. Fijando los vectores que representan a los puntos, podemos definir para cada $\ell \in \mathbb{N}$ el mapa evaluación $\varphi_\ell : \mathcal{S}_\ell \to \mathbb{K}^d$ que consiste en evaluar cada polinomio homogéneo de grado ℓ en el conjunto de d puntos. Por definición es claro que $\ker(\varphi_\ell) = I(X)_\ell$, por lo que por el Primer Teorema de Isomorfía, $\text{im}(\varphi_\ell) \cong \mathcal{S}(X)_\ell$ (recuérdese la Definición 2.4). Veamos que, para $\ell \geq d - 1$ se tiene que φ_ℓ es epimorfismo; esto directamente nos dirá que $h_X(\ell) = d$. En efecto, para cada $i = 1, ..., d$ y cada $j \neq i$ podemos encontrar una forma lineal $H_i \in \mathcal{S}$ tal que se anule en p_i pero no en cualquier otro p_j. Así, $F_i = \prod_{j \neq i} H_j$ es un polinomio homogéneo de grado $d - 1$ que se anula en todos los p_j

salvo en p_i. Si fijamos ahora un polinomio homogéneo G de grado $\ell-d+1$, podemos concluir que las imágenes a través de φ_ℓ de los elementos $GF_1, ..., GF_d$ generan $\mathbb{K}^d$, lo que prueba la sobreyectividad de φ_ℓ.

Recíprocamente, supongamos que h_X toma el valor constante d para $\ell \gg 0$. Si X no fuera finito, entonces podríamos encontrar $Z \subseteq X$ conjunto de $d+1$ puntos y por tanto tendríamos el epimorfismo $\mathcal{S}(X) \to \mathcal{S}(Z)$, pero para valores grandes de ℓ tenemos que $h_X(\ell) = d$ y $h_Z(\ell) = d+1$, es decir, $\dim_{\mathbb{K}}\mathcal{S}(X)_\ell < \dim_{\mathbb{K}}\mathcal{S}(Z)_\ell$, lo que contradice la exixtencia del epimorfismo. De esta forma, X es un conjunto finito, y por la primera implicación, consiste en d puntos.

■

Lema 3.9 *Sea I un ideal homogéneo de $\mathcal{S}$ y sea J la intersección de las componentes no irrelevantes de una descomposición primaria irredundante de I. Entonces $h_I(\ell) = h_J(\ell)$ para $\ell \gg 0$. En particular, $h_I(\ell) = h_{\mathrm{Sat}(I)}(\ell)$ para $\ell \gg 0$.*

Demostración: Si bien se puede probar a partir de la propiedad dada por el Lema 3.6, una demostración directa resulta de aplicar la Proposición 1.14 y la definición de función de Hilbert.

■

Estamos ya en disposición de probar que la función de Hilbert, para valores suficientemente grandes de ℓ, viene dada por un polinomio, al cual llamaremos *polinomio de Hilbert*. No obstante, demostramos primero un lema previo. En la notación de dicho lema, si $\mathcal{M}$ es un $\mathcal{R}$-módulo graduado, $\mathcal{M}(-d)$ es otro $\mathcal{R}$-módulo graduado que, como conjunto, coincide con $\mathcal{M}$, pero cuya parte homogénea de grado ℓ coincide con la parte homogénea de grado $\ell - d$ de $\mathcal{M}$.

Lema 3.10 *Sea F un polinomio homogéneo de grado d que no está contenido en ningún primo asociado de un ideal homogéneo I. Entonces la multiplicación por F induce un monomorfismo graduado $(\mathcal{S}/I)(-d) \xrightarrow{\phi_1} \mathcal{S}/I$ y por tanto hay una sucesión exacta graduada*

$$0 \longrightarrow (\mathcal{S}/I)(-d) \xrightarrow{\phi_1} \mathcal{S}/I \xrightarrow{\phi_2} \mathcal{S}/(I + \langle F\rangle) \longrightarrow 0$$

lo que hace que en particular:

$$h_{I+\langle F\rangle}(\ell) = h_I(\ell) - h_I(\ell - d)$$

Demostración: Sea $I = I_1 \cap ... \cap I_r$ una descomposición primaria de I y sean $P_1, ..., P_r$ sus primos asociados (i.e. los radicales de las componentes primarias). Tomamos F homgéneo tal que $F \notin P_1 \cup ... \cup P_r$. Veamos que efectivamente $\ker(\phi_1) = 0$. Si $G \in \ker(\phi_1)$, entonces $FG + I = 0$, o lo que es lo mismo, $FG \in I$ y en particular $FG \in I_i$ para todo $i = 1, ..., r$. Pero como $F \notin P_i$, por ser los I_i primarios se tiene que $G \in I_i$, por lo que $G \in I$ y por tanto $G + I = 0$.

La sobreyectividad de ϕ_2 es directa. Solo nos falta probar que $\mathrm{im}(\phi_1) = \ker(\phi_2)$. En efecto, $\phi_2(G + I) = 0 \Leftrightarrow G \in I + \langle F\rangle \Leftrightarrow G = H_1 + H_2F$ con $H_1 \in I$ y $H_2 \in \mathcal{S}$, lo que hace que $G + I = H_2F + I = \phi_1(H_2 + I)$. La sucesión entonces es exacta y también graduada, y la última afirmación se desprende de aplicar la Proposición 3.5.

■

Teorema 3.11 (Existencia del polinomio de Hilbert) *Sea I un ideal homogéneo de $\mathcal{S}$. Entonces existe un polinomio $P_I \in \mathbb{Q}[T]$ tal que $h_I(\ell) = P_I(\ell)$ para $\ell \gg 0$.*

Demostración: Vamos a hacer inducción sobre el número de variables n. Para $n = 0$, o bien $I = \{0\}$ y por tanto $P_I = 1$ o bien $\mathfrak{M} \subseteq \sqrt{I}$, por lo que $P_I = 0$.

Asumimos entonces que $n > 0$. Si $\mathfrak{M} \subseteq \sqrt{I}$ entonces directamente se tiene que $P_I = 0$ es el polinomio nulo por la Proposición 3.7. Además, dado que vamos a estudiar el comportamiento de h_I para $\ell \gg 0$, en virtud del Lema 3.9 vamos a limitarnos a estudiar la función de Hilbert de su saturación $\mathrm{Sat}(I)$.

Veamos que existe una forma lineal $H \in \mathcal{S}$ que no pertenece a ningún primo asociado de $\mathrm{Sat}(I)$. En efecto, como $\mathfrak{M}$ no es un primo asociado de $\mathrm{Sat}(I)$ (véase Proposición 1.14), si una descomposición irredundante de $\mathrm{Sat}(I)$ es $\mathrm{Sat}(I) = I_1 \cap ... \cap I_r$, entonces por el Teorema débil de los ceros de Hilbert $V(I_i) \neq \emptyset$ para $i = 1, .., r$. Podemos tomar entonces $p_i \in V(I_i)$ y sea H una forma lineal que no contenga a ninguno de dichos puntos (siempre podemos hacer eso por ser el conjunto de puntos finitos). Es claro entonces que $H \notin I_i \subseteq \sqrt{I_i}$ para todo i, por lo que H no pertenece a ningún primo asociado de $\mathrm{Sat}(I)$.

Por el Lema 3.10 se tiene que $h_{\mathrm{Sat}(I)+\langle H\rangle}(\ell) = h_{\mathrm{Sat}(I)}(\ell) - h_{\mathrm{Sat}(I)}(\ell - 1)$. Haciendo un cambio de coordenadas si es necesario, podemos asumir que $H = X_n$. Así, $\mathcal{S}/(\mathrm{Sat}(I) + \langle X_n\rangle) \cong \mathbb{K}[X_0, ..., X_{n-1}]/J'$ donde J' es el resultado de sustituir $X_n = 0$ en el ideal $\mathrm{Sat}(I) + \langle X_n\rangle$. Aplicando la hipótesis de inducción, existe un polinomio $P_{\mathrm{Sat}(I)+\langle X_n\rangle}(T) \in \mathbb{Q}[T]$ tal que $h_{\mathrm{Sat}(I)+\langle X_n\rangle}(\ell) = P_{\mathrm{Sat}(I)+\langle X_n\rangle}(\ell)$ para $\ell \gg 0$.

Tenemos ahora que construir un polinomio $Q(T) \in \mathbb{Q}[T]$ tal que $P_{\mathrm{Sat}(I)+\langle X_n\rangle}(T) = Q(T) - Q(T-1)$. Si $P_{\mathrm{Sat}(I)+\langle X_n\rangle}$ tiene grado d, notando que $\binom{T}{0}, ..., \binom{T}{d}$ es una base del conjunto de polinomios de $\mathbb{Q}[T]$ de grado al menos d, entonces $P_{\mathrm{Sat}(I)+\langle X_n\rangle}(T) = a_0\binom{T}{0} + ... + a_d\binom{T}{d}$ con los $a_i \in \mathbb{Q}$ (incluso se puede probar que con esta base los coeficientes están en $\mathbb{Z}$). Puesto que $\binom{T}{k} = \binom{T+1}{k+1} - \binom{T}{k+1}$, es claro que el polinomio $Q(T) = a_0\binom{T+1}{1} + ... + a_d\binom{T+1}{d+1}$ satisface la condición buscada.

Finalmente, si consideramos $c(\ell) := h_I(\ell) - Q(\ell) = h_{\mathrm{Sat}(I)}(\ell) - Q(\ell)$ es claro que $c(\ell) - c(\ell - 1) = h_{\mathrm{Sat}(I)}(\ell) - Q(\ell) - h_{\mathrm{Sat}(I)}(\ell - 1) + Q(\ell - 1) = h_{\mathrm{Sat}(I)+\langle H\rangle}(\ell) - Q(\ell) + Q(\ell - 1) \equiv 0$ para $\ell \gg 0$, lo que implica que $c(\ell) \equiv c_0$ con c_0 constante para $\ell \gg 0$. Consecuentemente, $h_I(\ell) = c(\ell) + Q(\ell) = c_0 + Q(\ell) =: P_I(\ell)$ es un polinomio para $\ell \gg 0$.

■

Al polinomio P_I se le denomina *polinomio de Hilbert* del ideal I. Llamamos *polinomio de Hilbert* del conjunto proyectivo X al polinomio $P_X := P_{I(X)}$. Podemos traducir ahora todos los resultados importantes del capítulo en términos del polinomio de Hilbert:

Proposición 3.12 *Sean I, I_1, I_2 ideales homogéneos y sea X una variedad proyectiva. Entonces el polinomio de Hilbert satisface las siguientes propiedades:*

1. $P_{I_1 \cap I_2} = P_{I_1} + P_{I_2} - P_{I_1+I_2}$.
2. $P_I = 0$ *si y solo si* $V(I) = \emptyset$.
3. P_X *es constante y no nula si y solo si X es un conjunto finito de puntos. En ese caso, P_X da el número de puntos en X.*
4. *Si I es un ideal homogéneo y J es la intersección de las componentes primarias no irrelevantes de una descomposición irredundante de I, entonces $P_I = P_J$.*

5. *Si F es un polinomio homogéneo de grado d que no está contenido en ningún primo asociado de I, entonces $P_{I+\langle F\rangle}(T) = P_I(T) - P_I(T-d)$.*

3.3. Teorema fuerte de los ceros de Hilbert

Una de las primeras aplicaciones del polinomio de Hilbert es demostrar de forma casi directa el Teorema fuerte de los ceros de Hilbert en su versión proyectiva [2], el cual nos permite establecer una biyección entre los ideales homogéneos radicales de $\mathcal{S}$ y los conjuntos proyectivos de $\mathbb{P}^n$ tal y como comentamos en el capítulo anterior.

Lema 3.13 *Sea I un ideal homogéneo que no es $\mathfrak{M}$-primario y consideramos el conjunto proyectivo $X = V(I)$. Entonces* $\deg P_I$ *es el máximo entero m tal que cualquier subespacio lineal de $\mathbb{P}^n$ de codimensión m corta a X.*

Demostración: Sea m el grado del polinomio de Hilbert de I. Por el Teorema débil de los ceros de Hilbert se tiene que $X \neq \emptyset$ y por la Proposición 3.12 (2) se tiene que $m > 0$. Tomamos un subespacio lineal $A \subset \mathbb{P}^n$ de codimensión $r \leq m$, es decir, definido por r formas lineales independientes $H_1, ..., H_r$. Tenemos entonces la sucesión de módulos:

$$0 \longrightarrow (\mathcal{S}/I)(-1) \xrightarrow{\cdot H_1} \mathcal{S}/I \longrightarrow \mathcal{S}/(I + \langle H_1\rangle) \longrightarrow 0$$

que, si bien puede ser que no sea exacta en todas las posiciones (no está asegurada la inyectividad de $\cdot H_1$), sí que satisface que $P_{I+\langle H_1\rangle}(T) \geq P_I(T) - P_I(T-1)$ (véase demostración de la Proposición 3.5). Como $P_I(T) - P_I(T-1)$ es un polinomio de grado $m-1$ con coeficiente principal positivo, entonces $P_{I+\langle H_1\rangle}(T)$ tiene grado al menos $m-1$. Podemos iterar este método para afirmar que el polinomio de Hilbert de $I + \langle H_1, ..., H_r\rangle$ tiene grado al menos $m - r \geq 0$, por lo que no es el polinomio nulo. Por ello, $V(I + \langle H_1, ..., H_r\rangle) = X \cap A$ es no nulo por la Proposición 3.12 (2).

Nos falta comprobar que existe un subespacio lineal de codimensión $m+1$ que no corta a X. Dado que I no es $\mathfrak{M}$-primario, siempre podemos encontrar una forma lineal H_1 que no esté en ningún primo asociado de I (véase la demostración del Teorema 3.11). De esta forma, por la Proposición 3.12 (5) se tiene que $P_{I+\langle H_1\rangle}(T) = P_I(T) - P_I(T-1)$, y por tanto $P_{I+\langle H_1\rangle}(\ell)$ tiene grado $m-1$. Podemos repetir el proceso hasta encontrar $H_1, ..., H_{m+1}$ formas lineales que hagan que el polinomio de Hilbert de $I + \langle H_1, ..., H_{m+1}\rangle$ sea cero. En ese caso, por la Proposición 3.12 (2) se tiene que $V(I + \langle H_1, ..., H_{m+1}\rangle) = X \cap V(H_1, ..., H_{m+1}) = \emptyset$, probando el resultado.

■

Teorema 3.14 (Fuerte de los ceros de Hilbert) *Sea I un ideal homogéneo no $\mathfrak{M}$-primario de $\mathcal{S}$. Entonces $I(V(I)) = \sqrt{I}$.*

Demostración: Tomando radicales en la descomposición primaria de I se tiene que $\sqrt{I} = I_1 \cap ... \cap I_r$ con los I_i ideales primos. Puesto que $I(V(I)) = I(V(I_1)) \cap ... \cap I(V(I_r))$, solo es necesario probar el aserto para ideales primos (que a su vez son radicales).

Supongamos I primo y tomemos $F \in I(V(I))$ un polinomio homogéneo. Si $F \notin I$, entonces por la Proposición 3.12 (5) se sigue que el polinomio de Hilbert de $I + \langle F\rangle$ tiene grado $m-1$, donde m es el grado del polinomio de Hilbert del ideal I. Pero el Lema 3.13 nos da una contradicción.

Por un lado, existe un subespacio lineal de $\mathbb{P}^n$ de codimensión m que no corta a $V(I + \langle F \rangle)$, y por el otro lado, todos los subespacios lineales de codimensión m de $\mathbb{P}^n$ deberían cortar a $V(I)$. Pero como $F \in I(V(I))$, entonces $V(I + \langle F \rangle) = V(I)$ por lo que es una contradicción. Concluimos así que $F \in I$ y por tanto $I(V(I)) \subseteq I = \sqrt{I}$. Por su parte el otro contenido siempre se tiene.

■

Capítulo 4

Multiplicidad de intersección de curvas planas

Una vez construido el polinomio de Hilbert, en este capítulo presentamos el resultado principal del texto, que consiste en comprobar que la definición de multiplicidad de intersección dada a partir del polinomio de Hilbert coincide con la definición que se vio en la asignatura de Curvas Algebraicas. Aunque posiblemente sea un resultado conocido, no hemos logrado encontrar una demostración explícita en la literatura, por lo que lo que aquí presentamos es una demostración original. Esto nos permite cerrar el círculo y hablar de dos teorías totalmente equivalentes pero que usan distintas técnicas. Así, el estudio de las curvas planas se puede hacer desde un punto de vista elemental o bien se pueden utilizar herramientas más profundas como es el polinomio de Hilbert, las cuales nos permiten demostrar resultados muy potentes de forma sencilla. En la primera sección del capítulo recordamos la noción de rama y multiplicidad de intersección vista en la asignatura de Curvas Algebraicas, mientras que la segunda sección introduciremos la definición de multiplicidad de intersección a partir del polinomio de Hilbert. Será en la última sección donde demostraremos el teorema de equivalencia de sendas definiciones.

Hay que notar que en este capítulo se trabaja en todo momento con curvas planas, por lo que debemos trasladar todos los conceptos vistos hasta ahora a dimensión 2. No obstante, la definición de multiplicidad de intersección que utiliza el polinomio de Hilbert es válida para cualquier dimensión.

4.1. Multiplicidad a partir de ramas

En esta presente sección vamos a recordar las nociones de rama y multiplicidad vistas en la asignatura de Curvas Algebraicas. Hay que destacar que vamos a trabajar con curvas afines, pues la definición de multiplicidad de intersección que daremos se hará en términos de curvas en el afín. Comenzamos recordando la definición de *parametrización formal* de una curva en un punto dado.

Definición 4.1 (Parametrización formal) *Se llama parametrización formal en (a, b) de una curva afín de ecuación minimal $f \in \mathbb{K}[X, Y]$ a un par $(p_1(T), p_2(T))$ de series formales $p_1, p_2 \in \mathbb{K}[[T]]$ tales que $f(p_1, p_2) = 0$, $p_1(0) = a$ y $p_2(0) = b$.*

Si bien las parametrizaciones formales van a dar lugar a las distintas ramas de una curva, no todas las parametrizaciones dan ramas distintas. Aquí aparece el concepto de *parametrizaciones equivalentes.*

Definición 4.2 (Parametrizaciones equivalentes) *Dos parametrizaciones formales* (p_1, p_2) *y* (p_1', p_2') *son equivalentes cuando están relacionadas mediante una reparametrización de la forma:*

$$(p_1', p_2') = (p_1 \circ g, p_2 \circ g)$$

donde g *es una serie formal de orden 1.*

Es una simple comprobación ver que la relación *parametrizaciones equivalentes* es una relación de equivalencia, pues las series de orden 1 son precisamente las que admiten inversa para la composición. Las clases de parametrizaciones cumplen una serie de propiedades fundamentales a la hora de estudiar las ramas de las curvas:

Lema 4.3 *Dada la curva afín* $V(f)$ *y un punto* $(a, b) \in V(f)$ *se cumplen las siguientes propiedades:*

1. *Toda parametrización formal de* $V(f)$ *en* (a, b) *es equivalente a una de la forma* $(a+T^r, p(T))$ *donde* $p \in \mathbb{K}[[T]]$ *con* $p(0) = b$.
2. *Dos parametrizaciones como las del punto (1.) son equivalentes si y solo si se pasa de una a otra mediante la sustitución* $T \mapsto \omega T$*, donde* ω *es una raíz* r*-ésima de la unidad.

Definición 4.4 (Parametrización reducida) *Decimos que una parametrización es reducida cuando su equivalente como las del punto (1.) del Lema 4.3 satisface que el máximo común divisor de* r *y los exponentes de* p *es 1.*

Podemos ahora definir rigurosamente el concepto de rama de una curva.

Definición 4.5 (Rama de una curva plana en un punto) *Se llama rama de la curva* $V(f)$ *en el punto* $(a, b) \in V(f)$ *a una clase de parametrización formal reducida de* $V(f)$ *en* (a, b).

Observación 4.6 *De aquí en adelante nos interesará el caso en el que el punto de estudio sea el origen* $(0, 0)$*, pues como veremos a continuación, cuando hacemos* $a = 0$ *aparecen de forma natural las series de Puiseux. Nótese que siempre podemos colocarnos en el origen sin más que aplicar una simple traslación.*

Observación 4.7 *Dada una parametrización reducida de la forma:*

$$(T^r, p(T)) = (T^r, b_0 + b_1 T + b_2 T^2 + ...)$$

si introducimos el símbolo $X^{1/r}$*, tenemos que* $p(X^{1/r}) = b_0 + b_1 X^{1/r} + b_2 X^{2/r} + ...$ *es una raíz de* f *como polinomio en la variable* Y *y con coeficientes en* $\mathbb{K}[[X]]$*. Por tanto, aparece de forma natural el anillo de series de Puiseux, el cual se define como sigue* [1]*:*

$$\mathbb{K}\{\{X\}\} := \bigcup_{r=1}^{\infty} \mathbb{K}[[X^{1/r}]]$$

Consecuentemente, la rama en el punto $(0, p(0))$ que representa dicha parametrización tiene asociada la serie de Puiseux $q(X) := p(X^{1/r})$. Además, por ser dicha parametrización reducida, el valor de r es el mínimo posible con el que podemos construir la serie de Puiseux.

Es más, por el punto (2.) del Lema 4.3, el resto de series de Puiseux que son raíces de f y están asociadas a la rama son las series conjugadas de $q(X)$; esto es, las series de la forma $q_\omega(X) := p(\omega X^{1/r}) = b_0 + b_1\omega X^{1/r} + b_2\omega^2 X^{2/r} + ...$ con ω una raíz r-ésima de la unidad. Esto no deja de ser teoría de Galois. Si extendemos el cuerpo de fracciones $\mathbb{K}((X))$ a $\mathbb{K}((X^{1/r}))$, las raíces del polinomio mínimo de $X^{1/r}$ (que es $P_{\min}(T) = T^r - X$) son precisamente los $\omega X^{1/r}$, de ahí el nombre de series conjugadas.

Podemos ahora definir la multiplicidad de intersección de una rama con una curva:

Definición 4.8 (Multiplicidad de intersección de una rama con una curva) *Se llama multiplicidad de intersección de una rama con una curva $V(g)$ en el punto $p = (a, b)$ al orden de $g(p_1, p_2)$, donde (p_1, p_2) es un representante de la rama. Dicha multiplicidad la denotaremos por $\mathrm{mult}_p(V(g), R)$, siendo R la rama en cuestión.*

La definición de multiplicidad de intersección de dos curvas planas en un punto a través de ramas se define entonces como sigue:

Definición 4.9 (Multiplicidad de intersección #1) *La multiplicidad de intersección de dos curvas afines $C, D \subset \mathbb{A}^2_{\mathbb{K}}$ en un punto $p \in C \cap D$ es la suma de las multiplicidades de intersección en p de cada rama de C en p con D. Denotaremos dicha multiplicidad como $\mathrm{mult}_1(C, D)_p$.*

En ocasiones es recomendable realizar un cambio de coordenadas para que uno de los polinomios a estudiar sea mónico en Y (por ejemplo, si homogeneizamos con respecto a X_0, una forma de conseguir esto es pedir que la curva proyectiva asociada no pase por $(0 : 0 : 1)$). En esta situación tenemos el siguiente resultado general:

Proposición 4.10 *Si $f \in \mathbb{K}\{\{X\}\}[Y]$ es mónico en la variable Y, entonces todas las raíces de f están en $\mathbb{K}\{\{X\}\}$.*

En particular, si tenemos un polinomio $f \in \mathbb{K}[X, Y]$ mónico en la variable Y, siempre vamos a poder descomponerlo como producto de series de Puiseux como sigue:

$$f = \prod_k (Y - q_k)$$

donde $q_k \in \mathbb{K}\{\{X\}\}$. Además, como f no tiene exponentes fraccionarios, cada vez que aparece una raíz $q_k \in \mathbb{K}[[X^{1/r_k}]]$ en la descomposición anterior, también aparecen las raíces conjugadas, por lo que podemos reagrupar las raíces de la expresión anterior:

$$f = \prod_k (Y - q_k) = \prod_{i=1}^{t} \prod_{j=1}^{r_i} (Y - q_{ij}) \qquad \text{con} \qquad f_i := \prod_{j=1}^{r_i} (Y - q_{ij}) \in \mathbb{K}[[X]][Y]$$

donde las series q_{ij} son las r_i raíces conjugadas que dan la misma clase de parametrización. Por su parte, que los $f_i \in \mathbb{K}[[X]][Y]$ es bastante claro, pues el automorfismo que manda $X^{1/r_i} \mapsto \omega X^{1/r_i}$ con $\omega^{r_i} = 1$ deja invariante a f_i.

Observación 4.11 *El comentario anterior junto con la Observación 4.7 nos permite extraer las siguientes conclusiones:*

- *Un polinomio f mónico en Y siempre admite una descomposición de la forma $f = f_1, ..., f_t$ donde los $f_i \in \mathbb{K}[[X]][Y]$ y donde cada uno de ellos representa a una rama distinta en un punto de la recta $V(X)$.*
- *Los tériminos f_i son irreducibles, pues cualquier posible descomposición con menos factores no tendría a todas las raíces conjugadas, por lo que sus factores no estarían en $\mathbb{K}[[X]][Y]$. Es más, los f_i son los polinomios mínimos de las raíces q_{ij} sobre $\mathbb{K}[[X]][Y]$.*

Observación 4.12 *Siguiendo la notación de la Observación 4.11, y atendiendo a la Definición 4.8, denotamos $q_i \in \mathbb{K}[[X^{1/r_i}]]$ a una de las raíces de Puiseux conjugadas q_{ij} (sin pérdida de generalidad podemos tomar la primera q_{i1} de cada f_i) y denotemos por p_i a la serie formal tal que $p_i(X^{1/r_i}) = q_i(X)$. Sustituyendo en g siempre podemos escribir:*

$$g(T^{r_i}, p_i(T)) = T^{m_i} v_i(T)$$

con $v_i(0) \neq 0$ y donde cada m_i es la multiplicidad de intersección de la rama R_i con la curva $V(g)$. De esta forma, es claro que

$$\text{mult}_p(V(g), R_i) = m_i = \dim_{\mathbb{K}} \frac{\mathbb{K}[[T]]}{\langle T^{m_i} \rangle} = \frac{\mathbb{K}[[T]]}{\langle T^{m_i} v_i(T) \rangle} = \dim_{\mathbb{K}} \frac{\mathbb{K}[[T]]}{\langle g(T^{r_i}, p_i(T)) \rangle}$$

puesto que $v_i(T)$ es unidad en $\mathbb{K}[[T]]$ y una base de dicho espacio sería $\mathcal{B} = \{1, T, ..., T^{m_i - 1}\}$.

4.2. Multiplicidad a partir del polinomio de Hilbert

Comenzamos la sección definiendo multiplicidad de intersección a través del polinomio de Hilbert.

Definición 4.13 (Multiplicidad de intersección #2) *La multiplicidad de intersección de dos conjuntos proyectivos $X, Y \subset \mathbb{P}^n$ en un punto p de su intersección es el valor del polinomio de Hilbert de la componente $I(p)$-primaria de $I(X) + I(Y)$ (asumiendo que p es una componente irreducible de $X \cap Y$). Denotaremos dicha multiplicidad como* $\text{mult}_2(X, Y)_p$.

Nótese que dicha multiplicidad de intersección está bien definida puesto que, si p es una componente irreducible, entonces la componente $I(p)$-primaria es minimal y por tanto independiente de la descomposición primaria de $I(X \cap Y)$.

Dado que la definición en términos de ramas se ha dado para el caso afín, será recomendable traducir la definición que acabamos de dar al caso afín y eliminar la dependencia en el valor de $\ell \gg 0$ que aporta el polinomio de Hilbert. El siguiente lema nos ayudará con esta tarea.

Lema 4.14 *Sean $F, G \in \mathbb{K}[X_0, X_1, X_2]$ dos polinomios homogéneos primos entre sí tales que las curvas proyectivas $V(F)$ y $V(G)$ no tienen puntos en común en la recta $V(X_0)$. Denotemos por f, g a los respectivos polinomios deshomogeneizados con respecto a la variable X_0. En esta situación y para ℓ lo suficientemente grande, la aplicación dada por:*

$$\frac{\mathbb{K}[X_0, X_1, X_2]_\ell}{\langle F, G \rangle_\ell} \longrightarrow \frac{\mathbb{K}[X, Y]}{\langle f, g \rangle} \qquad Q_\ell + \langle F, G \rangle_\ell \mapsto Q_\ell(1, X, Y) + \langle f, g \rangle$$

es un isomorfismo de $\mathbb{K}$-espacios vectoriales.

Demostración: Veamos en primer lugar que la aplicación está bien definida. Si Q_ℓ y Q'_ℓ dan la misma clase módulo $\langle F, G\rangle$, entonces $Q_\ell - Q'_\ell = AF + BG$, por lo que $Q_\ell(1, X, Y) - Q'_\ell(1, X, Y) = A(1, X, Y)F(1, X, Y) + B(1, X, Y)G(1, X, Y) = A(1, X, Y)f + B(1, X, Y)g$, luego las clases de $Q_\ell(1, X, Y)$ y $Q'_\ell(1, X, Y)$ son las mismas.

Probemos ahora que la aplicación es inyectiva. Para ello, sea $Q_\ell + \langle F, G\rangle_\ell$ un elemento de su núcleo. Entonces, $Q_\ell(1, X, Y) = h_1 f + h_2 g$ con $h_i \in \mathbb{K}[X, Y]$. Como los homogeneizados de f, g son precisamente F, G (por hipótesis F, G no pueden ser divisibles por X_0), se tienen las siguientes igualdades:

$$F = X_0^{\deg(F)} F\left(1, \frac{X_1}{X_0}, \frac{X_2}{X_0}\right) \qquad G = X_0^{\deg(G)} G\left(1, \frac{X_1}{X_0}, \frac{X_2}{X_0}\right)$$

Tomando $m \geq \max\{\ell, \deg(h_1) + \deg(F), \deg(h_2) + \deg(G)\}$ tenemos las siguientes igualdades:

$$\begin{aligned} X_0^{m-\ell} Q_\ell &= X_0^m Q_\ell\left(1, \frac{X_1}{X_0}, \frac{X_2}{X_0}\right) \\ &= X_0^m h_1\left(\frac{X_1}{X_0}, \frac{X_2}{X_0}\right) f\left(\frac{X_1}{X_0}, \frac{X_2}{X_0}\right) + X_0^m h_2\left(\frac{X_1}{X_0}, \frac{X_2}{X_0}\right) g\left(\frac{X_1}{X_0}, \frac{X_2}{X_0}\right) \\ &= X_0^{m-\deg(H_1)-\deg(F)} H_1 F + X_0^{m-\deg(H_2)-\deg(G)} H_2 G \end{aligned}$$

con H_1, H_2 los polinomios homogeneizados de h_1, h_2. Consecuentemente, $X_0^{m-\ell} Q_\ell \in \langle F, G\rangle$ y por ello está en todas la componentes primarias de dicho ideal. Pero como $\langle F, G\rangle$ es saturado por el Lema 1.15, todas las componentes primarias de $\langle F, G\rangle$ corresponden a los puntos de $V(F) \cap V(G)$, ninguno de ellos contenido en $V(X_0)$ por hipótesis. Así, $X_0^{m-\ell}$ no está en el radical de ninguna de estas componentes, lo que hace que Q_ℓ sí que esté en todas ellas y por tanto $Q_\ell \in \langle F, G\rangle_\ell$.

Para probar la suprayectividad debemos suponer además que $\ell \geq \deg(\mathrm{res}_Y(f, g)) + \deg(\mathrm{res}_X(f, g))$. Tomamos una clase de $\mathbb{K}[X, Y]/\langle f, g\rangle$ de la forma $p + \langle f, g\rangle$. Si $\deg(p) \leq \ell$ entonces dicha clase es imagen de $X_0^{\ell-\deg(p)} P + \langle F, G\rangle_\ell$, donde P es el homogeneizado de p. Si por el contrario $\deg(p) > \ell$, entonces procedemos como sigue:

1. Dividimos los coeficientes de p como polinomio en Y por $\mathrm{res}_Y(f, g) \in \langle f, g\rangle$ (véase [4]), lo que nos produce otro polinomio p' de la misma clase que p y cuyo grado en X es menor que el grado de $\mathrm{res}_Y(f, g)$.

2. Dividimos los coeficientes de p' como polinomio en X por $\mathrm{res}_X(f, g)$, lo que nos produce otro polinomio p'' de la misma clase que p' y cuyo grado en Y es menor que el grado de $\mathrm{res}_X(f, g)$.

Obtenemos así que $p + \langle f, g\rangle = p'' + \langle f, g\rangle$ con $\deg(p'') < \deg(\mathrm{res}_Y(f, g)) + \deg(\mathrm{res}_X(f, g)) \leq \ell$. Así, por lo que hemos dicho antes, la clase de p'', que es la clase de p, está en la imagen de la aplicación.

■

4.3. Equivalencia de las definiciones de multiplicidad

Tal y como indica el título de la sección, vamos a dedicar el resto del capítulo a demostrar que ambas definiciones de multiplicidad de intersección dadas son la misma. Para facilitar el seguimiento del hilo conductor, esbozamos previamente una idea de cómo irá la demostración.

Nuestra **hoja de ruta** va a consistir en tomar la definición de multiplicidad de intersección dada por el polinomio de Hilbert y transformarla paulatinamente hasta hacerla coincidir con la definición #1 de multiplicidad de intersección.

Situándonos en las hipótesis y notación del Lema 4.14, comenzaremos deshomogeneizando la definición #2 para que coincida con la dimensión de $\mathbb{K}[X,Y]/I_1'$, donde I_1' es la componente primaria de $\langle f,g\rangle$ asociada al punto que estemos estudiando. Esto se hará en la Proposición 4.15.

Tomando coordenadas para que el punto a estudiar sea el $(0,0)$ y suponiendo que en la recta $V(X)$ no hay más puntos de intersección, podemos entonces sustituir $\mathbb{K}[X]$ por $\mathbb{K}[[X]]$, lo que nos permitiría estudiar más facilmente la multiplicidad de intersección en el origen. En la Proposición 4.16 comprobaremos que, en efecto, la dimensión de $\mathbb{K}[[X]][Y]/\langle f,g\rangle$ coincide con la multiplicidad de intersección de $V(f)$ y $V(g)$ en $(0,0)$.

Factorizando $f = f_1 \cdot ... \cdot f_t$ en $\mathbb{K}[[X]][Y]$ como en la Observación 4.11, sería esperable que la aplicación natural de $\mathbb{K}[[X]][Y]/\langle f,g\rangle$ a $\bigoplus_i \mathbb{K}[[X]][Y]/\langle f_i,g\rangle$ fuera un isomorfismo. Veremos que eso no es así, aunque probaremos en la Proposición 4.20 que, de todas formas, dichos espacios tienen la misma dimensión, que es realmente el resultado que nos interesa.

Finalmente, como cada f_i representa a una rama distinta de $V(f)$, extraeremos información sobre la intersección de $V(g)$ con la rama que representa f_i de cada espacio $\mathbb{K}[[X]][Y]/\langle f_i,g\rangle$. Para conseguir esto último y utilizando la notación de la observación 4.12, cabría pensar que el morfismo natural de $\mathbb{K}[[X]][Y]/\langle f_i,g\rangle$ a $\mathbb{K}[[T]]/\langle g(T^{r_i},p_i(T))\rangle$, el cual consiste en mandar la clase de $h(X,Y)$ a la clase de $h(T^{r_i},p_i(T))$, es un isomorfismo, lo que nos permitiría concluir nuestro trabajo. Sin embargo, esto último vuelve a ser falso, aunque probaremos que ambos espacios tienen la misma dimensión en la Proposición 4.24.

Pasamos pues a detallar los pasos que acabamos enumerar.

Proposición 4.15 *Sean $F,G \in \mathbb{K}[X_0,X_1,X_2]$ dos polinomios homogéneos primos entre sí y denotemos por f,g a los respectivos polinomios deshomogeneizados con respecto a la variable X_0. Si tomamos $p \in V(F)\cap V(G)$ no perteneciente a $V(X_0)$, entonces:*

$$\text{mult}_2(V(F),V(G))_p = \dim_{\mathbb{K}} \frac{\mathbb{K}[X,Y]}{I_1'}$$

donde I_1' es el ideal deshomogeneizado de I_1 con respecto a X_0 e I_1 es la componente primaria de $\langle F,G\rangle$ correspondiente al punto p.

Demostración: Como los polinomios F,G son coprimos, por el Lema 1.15 el ideal $\langle F,G\rangle$ que define la intersección de las curvas $V(F)\cap V(G)$ es saturado y por ende su descomposición primaria no contiene componentes irrelevantes. Así, si escribimos la descomposición como

$$\langle F,G\rangle = I_1 \cap ... \cap I_r$$

y aplicando el Teorema débil de Bézout (cuya demostración veremos en el capítulo siguiente) podemos estar seguros de que cada $V(I_i)$ coincide con un punto de la intersección de $V(F)$ y $V(G)$. Tomamos entonces sin pérdida de generalidad $p = V(I_1)$. Procedemos a deshomogeneizar la descomposición primaria con respecto a X_0. Denotando I_i' al deshomogeneizado de I_i tenemos la descomposición $\langle f,g\rangle = I_1' \cap ... \cap I_r'$.

Recordemos que la multiplicidad de intersección #2 de $V(F), V(G)$ en p se define como:

$$\text{mult}_2(V(F), V(G))_p = P_{I_1}(\ell) = h_{I_1}(\ell) = \dim_{\mathbb{K}} \frac{\mathbb{K}[X_0, X_1, X_2]_\ell}{(I_1)_\ell} \tag{4.1}$$

con $\ell \in \mathbb{N}$ lo suficientemente grande. Siguiendo la misma demostración del Lema 4.14 y haciendo uso de que $\mathbb{K}[X_0, X_1, X_2]$ es un anillo noetheriano se puede ver que:

$$\frac{\mathbb{K}[X_0, X_1, X_2]_\ell}{(I_i)_\ell} \cong \frac{\mathbb{K}[X, Y]}{I_i'} \tag{4.2}$$

como $\mathbb{K}$-espacios vectoriales (solo hace falta escribir $I_i = \langle F_1, ..., F_r \rangle$ y ajustar el valor de ℓ a los grados de dichos polinomios generadores). Juntando (4.1) y (4.2) obtenemos el resultado buscado.

■

Proposición 4.16 *Bajo las hipótesis de la Proposición 4.15 y utilizando su misma notación, supongamos que $p = (1 : 0 : 0) \in V(F) \cap V(G)$ de tal forma que el único punto de intersección de $V(f)$ y $V(g)$ con $X = 0$ es el origen. En esta situacion, se cumplen las siguientes propiedades:*

1. *La aplicación natural φ dada por:*

$$\frac{\mathbb{K}[X, Y]}{\langle f, g \rangle} \xrightarrow{\varphi} \frac{\mathbb{K}[[X]][Y]}{\langle f, g \rangle} \qquad h + \langle f, g \rangle \mapsto h + \langle f, g \rangle$$

   es suprayectiva.

2. $\ker \varphi = I_1' / \langle f, g \rangle$ *con la notación de la Proposición 4.15.*

3. *φ induce un isomorfismo $\mathbb{K}[X, Y]/I_1' \cong \mathbb{K}[[X]][Y]/\langle f, g \rangle$, lo que hace que ambos espacios tengan la misma dimensión como $\mathbb{K}$-espacios vectoriales.*

Demostración: Siguiendo la notación de la Proposición 4.15, recordemos que tenemos las siguientes descomposiciones:

$$\langle F, G \rangle = I_1 \cap ... \cap I_r \qquad \langle f, g \rangle = I_1' \cap ... \cap I_r'$$

Si escribimos la resultante de f, g respecto de Y, como $(0, 0)$ es raíz común de f, g:

$$res_Y(f, g) = X^s u(X) \in \langle f, g \rangle \qquad \text{tal que} \qquad u(0) \neq 0$$

Dado que tenemos la inclusión natural $\mathbb{K}[X, Y] \subseteq \mathbb{K}[[X]][Y]$, y como $u(X)$ es una unidad en $\mathbb{K}[[X]]$, se tiene que $X^s \in \langle f, g \rangle$. Más aún, como $u(0) \neq 0$, entonces $u(X) \notin I_1'$ y necesariamente $u(X) \in I_2' \cap ... \cap I_r'$. Podemos ahora demostrar cada una de las afirmaciones.

(1.) Tomamos un elemento $h + \langle f, g \rangle \in \mathbb{K}[[X]][Y]/\langle f, g \rangle$, si denotamos como $\bar{h}$ al polinomio resultado de truncar la serie formal h a orden $s - 1$, por lo comentado anteriormente se tiene que $h + \langle f, g \rangle = \bar{h} + \langle f, g \rangle$, por lo que $h + \langle f, g \rangle = \varphi(\bar{h} + \langle f, g \rangle)$.

(2.) En primer lugar, $I_1'/\langle f, g \rangle$ es un ideal de $\mathbb{K}[X, Y]/\langle f, g \rangle$ puesto que $\langle f, g \rangle \subseteq I_1'$. Para probar el contenido [$\supseteq$], tomamos $h \in I_1'$. Es claro que $hu(X) \in \langle f, g \rangle$, por lo que:

$$\begin{aligned} 0 + \langle f, g \rangle = \varphi(0 + \langle f, g \rangle) = \varphi(hu(X) + \langle f, g \rangle) = \varphi(h + \langle f, g \rangle)\varphi(u(X) + \langle f, g \rangle) = \\ = (h + \langle f, g \rangle)(u(X) + \langle f, g \rangle) = hu(X) + \langle f, g \rangle \;\Rightarrow\; hu(X) \in \langle f, g \rangle \end{aligned}$$

En particular, como $u(X)$ es una unidad en $\mathbb{K}[[X]]$, entonces $h \in \langle f, g\rangle$, por lo que $\varphi((h + \langle f, g\rangle) = 0 + \langle f, g\rangle$, probando así el contenido. Nótese que hay que tener siempre presente cuando los ideales viven en $\mathbb{K}[X, Y]$ y cuando viven en $\mathbb{K}[[X]][Y]$.

Para el otro contenido [$\subseteq$], tomamos $h \in \ker \varphi$. En particular, sabemos que $h + \langle f, g\rangle \equiv 0$, por lo que $h = h_1 f + h_2 g$ con $h_1, h_2 \in \mathbb{K}[[X]][Y]$. Dichas series de potencias siempre las vamos a poder escribir como $h_1 = \overline{h_1} + X^s h_1'$ y $h_2 = \overline{h_2} + X^s h_2'$ donde $\overline{h_1}$, $\overline{h_2}$ son los polinomios resultado de trucar la serie a orden $s-1$ y h_1', h_2' son series de potencias. De esta forma:

$$h = \overline{h_1} f + X^s h_1' f + \overline{h_2} g + X^s h_2' g \qquad \Rightarrow \qquad h - \overline{h_1} f - \overline{h_2} g = X^s (h_1' f + h_2' g)$$

es decir, $h - \overline{h_1} f - \overline{h_2} g \in \mathbb{K}[X, Y]$ y además es múltiplo de X^s si lo vemos como serie formal. Consecuentemente, vamos a poder escribir $h - \overline{h_1} f - \overline{h_2} g = X^s h'$ con $h' \in \mathbb{K}[X, Y]$. Multiplicando por la unidad $u(X)$ obtenida en la resultante de f, g:

$$hu = \overline{h_1} f u + \overline{h_2} g u + X^s u h' \in \langle f, g\rangle$$

puesto que $X^s u \in \langle f, g\rangle$. En particular, $hu \in I_1'$, y como $u(0) \neq 0$, entonces $u \notin \sqrt{I_1'}$. Por ser I_1' primario, se tiene que $h \in I_1'$, tal y como queríamos probar.

(3.) Por el Primer y Segundo Teorema de Isomorfía aplicado sobre φ tenemos que

$$\frac{\mathbb{K}[X, Y]}{I_1'} \cong \frac{\mathbb{K}[X, Y]/\langle f, g\rangle}{I_1'/\langle f, g\rangle} \cong \frac{\mathbb{K}[X, Y]/\langle f, g\rangle}{\ker \varphi} \cong \frac{\mathbb{K}[[X]][Y]}{\langle f, g\rangle} \tag{4.3}$$

Esta cadena de isomorfismos nos arroja el resultado que buscábamos.

■

Una vez hemos trasladado la noción de multiplicidad al anillo de series formales, debemos ser capaces de separar las contribuciones de cada rama.

Observación 4.17 *Siguiendo la notación de la Observación 4.11 y suponiendo f mónico en Y, una forma natural de separar las contribuciones de cada una de las ramas sería probar que el morfismo natural*

$$\frac{\mathbb{K}[[X]][Y]}{\langle f, g\rangle} \xrightarrow{\psi} \bigoplus_{i=1}^{t} \frac{\mathbb{K}[[X]][Y]}{\langle f_i, g\rangle} \qquad \psi(h + \langle f, g\rangle) := [h + \langle f_1, g\rangle, ..., h + \langle f_t, g\rangle]$$

es un isomorfismo. No obstante, se puede comprobar que no es aplicable el Teorema Chino del Resto (ni antes ni después de cocientar por el polinomio g) y que por lo general esta afirmación es falsa, tal y como se puede comprobar en el siguiente ejemplo.

Ejemplo 4.18 *Consideremos los polinomios $f = Y^2 - X^2 - X^3$ y $g = X$ y estudiemos las distintas ramas de $V(f)$ en el origen. Se puede ver fácilmente que $V(f)$ tiene dos ramas en el origen dadas por las series formales:*

$$p_1 = X + \frac{1}{2}X^2 + ... \qquad p_2 = -X - \frac{1}{2}X^2 + ...$$

De esta forma, la aplicación ψ tiene el aspecto:

$$\frac{\mathbb{K}[[X]][Y]}{\langle Y^2 - X^2 - X^3, X\rangle} \xrightarrow{\psi} \frac{\mathbb{K}[[X]][Y]}{\langle Y + p_1, X\rangle} \oplus \frac{\mathbb{K}[[X]][Y]}{\langle Y + p_2, X\rangle} = \frac{\mathbb{K}[[X]][Y]}{\langle X, Y\rangle} \oplus \frac{\mathbb{K}[[X]][Y]}{\langle X, Y\rangle}$$

$$\psi(h + \langle Y^2 - X^2 - X^3, X\rangle) := [h + \langle X, Y\rangle, h + \langle X, Y\rangle]$$

Por lo que la imagen de ψ es la diagonal, así que dicha aplicación no puede ser sobreyectiva.

Como consecuencia de la Observación 4.17, debemos hacer uso de herramientas más profundas como es el Lema de la serpiente 1.18. Con él, probaremos que tanto el núcleo como el conúcleo de ψ tienen la misma dimensión, lo que será suficiente para probar que las dimensiones tanto del dominio como codominio de ψ coinciden.

Para poder aplicar el Lema de la serpiente, debemos demostrar un lema previo en el que solo participa una de las curvas iniciales.

Lema 4.19 *Con la notación introducida en la Observación 4.11, el conúcleo de la aplicación ϕ dada por*

$$\frac{\mathbb{K}[[X]][Y]}{\langle f\rangle} \xrightarrow{\phi} \bigoplus_{i=1}^{t} \frac{\mathbb{K}[[X]][Y]}{\langle f_i\rangle} \qquad \phi(h+\langle f\rangle) := [h+\langle f_1\rangle, ..., h+\langle f_t\rangle]$$

es un espacio vectorial de dimensión finita.

Demostración: Nuestra intención es aplicar el Teorema Chino del Resto sobre la descomposición $f = f_1 \cdot \cdots \cdot f_t$. Como los f_i no son coprimos sobre $\mathbb{K}[[X]][Y]$, debemos trabajar sobre el anillo de polinomios con coeficientes en el cuerpo de fracciones $\mathbb{K}((X))$. Así, introducimos los siguientes anillos:

$$\frac{\mathbb{K}((X))[Y]}{\langle f\rangle} \qquad \frac{\mathbb{K}((X))[Y]}{\langle f_i\rangle}$$

Ya sobre estos nuevos anillos, los polinomios f_i son coprimos entre sí, puesto que son polinomios irreducibles distintos en la indeterminada Y y coeficientes en el cuerpo $\mathbb{K}((X))$ (nótese que son irreducibles en $\mathbb{K}[[X]][Y]$ por la Observación 4.11 y por el Lema de Gauss [4] también lo son en $\mathbb{K}((X))[Y]$). Consecuentemente, podemos aplicar el Teorema Chino del Resto [4], con el que concluimos que:

$$\frac{\mathbb{K}((X))[Y]}{\langle f\rangle} \cong \bigoplus_{i=1}^{t} \frac{\mathbb{K}((X))[Y]}{\langle f_i\rangle}$$

donde el isomorfismo vendrá dado por el morfismo natural análogo a ϕ. En particular, los elementos $e_1 := [1+\langle f_1\rangle, 0, ..., 0], e_2 := [0, 1+\langle f_2\rangle, 0, ..., 0], \dots e_t := [0, ..., 0, 1+\langle f_t\rangle]$ tendrán preimágenes en $\mathbb{K}((X))[Y]/\langle f\rangle$. Cada una de las preimágenes $\{h_1+\langle f\rangle, ..., h_t+\langle f\rangle\}$ es una clase cuyo representante es un polinomio con coeficientes en $\mathbb{K}((X))$. Nótese que cada polinomio h_i tiene un número finito de coeficientes, cada uno de ellos con un denominador que es potencia de X. Escogiendo a mayor que todos los exponentes de X que aparecen en los denominadores de los h_i tenemos que los polinomios $X^a h_i$ tienen sus coeficientes en $\mathbb{K}[[X]]$ y por tanto sus imágenes por ϕ:

$$\phi\left(h_i+\langle f\rangle\right) = e_i \qquad \Rightarrow \qquad \phi(X^a h_i+\langle f\rangle) = X^a e_i$$

por lo que las tuplas de la forma $X^a e_i \in \mathrm{im}(\phi)$. Esto nos permite afirmar que toda tupla de la forma pe_i donde $p \in \mathbb{K}[[X]][Y]$ tiene orden al menos a en X pertenece a la imagen de ϕ, pues siempre podemos escribir $p = X^a p'$ y por tanto pe_i es imagen de $X^a h_i p' + \langle f\rangle$. Finalmente, como cada f_i tiene grado r_i en Y, si tenemos una tupla de la forma pe_i con $p \in \mathbb{K}[[X]][Y]$ de grado mayor que r_i, siempre podemos dividir por f_i, y por tanto $p+\langle f_i\rangle = r+\langle f_i\rangle$ donde r es el resto de la división y su grado sobre Y es estrictamente menor que r_i.

Una vez hecho este análisis, observamos que el conúcleo de ϕ está generado por las tuplas de la forma $X^\ell Y^m e_i$ con $\ell < a$ y $m < r_i$, por lo que el conúcleo de ϕ tiene dimensión finita.

■

Estamos ya preparados para aplicar el Lema de la serpiente y así separar las contribuciones de cada una de las ramas de $V(f)$.

Proposición 4.20 *Con las hipótesis y notación de la Proposición 4.16 y suponiendo que f es mónico en Y, se satisface:*

$$\dim_{\mathbb{K}} \frac{\mathbb{K}[[X]][Y]}{\langle f, g\rangle} = \sum_{i=1}^{t} \dim_{\mathbb{K}} \frac{\mathbb{K}[[X]][Y]}{\langle f_i, g\rangle}$$

Donde $f = f_1 \cdot ... \cdot f_t$ es la descomposición de f vista en la Observación 4.11.

Demostración: Consideremos el siguiente diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{K}[[X]][Y]/\langle f\rangle & \xrightarrow{\alpha} & \mathbb{K}[[X]][Y]/\langle f\rangle & \xrightarrow{\pi} & \mathbb{K}[[X]][Y]/\langle f, g\rangle & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & \bigoplus_{i=1}^{t} \mathbb{K}[[X]][Y]/\langle f_i\rangle & \xrightarrow{\beta} & \bigoplus_{i=1}^{t} \mathbb{K}[[X]][Y]/\langle f_i\rangle & \xrightarrow{\pi'} & \bigoplus_{i=1}^{t} \mathbb{K}[[X]][Y]/\langle f_i, g\rangle & \longrightarrow & 0 \end{array}$$

donde π y π' son las proyecciones correspondientes a los cocientes y el resto de morfismos se definen como sigue:

$$\phi(h + \langle f\rangle) := [h + \langle f_1\rangle, ..., h + \langle f_t\rangle] \qquad \psi(h + \langle f, g\rangle) := [h + \langle f_1, g\rangle, ..., h + \langle f_t, g\rangle]$$

$$\alpha(h + \langle f\rangle) := hg + \langle f\rangle \qquad \beta([h_1 + \langle f_1\rangle, ..., h_t + \langle f_t\rangle]) := [h_1 g + \langle f_1\rangle, ..., h_t g + \langle f_t\rangle]$$

Comprobemos que dicho diagrama satisface las hipótesis del Lema 1.18 de la serpiente.

Para la fila superior, es claro que π es epimorfismo por ser una proyección. Además, el morfismo α es monomorfismo. En efecto, si $h \in \ker(\alpha)$ entonces $hg \in \langle f\rangle$. Pero como f, g son coprimos, entonces $h \in \langle f\rangle$, con lo que concluimos que $h + \langle f\rangle \equiv 0 + \langle f\rangle$. Finalmente, para ver la exactitud en la posición central:

$$\ker(\pi) = \{h + \langle f\rangle \mid h \in \langle f, g\rangle\} = \{h + \langle f\rangle \mid h = h_1 f + h_2 g\} = \{h + \langle f\rangle \mid h + \langle f\rangle = h_2 g + \langle f\rangle\}$$

$$\mathrm{im}(\alpha) = \{hg + \langle f\rangle \mid h \in \mathbb{K}[[X]][Y]\}$$

por lo que efectivamente, $\ker(\pi) = \mathrm{im}(\alpha)$.

Para la fila inferior, es claro que π' es epimorfismo por ser una proyección, mientras que β es monomorfismo. En efecto, si $[h_1 + \langle f_1\rangle, ..., h_t + \langle f_t\rangle] \in \ker(\beta)$ entonces $h_i g \in \langle f_i\rangle$ para todo i. Pero como los f_i son irreducibles en $\mathbb{K}[[X]][Y]$ y $\mathbb{K}[[X]][Y]$ es un DFU, entonces los $\langle f_i\rangle$ son primos. Y dado que f, g no comparten factores irreducibles, entonces $g \notin \langle f_i\rangle$ para todo i, con lo que concluimos que $h_i \in \langle f_i\rangle$ y por ello se tiene $[h_1 + \langle f_1\rangle, ..., h_t + \langle f_t\rangle] \equiv [0 + \langle f_1\rangle, ..., 0 + \langle f_t\rangle]$. Finalmente, para ver la exactitud en la posición central:

$$\ker(\pi') = \{[h_1 + \langle f_1\rangle, ..., h_t + \langle f_t\rangle] \mid h_i = \delta_i f_i + \gamma_i g\} = \{[h_1 + \langle f_1\rangle, ..., h_t + \langle f_t\rangle] \mid h_i + \langle f_i\rangle = \gamma_i g + \langle f_i\rangle\}$$

$$\mathrm{im}(\beta) = \{[h_1 g + \langle f_1\rangle, ..., h_t g + \langle f_t\rangle]\}$$

por lo que efectivamente $\ker(\pi') = \mathrm{im}(\beta)$.

Además, es claro por construcción que tanto el primer cuadrado como el segundo son conmutativos. Podemos aplicar entonces el Lema de la serpiente y concluir que la sucesión

$$0 \to \ker(\phi) \to \ker(\phi) \to \ker(\psi) \to \mathrm{coker}(\phi) \to \mathrm{coker}(\phi) \to \mathrm{coker}(\psi) \to 0 \tag{4.4}$$

está bien definida y es exacta. Hay que notar también que ϕ es monomorfismo, por lo que su núcleo es nulo. En efecto, si $h \in \langle f_i \rangle$ para todo i, entonces directamente $h = h'f$, por lo que $h \in \langle f \rangle$. Esto simplifica sustancialmente la sucesión exacta (4.4):

$$0 \to \ker(\psi) \to \operatorname{coker}(\phi) \to \operatorname{coker}(\phi) \to \operatorname{coker}(\psi) \to 0 \tag{4.5}$$

Además, hay que notar que tanto $\operatorname{coker}(\psi)$ como $\ker(\psi)$ son espacios vectoriales de dimensión finita por tener los espacios $\mathbb{K}[[X]][Y]/\langle f, g\rangle$ y $\bigoplus_{i=1}^{t} \mathbb{K}[[X]][Y]/\langle f_i, g\rangle$ dimensión finita, y a su vez, $\operatorname{coker}(\phi)$ es un espacio vectorial de dimensión finita por el Lema 4.19.

Así, aplicando el Lema 1.17 a la sucesión (4.5) concluimos que $\dim_{\mathbb{K}}\ker(\psi) = \dim_{\mathbb{K}}\operatorname{coker}(\psi)$, por lo que volviendo a aplicar el Lema 1.17 a la siguiente sucesión (que es exacta por el Lema 1.16):

$$0 \to \ker(\psi) \xhookrightarrow{i} \mathbb{K}[[X]][Y]/\langle f, g\rangle \xrightarrow{\psi} \bigoplus_{i=1}^{t} \mathbb{K}[[X]][Y]/\langle f_i, g\rangle \xrightarrow{p} \operatorname{coker}(\psi) \to 0$$

concluimos que:

$$\dim_{\mathbb{K}} \frac{\mathbb{K}[[X]][Y]}{\langle f, g\rangle} = \sum_{i=1}^{t} \dim_{\mathbb{K}} \frac{\mathbb{K}[[X]][Y]}{\langle f_i, g\rangle}$$

■

Para acabar de conectar ambas definiciones necesitamos un último paso, que consiste en calcular la dimensión de cada cociente $\mathbb{K}[[X]][Y]/\langle f_i, g\rangle$ y relacionarla con la multiplicidad de intersección de cada rama con la curva $V(g)$.

Observación 4.21 *Al igual que antes, una forma natural de probar que la dimensión de cada término* $\mathbb{K}[[X]][Y]/\langle f_i, g\rangle$ *coincide con* $\operatorname{mult}_{(0,0)}(V(g), R_i)$ *sería comprobar que la aplicación*

$$\frac{\mathbb{K}[[X]][Y]}{\langle f_i, g\rangle} \xrightarrow{\tilde{\psi}} \frac{\mathbb{K}[[T]]}{\langle T^{m_i}\rangle} \qquad \tilde{\psi}(h + \langle f_i, g\rangle) := h(T^{r_i}, p_i(T)) + \langle T^{m_i}\rangle$$

es un isomorfismo (véase la Observación 4.12). Lamentablemente, por lo general esta afirmación es falsa, tal y como muestra el siguiente ejemplo.

Ejemplo 4.22 *Consideremos los polinomios* $f = Y^2 - X^3$ *y* $g = Y$ *y estudiemos las distintas ramas de* $V(f)$ *en el origen. Está claro que* $f = (Y + X^{3/2})(Y - X^{3/2})$*, por lo que* $V(f)$ *tiene una única rama en el origen que viene dada por el propio polinomio* f *(es decir, en la notación de la observación anterior,* $f_i = f$ *y* $r_i = 2$*). La serie de Puiseux asociada (salvo conjugación) es* $q_i(T) \equiv q(T) = T^{3/2}$*, y la serie formal asociada es* $p_i(T) \equiv p(T) = T^3$*. Además, como* $g = Y$*, se tiene que* $g(T^2, p(T)) = T^3$ *y por tanto* $m_i = 3$*.*

La aplicación $\tilde{\psi}$ *entonces toma la forma:*

$$\frac{\mathbb{K}[[X]][Y]}{\langle Y^2 - X^3, Y\rangle} \xrightarrow{\tilde{\psi}} \frac{\mathbb{K}[[T]]}{\langle T^3\rangle} \qquad \tilde{\psi}(h + \langle Y^2 - X^3, Y\rangle) := h(T^2, T^3) + \langle T^3\rangle$$

Dicha aplicación no es sobreyectiva. Si lo fuera, existiría un polinomio $h \in \mathbb{K}[[X]][Y]$ *tal que* $h(T^2, T^3) + \langle T^3\rangle = T + \langle T^3\rangle$*. Pero esto no es posible, pues los monomios no constantes de* $h(T^2, T^3)$ *tienen todos grado al menos 2 (recordemos que* h *no tiene exponentes fraccionarios).*

Sin embargo, $T + \langle T^3\rangle$ *sí que es imagen de la clase* $Y/X + \langle Y^2 - X^3, Y\rangle$*, lo que motiva la introducción del cuerpo de fracciones* $\mathbb{K}((X))$ *en el siguiente lema.*

De forma similar al paso anterior, haremos uso del Lema de la serpiente, con el que probaremos que tanto el núcleo como conúcleo de $\tilde{\psi}$ tienen la misma dimensión. Para ello, demostramos un lema previo.

Lema 4.23 *Con la notación introducida en la Observación 4.12, el conúcleo de la aplicación $\tilde{\phi}$ dada por*

$$\frac{\mathbb{K}[[X]][Y]}{\langle f_i\rangle} \xrightarrow{\tilde{\phi}} \mathbb{K}[[T]] \qquad \tilde{\phi}(h + \langle f_i\rangle) := h(T^{r_i}, p_i(T))$$

es un espacio vectorial de dimensión finita.

Demostración: En primer lugar vamos a comprobar el siguiente isomorfismo

$$\frac{\mathbb{K}[[X]][Y]}{\langle f_i\rangle} \cong \mathbb{K}[[X]][q_i] \tag{4.6}$$

Si definimos la aplicación $\mathbb{K}[[X]][Y] \xrightarrow{\gamma} \mathbb{K}[[X]][q_i]$ que consiste en evaluar Y en q_i, podemos comprobar fácilmente que su núcleo son aquellos polinomios $h \in \mathbb{K}[[X]][Y]$ que tienen q_i como raíz. Como f_i es el polinomio mínimo de q_i, se tiene que $\ker \gamma = \langle f_i\rangle$. Además, es claro que γ es sobreyectiva. Por ello, sin más que aplicar el Primer Teorema de Isomorfía se prueba (4.6)

A su vez, trabajando sobre los cuerpos

$$\frac{\mathbb{K}((X))[Y]}{\langle f_i\rangle} \qquad \mathbb{K}((X))[q_i]$$

y de forma similar a (4.6) se prueba que $\mathbb{K}((X))[Y]/\langle f_i\rangle \cong \mathbb{K}((X))[q_i]$.

Otra cosa que debemos comprobar es que $\mathbb{K}[[X^{1/r_i}]] = \mathbb{K}[[X]][X^{1/r_i}]$. Veamos en primer lugar que un elemento $h \in \mathbb{K}[[X^{1/r_i}]]$ siempre se puede escribir como $h = h_0 + ... + h_{r_i-1}X^{(r_i-1)/r_i}$ con los $h_j \in \mathbb{K}[[X]]$. En efecto, si $h(X) = \sum_{k=0}^{\infty} a_k X^{k/r_i}$ con $a_k \in \mathbb{K}$, aplicando el algoritmo de división de los enteros y quedándonos con resto positivo, siempre podemos escribir $k = r_i m + n$ con $0 \leq n < r_i$, por lo que $X^{k/r_i} = X^{(mr_i+n)/r_i} = X^m X^{n/r_i}$. Metiendo los X^m en los coeficientes a_k y agrupando términos tenemos la representación buscada. Esto también prueba la inclusión $\mathbb{K}[[X^{1/r_i}]] \subseteq \mathbb{K}[[X]][X^{1/r_i}]$. Para la otra inclusión, tomamos $h \in \mathbb{K}[[X]][X^{1/r_i}]$ que se puede escribir como $h = h_{j_1}X^{j_1/r_i} + ... + h_{j_s}X^{j_s/r_i}$ con los $h_{j_k} \in \mathbb{K}[[X]]$. Introduciendo los X^{j_k/r_i} en los h_{j_k} y haciendo común denominador r_i en los exponentes de las indeterminadas X, tras reorganizar términos se puede ver que $h \in \mathbb{K}[[X^{1/r_i}]]$, probando el otro contenido. El mismo argumento nos permite probar que $\mathbb{K}((X^{1/r_i})) = \mathbb{K}((X))[X^{1/r_i}]$, donde $\mathbb{K}((X^{1/r_i}))$ es el cuerpo de fracciones de $\mathbb{K}[[X^{1/r_i}]]$

En este punto hay que observar que tanto $\mathbb{K}((X^{1/r_i}))$ como $\mathbb{K}((X))[q_i]$ son extensiones de cuerpos sobre $\mathbb{K}((X))$, y ambas con el mismo grado de extensión r_i, por lo que dichos cuerpos son en realidad el mismo. Por un lado, $P_1(T) := f_i(T) = \prod_j^{r_i}(T - q_{ij})$ es el polinomio mínimo de q_i sobre $\mathbb{K}((X))$, por lo que la extensión de $\mathbb{K}((X))[q_i]$ sobre $\mathbb{K}((X))$ tiene grado r_i. De forma similar, si definimos $P_2(T) := T^{r_i} - X$, dicho polinomio se anula en X^{1/r_i} y es irreducible. Esto último se puede ver utilizando el Criterio de Eisenstein [4], puesto que P_2 es primitivo y X divide a a_0 pero X^2 no.

Visto esto tenemos el siguiente isomorfismo:

$$\tilde{\phi}: \ \frac{\mathbb{K}((X))[Y]}{\langle f_i\rangle} \cong \mathbb{K}((X))[q_i] = \mathbb{K}((X^{1/r_i})) \cong \mathbb{K}((T))$$

donde el último isomorfismo consiste en sustituir $X \mapsto T^{r_i}$. Tenemos por tanto un isomorfismo $\mathbb{K}((X))[Y]/\langle f_i\rangle \cong \mathbb{K}((T))$ definido de forma similar a $\tilde{\phi}$. En particular, las series $\{T, T^2, T^3, ..., T^{r_i-1}\}$ tienen preimágenes que son clases de polinomios $\{h_1, .., h_{r_i-1}\}$. Siendo a mayor que todos los exponentes de X que aparecen en los denominadores de $\{h_1, .., h_{r_i-1}\}$, tenemos que cada $X^a h_j$ está en $\mathbb{K}[[X]][Y]$ y su imagen por $\tilde{\phi}$ será T^{ar_i+j}:

$$\tilde{\phi}(h_j + \langle f_i\rangle) = T^j \qquad \Rightarrow \qquad \tilde{\phi}(X^a h_j + \langle f_i\rangle) = T^{ar_i+j}$$

Por tanto, los monomios $\{T^{ar_i+1}, .., T^{ar_i+r_i-1}\} \in \mathrm{im}(\tilde{\phi})$. Finalmente, cada serie $p(T)$ de orden estrictamente mayor que ar_i se puede reescribir (agrupando exponentes según su clase módulo r_i) como $p(T) = p_0(T^{r_i}) + T^{ar_i+1}p_1(T^{r_i}) + ... + T^{ar_i+r_i-1}p_{r_i-1}(T^{r_i})$, lo que hace que $p \in \mathrm{im}(\tilde{\phi})$, pues los $p_k(T^{r_i})$ son imagen de $p_k(X)$. Esto nos permite concluir que el conúcleo de $\tilde{\phi}$ está generado por los monomios $\{1, T, ..., T^{ar_i}\}$ y por tanto tiene dimensión finita.

■

Enunciamos y demostramos el último resultado antes de poder enunciar en su totalidad el Teorema de equivalencia de definiciones de multiplicidad de intersección.

Proposición 4.24 *Con las hipótesis y notación de la Proposición 4.16 y suponiendo que f es mónico en Y, se satisface:*

$$\dim_{\mathbb{K}} \frac{\mathbb{K}[[X]][Y]}{\langle f_i, g\rangle} = \dim_{\mathbb{K}} \frac{\mathbb{K}[[T]]}{\langle T^{m_i}\rangle} = m_i = \mathrm{mult}_{(0,0)}(V(g), R_i) \qquad i = 1, ..., t$$

Donde R_i es la rama asociada a f_i y el exponente m_i es el que se obtiene de sustituir la rama R_i en la ecuación de g, tal y como se explica en las Observaciones 4.11 y 4.12.

Demostración: Para cada rama f_i consideremos el siguiente diagrama:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{K}[[X]][Y]/\langle f_i\rangle & \xrightarrow{\tilde{\alpha}} & \mathbb{K}[[X]][Y]/\langle f_i\rangle & \xrightarrow{\tilde{\pi}} & \mathbb{K}[[X]][Y]/\langle f_i, g\rangle & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{\phi}} & & \downarrow{\scriptstyle \tilde{\phi}} & & \downarrow{\scriptstyle \tilde{\psi}} & & \\ 0 & \longrightarrow & \mathbb{K}[[T]] & \xrightarrow{\tilde{\beta}} & \mathbb{K}[[T]] & \xrightarrow{\tilde{\pi}'} & \mathbb{K}[[T]]/\langle T^{m_i}\rangle & \longrightarrow & 0 \end{array}$$

donde $\tilde{\pi}$ y $\tilde{\pi}'$ son las proyecciones correspondientes a los cocientes y el resto de morfismos se definen como sigue:

$$\tilde{\phi}(h + \langle f_i\rangle) := h(T^{r_i}, p_i(T)) \qquad \tilde{\psi}(h + \langle f_i, g\rangle) := h(T^{r_i}, p_i(T)) + \langle T^{m_i}\rangle$$

$$\tilde{\alpha}(h + \langle f_i\rangle) := hg + \langle f_i\rangle \qquad \tilde{\beta}(h) := hT^{m_i}v_i$$

Donde hemos hecho uso de que $g(T^{r_i}, p_i(T)) = T^{m_i}v_i(T)$ con $v_i(0) \neq 0$. Al igual que antes, comprobemos que dicho diagrama satisface las hipótesis del Lema 1.18 de la serpiente.

Para la fila superior, es claro que $\tilde{\pi}$ es epimorfismo por ser una proyección. Además, el morfismo $\tilde{\alpha}$ es monomorfismo. En efecto, si $h \in \ker(\tilde{\alpha})$ entonces $hg \in \langle f_i\rangle$. Pero como f_i es irreducible en $\mathbb{K}[[X]][Y]$ y $\mathbb{K}[[X]][Y]$ es un DFU, entonces $\langle f_i\rangle$ es primo. Y dado que f, g no comparten factores irreducibles, entonces $g \notin \langle f_i\rangle$, con lo que concluimos que $h \in \langle f_i\rangle$ y por ello $h + \langle f_i\rangle \equiv 0 + \langle f_i\rangle$. Finalmente, para ver la exactitud en la posición central:

$$\ker(\tilde{\pi}) = \{h + \langle f_i\rangle \mid h \in \langle f_i, g\rangle\} = \{h + \langle f_i\rangle \mid h = h_1 f_i + h_2 g\} = \{h + \langle f_i\rangle \mid h + \langle f_i\rangle = h_2 g + \langle f_i\rangle\}$$

$$\mathrm{im}(\tilde{\alpha}) = \{hg + \langle f_i \rangle \mid h \in \mathbb{K}[[X]][Y]\}$$

por lo que efectivamente, $\ker(\tilde{\pi}) = \mathrm{im}(\tilde{\alpha})$.

Para la fila inferior, es claro que $\tilde{\pi}'$ es epimorfismo por ser una proyección, mientras que $\tilde{\beta}$ es monomorfismo por ser el elemento $T^{m_i}v_i$ no nulo y ser $\mathbb{K}[[T]]$ un DI. Finalmente, para ver la exactitud en la posición central:

$$\ker(\tilde{\pi}') = \{h \in \mathbb{K}[[T]] \mid h = \gamma T^{m_i}\} = \{h \in \mathbb{K}[[T]] \mid h = \gamma v_i^{-1} v_i T^{m_i}\}$$

$$\mathrm{im}(\tilde{\beta}) = \{\delta v_i T^{m_i} \mid \delta \in \mathbb{K}[[T]]\}$$

por lo que efectivamente $\ker(\tilde{\pi}') = \mathrm{im}(\tilde{\beta})$.

Además, es claro por construcción que tanto el primer como el segundo cuadrado son conmutativos. Podemos aplicar entonces el Lema de la serpiente y concluir que la sucesión

$$0 \to \ker(\tilde{\phi}) \to \ker(\tilde{\phi}) \to \ker(\tilde{\psi}) \to \mathrm{coker}(\tilde{\phi}) \to \mathrm{coker}(\tilde{\phi}) \to \mathrm{coker}(\tilde{\psi}) \to 0 \tag{4.7}$$

está bien definida y es exacta. Hay que notar en primer lugar que $\tilde{\phi}$ es monomorfismo, por lo que su núcleo es nulo. En efecto, si $h(T^{r_i}, p_i) = 0$, entonces:

$$h = h'(Y - q_i)^{\alpha} \qquad \text{con} \qquad h'(T, q_i(T)) \neq 0$$

pero como $h \in \mathbb{K}[[X]][Y]$, necesariamente han de estar todas las raíces conjugadas en h', por lo que $h = h'' f_i^{\alpha}$ y por tanto $h + \langle f_i \rangle \equiv 0 + \langle f_i \rangle$. Esto simplifica sustancialmente la sucesión exacta (4.7):

$$0 \to \ker(\tilde{\psi}) \to \mathrm{coker}(\tilde{\phi}) \to \mathrm{coker}(\tilde{\phi}) \to \mathrm{coker}(\tilde{\psi}) \to 0 \tag{4.8}$$

Además, hay que notar que tanto $\mathrm{coker}(\tilde{\psi})$ como $\ker(\tilde{\psi})$ son espacios vectoriales de dimensión finita por tener los espacios $\mathbb{K}[[X]][Y]/\langle f_i, g \rangle$ y $\mathbb{K}[[T]]/\langle T^{m_i} \rangle$ dimensión finita, y de la misma forma, $\mathrm{coker}(\tilde{\phi})$ también tiene dimensión finita por el Lema 4.23.

Así, aplicando el Lema 1.17 a la sucesión (4.8) concluimos que $\dim_{\mathbb{K}}\ker(\tilde{\psi}) = \dim_{\mathbb{K}}\mathrm{coker}(\tilde{\psi})$, por lo que volviendo a aplicar el Lema 1.17 a la siguiente sucesión (que es exacta por el Lema 1.16):

$$0 \to \ker(\tilde{\psi}) \xhookrightarrow{i} \mathbb{K}[[X]][Y]/\langle f_i, g \rangle \xrightarrow{\tilde{\psi}} \mathbb{K}[[T]]/\langle T^{m_i} \rangle \xrightarrow{p} \mathrm{coker}(\tilde{\psi}) \to 0$$

concluimos que:

$$\dim_{\mathbb{K}} \frac{\mathbb{K}[[X]][Y]}{\langle f_i, g \rangle} = \dim_{\mathbb{K}} \frac{\mathbb{K}[[T]]}{\langle T^{m_i} \rangle}$$

Para la última parte de la igualdad solo debemos aplicar lo visto en la Observación 4.12.

■

Estamos ya en disposición de enunciar y demostrar el teorema de equivalencias juntando todos los resultados obtenidos hasta ahora.

Teorema 4.25 (Equivalencia de las definiciones de multiplicidad) *Sean $C, D \subset \mathbb{P}^2$ dos curvas planas sin componentes irreducibles comunes, y sea $p \in C \cap D$ un punto de su intersección. Entonces* $\mathrm{mult}_1(C, D)_p = \mathrm{mult}_2(C, D)_p$

Demostración: Aplicando un cambio de coordenadas si es necesario podemos suponer que $p = (1 : 0 : 0)$. Además, si F, G son ecuaciones minimales de las curvas C, D respectivamente y f, g

son sus deshomogeneizados con respecto a la variable X_0, también podemos suponer que el único punto de intersección de $V(f)$ y $V(g)$ con $X = 0$ es el origen (esto siempre se puede hacer ya que $V(f) \cup V(g) \neq \mathbb{A}^2_{\mathbb{K}}$). Puesto que la condición de que las curvas no tengan componentes irreducibles comunes se traduce a que F, G sean coprimos, podemos aplicar las Proposiciones 4.15 y 4.16, por lo que, usando la misma notación que en dichas proposiciones, se tiene que:

$$\text{mult}_2(C, D)_p = \dim_{\mathbb{K}} \frac{\mathbb{K}[X, Y]}{I_1'} = \dim_{\mathbb{K}} \frac{\mathbb{K}[[X]][Y]}{\langle f, g \rangle} \tag{4.9}$$

Suponiendo a su vez que f es mónico en Y (lo que siempre se puede asumir sin más que aplicar una rotación), podemos aplicar las Proposiciones 4.20 y 4.24, lo que nos arroja la siguiente cadena de igualdades (siguiendo la notación utilizada en esas proposiciones):

$$\dim_{\mathbb{K}} \frac{\mathbb{K}[[X]][Y]}{\langle f, g \rangle} = \sum_{i=1}^{t} \dim_{\mathbb{K}} \frac{\mathbb{K}[[X]][Y]}{\langle f_i, g \rangle} = \sum_{i=1}^{t} \dim_{\mathbb{K}} \frac{\mathbb{K}[[T]]}{\langle T^{m_i} \rangle} \tag{4.10}$$

La Observación 4.12 nos permiten afirmar que cada $\mathbb{K}[[T]]/\langle T^{m_i} \rangle$ tiene dimensión m_i y que $m_i = \text{mult}_{(0,0)}(V(g), R_i)$ o bien $m_i = 0$ cuando f_i no represente una rama de $V(f)$ en el origen.

De esta forma, juntando (4.9) y (4.10) tenemos que:

$$\text{mult}_2(C, D)_p = \sum_{i=1}^{t} \dim_{\mathbb{K}} \frac{\mathbb{K}[[T]]}{\langle T^{m_i} \rangle} = \sum_{i=1}^{t} \text{mult}_{(0,0)}(V(g), R_i) = \text{mult}_1(C, D)_p$$

Lo que concluye la prueba.

■

Capítulo 5

Estudio de curvas planas mediante la Geometría Algebraica

Una vez desarrollada toda la teoría en torno al polinomio de Hilbert de los conjuntos proyectivos y habiendo comprobado que la definición de multiplicidad de intersección dada por el polinomio de Hilbert coincide con la usual, acabamos el trabajo demostramos un resultado fundamental en el estudio de las curvas planas como es el Teorema de Bézout en su versión débil y fuerte.

En la primera sección hacemos un estudio del concepto de dimensión y grado de un conjunto proyectivo (en cualquier dimensión), dando una interpretación geométrica a los mismos y concretando para el caso de curvas planas en el plano proyectivo $\mathbb{P}^2$. En la segunda y ultima sección abordaremos la demostración del Teorema de Bézout.

5.1. Dimensión y grado de un conjunto proyectivo

Definición 5.1 (Dimensión de un conjunto proyectivo) *La dimensión de un conjunto proyectivo $X \subseteq \mathbb{P}^n$ se define como el grado del polinomio de Hilbert de dicho conjunto.*

Esta definición cobra sentido geométrico a través del Lema 3.13. Además, dicho Lema pone de manifiesto que la dimensión de un conjunto proyectivo no depende del ideal que lo defina, esto es, si I, J son dos ideales homogéneos tales que $V(I) = V(J)$, entonces $\deg P_I = \deg P_J$.

Veamos que esta definición de dimensión coincide con la noción de dimensión que tenemos para los subespacios lineales de $\mathbb{P}^n$ [5].

Ejemplo 5.2 *Los espacios lineales Λ se definen como los ceros de un conjunto de formas lineales independientes:*

$$\Lambda = \{p \in \mathbb{P}^n \mid H_{r+1}(p) = ... = H_n(p) = 0 \text{ con } H_i \text{ polinomios homogéneos de grado 1 L.I.}\}$$

En esta situación, decimos que $\dim(\Lambda) = n - (n - r) = r$. *Veamos desde otro de punto de vista al subespacio Λ. Haciendo cambios de coordendas siempre podemos suponer que $H_i = X_i$. Calculemos entonces $I(\Lambda)$. Por un lado, es claro que $\langle H_{r+1}, ..., H_n \rangle \subseteq I(\Lambda)$. Para ver el otro contenido, tomamos un polinomio homogéneo F que se anule en Λ. Eso quiere decir que $F(a_0, ..., a_r, 0, ..., 0) = 0$*

para cualquier valor de $a_0, ..., a_r$. *Por tanto,* $F(X_0, ..., X_r, 0, ..., 0) = 0$ *como polinomio, lo que quiere decir que todos los monomios de* F *tienen algún* $X_{r+1}, ..., X_n$, *luego están en el ideal* $\langle H_{r+1}, ...H_n\rangle$ *y por tanto* $I(\Lambda) \subseteq \langle H_{r+1}, ...H_n\rangle$.

Una vez conocemos su ideal asociado, procedemos a calcular el grado de su polinomio de Hilbert. El conjunto $\{X_0^{i_0} \cdot ... \cdot X_r^{i_r} \mid i_0 + ... + i_r = \ell\}$ *es base para la parte homogénea de grado* ℓ *de* $\mathbb{K}[X_0, ..., X_r]$. *Dado que el número de elementos de la base es* $\binom{r+\ell}{r}$, *entonces* $h_{I(\Lambda)}(\ell) = \binom{r+\ell}{r} = \frac{1}{r!}\ell^r + ...$ *lo que hace que* $\deg(P_{I(\Lambda)}) = r$. *Observamos así que ambas nociones de dimensión coinciden para subespacios lineales.*

La otra noción geométrica importante asociada al polinomio de Hilbert es el grado de un conjunto proyectivo.

Definición 5.3 (Grado de un conjunto proyectivo) *Definimos el grado de un conjunto proyectivo* $X \subseteq \mathbb{P}^n$ *de dimensión* r *como* $\deg(X) = ar!$ *donde* a *es el coeficiente director del polinomio de Hilbert de* X.

El concepto de grado de un conjunto proyectivo es menos intuitivo que el de dimensión. Si cortamos X con hiperplanos generales del tipo $V(H_i)$ con H_i una forma lineal que no esté contenida en ningún primo asociado de $I(X)$ y si denotamos $P_{I(X)}(T) = aT^r + ...$, entonces por la Proposición 3.12 (5) tenemos que $P_{I(X)+\langle H_1\rangle}(T) = P_{I(X)}(T) - P_{I(X)}(T-1) = arT^{r-1} + ...$ Procediendo de forma inductiva, acabaremos teniendo $P_{I(X)+\langle H_1,...,H_r\rangle} = ar! = \deg(X)$, por lo que $V(I(X) + \langle H_1, ..., H_r\rangle) = X \cap V(H_1, ..., H_r)$ será un conjunto finito de $ar!$ puntos. Es por ello por lo que $\deg(X)$ determina el número de puntos de intersección de X con r hiperplanos generales contados con su multiplicidad. [5].

De especial interés va a ser el estudio del grado y dimensión de los conjuntos proyectivos definidos por un único polinomio [5], puesto que estos conjuntos proyectivos son las curvas planas cuando trabajemos en $\mathbb{P}^2$.

Lema 5.4 *Sea* $X \subseteq \mathbb{P}^n$ *un conjunto proyectivo tal que* $X = V(F)$ *con* F *un polinomio homogéneo de grado* $d > 0$ *e* $I(X) = \langle F\rangle$ *(i.e.* $\langle F\rangle$ *es un ideal radical). Entonces* $\dim(X) = n-1$ *y* $\deg(X) = d$.

Demostración: Consideramos la sucesión exacta graduada

$$0 \longrightarrow \mathcal{S}(-d) \xrightarrow{\phi_1} \mathcal{S} \longrightarrow \mathcal{S}/\langle F\rangle \longrightarrow 0$$

donde ϕ_1 es la aplicación inducida por el producto por F. Tal y como vimos en el Ejemplo 5.2, $\dim_{\mathbb{K}}(\mathcal{S}_\ell) = \binom{n+\ell}{n}$. Así, por la Proposición 3.5 tenemos que $P_{I(X)}(T) = \binom{n+T}{n} - \binom{n+T-d}{n} = \frac{d}{(n-1)!}T^{n-1} + ...$, de lo que extraemos directamente que $\dim(X) = n-1$ y $\deg(X) = d$.

■

Para el caso concreto del plano proyectivo, está claro que las curvas planas tienen dimensión 1 y grado igual al grado de una ecuación minimal suya.

5.2. Teorema de Bézout para curvas planas

Estamos ya en disposición de enunciar y demostrar la versión débil del Teorema de Bézout para curvas planas [5].

Teorema 5.5 (Débil de Bézout) *Sean $C, D \subset \mathbb{P}^2$ dos curvas sin componentes irreducibles comunes cuyas ecuaciones minimales son $F, G \in \mathbb{K}[X_0, X_1, X_2]$ respectivamente. Entonces $C \cap D$ consiste en, a lo sumo* $\deg(F) \cdot \deg(G)$ *puntos.*

Demostración: Sean $F = F_1 \cdot ... \cdot F_r$ y $G = G_1 \cdot ... \cdot G_s$ las descomposiciones en factores irreducibles de F, G. Como los polinomios irreducibles son primos, es claro que la descomposición en componentes irreducibles de C y D es $C = V(F_1) \cup ... \cup V(F_r)$ y $D = V(G_1) \cup ... \cup V(G_s)$. Además, la hipótesis de que C, D no compartan componentes irreducibles se traduce en que F y G son coprimos, lo que hace que en particular G no esté en ningún primo asociado de $\langle F \rangle$. Por tanto, podemos aplicar la Proposición 3.12 (5) y por ello $P_{\langle F,G \rangle}(T) = P_{\langle F \rangle}(T) - P_{\langle F \rangle}(T - \deg(G))$.

Como $\dim(C) = 1$ y $\deg(C) = \deg(F)$, entonces $P_{\langle F \rangle}(T) = \deg(F)T + A$ para cierto $A \in \mathbb{Q}$. Pero entonces $P_{\langle F,G \rangle}(T) = \deg(F)T + A - (\deg(F)(T - \deg(G)) + A) = \deg(G)\deg(F)$. Esto nos permite afirmar que $V(\langle F, G \rangle)$ es un conjunto finito de $\deg(G)\deg(F)$ puntos. Pero como $\langle F, G \rangle \subseteq I(C \cap D)$, entonces $C \cap D = V(I(C \cap D)) \subseteq V(\langle F, G \rangle)$ y por tanto $C \cap D$ consta de, a lo sumo, $\deg(G)\deg(F)$ puntos.

■

Finalmente, demostramos el Teorema fuerte de Bézout para curvas planas utilizando la definición #2 de multiplicidad de intersección introducida en el Capítulo 4 [5].

Teorema 5.6 (Fuerte de Bézout) *Sean $C, D \subset \mathbb{P}^2$ dos curvas sin componentes irreducibles comunes cuyas ecuaciones minimales son $F, G \in \mathbb{K}[X_0, X_1, X_2]$ respectivamente. Entonces $C \cap D$ consiste en* $\deg(F) \cdot \deg(G)$ *puntos contados con su multiplicidad.*

Demostración: Del Teorema débil de Bézout sabemos que F, G son coprimos y que $C \cap D$ es un conjunto finito de puntos $\{p_1, ..., p_r\}$ con $p_i \neq p_j$ si $i \neq j$. Además, por el Lema 1.15, $\langle F, G \rangle$ es saturado, por lo que su descomposición primaria no tiene componentes $\mathfrak{M}$-primarias. Así, podemos escribir $\langle F, G \rangle = I_1 \cap ... \cap I_r$ donde cada I_i es un ideal homogéneo $I(p_i)$-primario.

Vamos a probar por inducción que $P_{\langle F,G \rangle}(T) = P_{I_1 \cap ... \cap I_r}(T) = P_{I_1}(T) + ... + P_{I_r}(T)$. Para $r = 2$, por la Proposición 3.12 (1) se tiene que $P_{I_1 \cap I_2}(T) = P_{I_1}(T) + P_{I_2}(T) - P_{I_1 + I_2}(T)$, pero como $V(I_1 + I_2) = \{p_1\} \cap \{p_2\} = \emptyset$ entonces $P_{I_1 + I_2}(T) = 0$ y por tanto $P_{I_1 \cap I_2}(T) = P_{I_1}(T) + P_{I_2}(T)$. Supuesto cierto para $r - 1$, volvemos a aplicar la Proposición 3.12 (1) y entonces $P_{I_1 \cap ... \cap I_r}(T) = P_{I_1 \cap ... \cap I_{r-1}}(T) + P_{I_r}(T) - P_{(I_1 \cap ... \cap I_{r-1}) + I_r}(T)$ Pero como $V((I_1 \cap ... \cap I_{r-1}) + I_r) = \{p_1, ..., p_{r-1}\} \cap \{p_r\} = \emptyset$, entonces $P_{(I_1 \cap ... \cap I_{r-1}) + I_r}(T) = 0$ y por tanto $P_{I_1 \cap ... \cap I_r}(T) = P_{I_1 \cap ... \cap I_{r-1}}(T) + P_{I_r}(T) = P_{I_1}(T) + ... + P_{I_r}(T)$ sin más que aplicar la hipótesis de inducción.

Finalmente, como por definición $\text{mult}_2(C, D)_{p_i} = P_{I_i}(T)$ y ya vimos que $P_{\langle F,G \rangle} = \deg(F)\deg(G)$ tenemos finalmente que $\deg(F)\deg(G) = P_{\langle F,G \rangle}(T) = P_{I_1 \cap ... \cap I_r}(T) = P_{I_1}(T) + ... + P_{I_r}(T) = \text{mult}_1(C, D)_{p_1} + ... + \text{mult}_1(C, D)_{p_r}$, con lo que concluye la prueba.

■

Bibliografía

[1] E. Arrondo (2019) *Apuntes de Curvas Algebraicas*

`http://www.mat.ucm.es/~arrondo/curvas.pdf`

[2] E. Arrondo (2017) *Introduction to projective varieties*

`http://www.mat.ucm.es/~arrondo/projvar.pdf`

[3] M. Atiyah y I. MacDonald (1969) *Introduction to commutative algebra*. Addison-Wesley-Longman

[4] J.F.Fernando y J.M.Gamboa (2017) *Estructuras algebraicas: Divisibilidad en anillos conmutativos*. Sanz y Torres.

[5] J.L. López (2020) *Multiplicidades de intersección*. Trabajo de Fin de Grado de la Facultad de Ciencias Matemáticas de la UCM, curso 2019/2020.

`http://www.mat.ucm.es/~arrondo/TFG-JoseLuis.pdf`