
*Facultad de Ciencias*

# GÉNERO DE CURVAS ALGEBRAICAS

(Genus of Algebraic Curves)

Trabajo de Fin de Máster
para acceder al

**MÁSTER EN MATEMÁTICAS Y COMPUTACIÓN**

Autor: Diego López Álvarez

Director: Luis Felipe Tabera Alonso

Julio - 2015

# Resumen

El objetivo principal de la presente memoria es el estudio de las curvas algebraicas planas y, más concretamente, el desarrollo y la implementación en el software matemático *SAGE* de un algoritmo simbólico para calcular el género de una curva plana definida sobre $\mathbb{Q}$.

El estudio del género, que constituye el primer invariante birracional de una curva, resulta interesante para determinar su racionalidad o para estudiar la equivalencia birracional entre curvas. Para su cálculo emplearemos un método local afín basado en la explosión de singularidades.

Asimismo, profundizaremos en el estudio de las herramientas básicas del Álgebra Conmutativa tales como la descomposición primaria de ideales, y, con el fin de realizar únicamente operaciones racionales, traduciremos a $\mathbb{Q}$ ciertos cálculos definidos sobre $\mathbb{C}$ mediante el uso de la conjugación de Galois.

**Palabras clave:** *Género, Curva algebraica plana, Descomposición primaria, Explosiones de puntos.*

# Abstract

The main goal of this report is the study of algebraic plane curves and, more precisely, the development and implementation, using the mathematical system software *SAGE*, of a symbolic algorithm for computing the genus of a plane curve defined over $\mathbb{Q}$.

The study of the genus, which is the first birational invariant of a curve, turns out to be interesting to determinate its rationality or the birational equivalence between curves. In order to compute it, we will use a method based on local affine blow ups of singularities.

We will also delve into the study of basic Commutative Algebra tools, like primary decomposition of ideals, and, for the purpose of using operations over the rationals only, we will translate to $\mathbb{Q}$ some calculations defined over $\mathbb{C}$ by means of Galois conjugation.

**Keywords:** *Genus, Algebraic plane curve, Primary decomposition, Blow up.*

# Índice general

# Introducción

El objetivo principal de la presente memoria es el estudio de las curvas algebraicas planas y, más concretamente, la elaboración de un algoritmo simbólico para calcular el género de una curva plana definida sobre $\mathbb{Q}$.

El género constituye el primer invariante birracional de una curva, y es, en realidad, un invariante topológico de curvas no singulares, que a grandes rasgos mide el número de asas de una superficie de Riemann (para una revisión histórica y multidisciplinar de la noción de género, véase [Pop11]). Además, su estudio resulta imprescindible para determinar si una curva es racional o no: una curva es racional si y sólo si tiene género cero ([Ful71], Cap. 8, § 3). Para su cálculo emplearemos una adaptación al caso afín del método de transformaciones cuadráticas presentado en [SWPD08], Chapter 3, § 2.

Dado que, por un lado, queremos profundizar en el estudio y empleo de las herramientas básicas del Álgebra Conmutativa y, por otro, no disponemos en el software empleado de un algoritmo de factorización en cuerpos de números no primitivos y queremos evitar el paso a una extensión primitiva, no usaremos el método natural de las resultantes sino que sustituiremos la factorización de polinomios por la descomposición primaria de ideales.

Asimismo, el cálculo de la multiplicidad de intersección de dos curvas en un punto, que puede definirse de diversas maneras ([Che51],[Ful71] o [Vai96] aportan diferentes puntos de vista), se realizará mediante el cálculo de la dimensión de un espacio vectorial asociado a un anillo local. Es por ello que resulta necesario transcribir operaciones o propiedades de un anillo local en operaciones y propiedades de una $\mathbb{K}$-álgebra finitamente generada, generalmente a través del Corolario 1.36, que establece una relación entre anillos locales y descomposición primaria para ideales cero-dimensionales de un anillo de polinomios con coeficientes en un cuerpo algebraicamente cerrado.

Para curvas definidas sobre $\mathbb{Q}$, de forma natural, las intersecciones o los puntos que resultan de una explosión viven en la clausura algebraica de $\mathbb{Q}$. Puesto que estamos tratando de realizar operaciones racionales, debemos traducir a $\mathbb{Q}$ los cálculos definidos sobre $\mathbb{C}$, para lo cual haremos uso de la conjugación de Galois (en realidad, estamos considerando la clausura algebraica de $\mathbb{Q}$, y no $\mathbb{C}$).

En el Capítulo 1 se presenta el marco sobre el que trabajaremos a lo largo de la memoria. Comenzaremos definiendo los conjuntos algebraicos (y más concretamente, las variedades o conjuntos algebraicos irreducibles), y se expondrán algunos de sus resultados fundamentales. A continuación introduciremos los conceptos necesarios para definir el cuerpo de funciones racionales de una variedad y la noción de equivalencia birracional entre variedades, estableciendo la relación existente entre ambas: dos variedades son birracionalmente isomorfas si y sólo si sus cuerpos de funciones racionales son isomorfos. Acto seguido definiremos la idea de anillo local de una variedad en un punto, y terminaremos desarrollando en la medida en que nos sea imprescindible las

herramientas que se emplearán con posterioridad o que habrán ido surgiendo de forma natural, aunque en ocasiones implícitamente, a lo largo de las secciones iniciales, como anillos de fracciones, anillos de valoración discreta o descomposición primaria. Éste último instrumento resultará especialmente útil, pues servirá a un doble propósito en este trabajo: por un lado, proporcionará rudimentos teóricos para demostrar ciertas propiedades de interés sobre los anillos locales; por otro, nos permitirá en la práctica llevar a cabo cálculos de manera simbólica.

En el Capítulo 2 se analizan las propiedades y conceptos asociados a las curvas algebraicas planas, describiendo cada noción de diferentes maneras para gozar así de una visión más amplia de la situación y de una mayor cantidad de métodos de cálculo, y culminando con la definición de género. Trabajaremos siempre sobre un cuerpo $\mathbb{K}$ algebraicamente cerrado y de característica cero.

Definiremos la noción de curva algebraica plana afín, la multiplicidad de un punto y sus tangentes, y expondremos los resultados básicos. Estudiaremos los puntos de intersección de curvas planas y, en aras de establecer el Teorema de Bézout, extenderemos al caso proyectivo algunos de los objetos introducidos en el afín. La multiplicidad de intersección será presentada desde diferentes puntos de vista, tanto axiomáticamente como mediante "fórmulas" explícitas, con el fin de extraer diferentes propiedades de la forma más sencilla posible.

Por su parte, definiremos el género de una curva no singular mediante el Teorema de Riemann y, puesto que es un invariante birracional, lo generalizaremos para curvas arbitrarias a través de isomorfismos birracionales. Esto requiere discutir la existencia de modelos birracionales no singulares de curvas planas, es decir, curvas (no necesariamente planas) birracionalmente equivalentes a una dada pero en la que las singularidades han sido "resueltas". En la práctica, para el cálculo del género basta con encontrar curvas birracionalmente equivalentes a la curva de interés en que todas las singularidades sean ordinarias, cuestión sobre la que haremos hincapié en la sección correspondiente y que puede resolverse sin salir del plano proyectivo empleando transformaciones cuadráticas.

En el último punto de este capítulo desarrollaremos la teoría de divisores de curvas no singulares, lo que culminará con la demostración del Teorema de Riemann y la definición del género propiamente dicho.

En el Capítulo 3 trabajaremos con curvas definidas por polinomios con coeficientes racionales, y analizaremos de qué manera podemos extraer la información deseada de una curva plana proyectiva de manera simbólica (sobre $\mathbb{Q}$). Afrontaremos esta problemática de dos maneras: por un lado, mediante el estudio conjunto de puntos "conjugados", y por otro, cuando sea indispensable, recurriendo a extensiones algebraicas de $\mathbb{Q}$.

Organizaremos el capítulo en dos secciones: la primera de ellas tiene por meta desarrollar la teoría que justifica la implementación realizada. Como citamos anteriormente, jugará un rol muy importante la descomposición primaria, teniendo pues que estudiar su comportamiento frente a cambios en el cuerpo base y frente a la homogeneización (relación afín-proyectivo). Finalmente, en la segunda sección expondremos algunos ejemplos ilustrativos.

# Capítulo 1

# El contexto algebraico

Como se ha dicho en la introducción, en este primer Capítulo presentamos el contexto algebraico en el que nos encontraremos a lo largo de la memoria.

Durante este capítulo y los subsiguientes, salvo que se especifique lo contrario, denotaremos por $\mathbb{K}$ al cuerpo base sobre el que trabajaremos. De esta forma, $\mathbb{A}^n(\mathbb{K})$ y $\mathbb{P}^n(\mathbb{K})$, que representan, respectivamente, el espacio afín y el espacio proyectivo $n$-dimensional sobre $\mathbb{K}$, serán con frecuencia denotados simplemente por $\mathbb{A}^n$ (o $\mathbb{K}^n$) y $\mathbb{P}^n$. Prácticamente la totalidad de la teoría será definida en primer lugar para el caso afín, y se discutirá a su debido momento cómo traducirla, de manera compatible, al caso proyectivo.

## 1.1. Conjuntos algebraicos y variedades afines

En ocasiones, con objeto de simplificar notación, denotaremos por $\mathbb{K}[\underline{x}]$ al anillo de polinomios en $n$ variables $x_1, \ldots, x_n$ con coeficientes en el cuerpo $\mathbb{K}$, y por $\underline{a}$ a los puntos $(a_1, \ldots, a_n)$ de $\mathbb{K}^n$. Los resultados aquí presentados pueden verse en [Ful71], Cap. 1.

**Definición 1.1.** *Sea $S \subset \mathbb{K}[\underline{x}]$. Llamaremos* ***conjunto algebraico afín*** *definido por $S$ al conjunto*

$$V(S) = \{\underline{a} \in \mathbb{K}^n / f(\underline{x}) = 0, \forall f \in S\}.$$

Las propiedades básicas sobre conjuntos algebraicos afines pueden consultarse en [Ful71], Cap. 1, § 2 y más detalladamente en [CLO97], Chapters 1,4. Cabe destacar que el conjunto vacío $\emptyset$, el total $\mathbb{K}^n$, la intersección arbitraria y la unión finita de conjuntos algebraicos son conjuntos algebraicos, por lo que éstos constituyen el conjunto cerrados de una topología en $\mathbb{K}^n$, que se denomina Topología de Zariski.

Del mismo modo que asociamos a un ideal de $\mathbb{K}[\underline{x}]$ el conjunto de ceros comunes a los polinomios que lo componen, podemos asociar a un conjunto de puntos en $\mathbb{K}^n$ el ideal de polinomios que se anulan en esos puntos.

**Definición 1.2.** *Sea $E \subset \mathbb{K}^n$. Llamamos* ***ideal asociado a E*** *al conjunto*

$$I(E) = \{f \in \mathbb{K}[\underline{x}] / f(\underline{a}) = 0, \forall \underline{a} \in E\}.$$

Ideales asociados y conjuntos algebraicos interactúan de la siguiente manera ([Ful71], Cap. 1, § 3):

**Proposición 1.3.**

- *Para todo ideal $J$ de $\mathbb{K}[\underline{x}]$, $J \subset \sqrt{J} \subset IV(J)$*
- *Si $E \subset \mathbb{K}^n$ entonces $E \subset VI(E)$.*
- *VIV(J) = V(J), IVI(E) = I(E).*
- *$VI(E) = \bar{E}$, donde $\bar{E}$ denota la clausura de $E$ en la topología de Zariski. Así, $E$ es un conjunto algebraico afín si y sólo si $VI(E) = E$.*

Uno de los resultados fundamentales a este respecto es el Nullstellensatz o Teorema de los Ceros de Hilbert, que es recogido en sus diferentes versiones (tal y como puede consultarse en [Ash02], Chapter 8) en el siguiente teorema (Ver [CLO97], Chapter 4, para mayor detalle):

**Teorema 1.4.** *Para todo cuerpo $\mathbb{K}$ y todo entero positivo $n$ son equivalentes:*

- *$\mathbb{K}$ es algebraicamente cerrado.*
- ***Teorema de ideales maximales.*** *Si $I$ es ideal de $\mathbb{K}[\underline{x}]$, entonces:*

$$I \text{ es ideal maximal} \Leftrightarrow \exists a_1, \ldots, a_n \in \mathbb{K} \text{ con } I = (x_1 - a_1, \ldots, x_n - a_n)$$

- ***Nullstellensatz débil.*** *Si $I$ es ideal de $\mathbb{K}[\underline{x}]$, entonces:*

$$V(I) = \emptyset \Leftrightarrow I = (1) = \mathbb{K}[\underline{x}].$$

- ***Nullstellensatz fuerte.*** *Para todo $I$ ideal de $\mathbb{K}[\underline{x}]$:*

$$IV(I) = \sqrt{I}.$$

Del Teorema de los Ceros de Hilbert en su versión fuerte se deduce que hay una correspondencia uno a uno entre ideales radicales de $\mathbb{K}[\underline{x}]$ y conjuntos algebraicos afines cuando el cuerpo $\mathbb{K}$ es algebraicamente cerrado. En dicha biyección, a puntos $\underline{a}$ corresponden ideales maximales $(x_1 - a_1, \ldots, x_n - a_n)$, y los ideales primos, que son radicales, estarán asociados a variedades:

**Definición 1.5.** *Sea $V$ un conjunto algebraico afín. Decimos que $V$ es* ***irreducible*** *si no se puede expresar como unión de conjuntos algebraicos afines estrictamente contenidos en $V$, esto es, si $V = V_1 \cup V_2$, con $V_1$ y $V_2$ algebraicos, entonces necesariamente $V = V_1$ o $V = V_2$. Los conjuntos algebraicos irreducibles son llamados* ***variedades afines****.*

**Proposición 1.6.** *Sea $V$ un conjunto algebraico afín no vacío. Entonces*

$$V \text{ es irreducible} \Leftrightarrow I(V) \text{ es un ideal primo.}$$

Además, teniendo en cuenta que en $\mathbb{K}[\underline{x}]$ toda cadena ascendente de ideales es estacionaria (Teorema de la Base de Hilbert), se deduce que todo conjunto algebraico afín puede expresarse como unión finita de conjuntos algebraicos irreducibles.

Para concluir esta sección, y dado que estamos interesados en trabajar en el plano, conviene estudiar los conjuntos algebraicos afines de $\mathbb{A}^2$. Para ello, y teniendo en cuenta lo anterior, basta con describir sus subconjuntos irreducibles.

**Proposición 1.7.** *Si $\mathbb{K}$ es un cuerpo infinito, las variedades en $\mathbb{A}^2$ son las siguientes: $\mathbb{A}^2$, $\emptyset$, los puntos y los $V(F)$ donde $F$ es un polinomio irreducible en dos variables y $V(F)$ es infinito.*

## 1.2. Funciones polinómicas y racionales

El fin último de esta sección será definir el cuerpo de funciones racionales sobre una variedad y, especialmente, ver que dos variedades tienen mismo cuerpo de funciones si y sólo si son equivalentes (de algún modo que definiremos a continuación). La noción de género de una curva, que será tratada en el segundo capítulo, depende únicamente del cuerpo de funciones, por lo que en virtud de este resultado estaremos interesados en encontrar "modelos más sencillos" que nuestra curva y equivalentes a ella para determinar el género con menores dificultades.

Comenzaremos, pues, definiendo el anillo de coordenadas de una variedad:

**Definición 1.8.** *Sea $V \subset \mathbb{A}^n$ una variedad. Entonces $I(V)$ es un ideal primo y podemos considerar el dominio de integridad*

$$\Gamma(V) = \mathbb{K}[x_1, \ldots, x_n]/I(V).$$

*$\Gamma(V)$ recibe el nombre de **anillo de coordenadas de V**, y es un anillo noetheriano dado que $\mathbb{K}[\underline{x}]$ lo es.*

Denotemos $\mathfrak{J}(V, \mathbb{K})$ al conjunto de funciones de $V$ en $\mathbb{K}$, que es un anillo con la suma y el producto usual de funciones. Podemos identificar $\mathbb{K}$ con el conjunto de funciones constantes de $V$ en $\mathbb{K}$.

**Definición 1.9.** *Sea $V \subset \mathbb{A}^n$ una variedad. Una función $\varphi \in \mathfrak{J}(V, \mathbb{K})$ es una **función polinómica** sobre $V$ si constituye la restricción a $V$ de un polinomio en $n$ variables, esto es, si existe $f \in \mathbb{K}[x_1, \ldots, x_n]$ de manera que, para todo $\underline{a} \in V$,*

$$\varphi(\underline{a}) = f(\underline{a}).$$

*En tal caso decimos que $f$ representa a $\varphi$.*

Observemos que las funciones polinómicas forman un anillo y que podemos identificarlas con los elementos de $\Gamma(V)$, pues dos polinomios $f$ y $g$ representan la misma función si y sólo si $f(\underline{a}) = g(\underline{a})$ para todo $\underline{a} \in V$, esto es, si $f - g \in I(V)$.

Las aplicaciones regulares o polinómicas generalizan este concepto:

**Definición 1.10.** *Sean $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ variedades. Una función $\varphi : V \to W$ se denomina **aplicación regular** o **aplicación polinómica** si existen polinomios $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ tales que, para todo punto $\underline{a} \in V$,*

$$\varphi(\underline{a}) = (f_1(\underline{a}), \ldots, f_m(\underline{a})).$$

**Definición 1.11.** *Una aplicación regular $\varphi : V \to W$ es un isomorfismo regular si existe una aplicación regular $\varphi : W \to V$ tal que $\varphi \circ \psi = id_W$ y $\psi \circ \varphi = id_V$. En este caso se dice que $V$ y $W$ son regularmente isomorfas.*

Los isomorfismos regulares que más vamos a utilizar son los cambios de coordenadas.

Aunque no vamos a detenernos en ello, cabe mencionar que existe una correspondencia 1-1 entre aplicaciones polinómicas de $V$ en $W$ y homomorfismos de $\Gamma(W)$ en $\Gamma(V)$, de modo que a isomorfismos regulares corresponden isomorfismos de $\mathbb{K}$-álgebras. Nosotros estaremos interesados en el resultado análogo para cuerpos de funciones y aplicaciones birracionales.

Estamos ya en disposición de definir el concepto de cuerpo de funciones de una variedad. Como, para toda variedad $V$ de $\mathbb{A}^n$, $\Gamma(V)$ es dominio de integridad, podemos considerar su cuerpo de fracciones:

**Definición 1.12.** *El* ***cuerpo de funciones racionales*** $\mathbb{K}(V)$ *sobre una variedad* $V \subset \mathbb{A}^n$ *es el cuerpo de fracciones de* $\Gamma(V)$*, esto es,*

$$\mathbb{K}(V) = Frac\Big(\mathbb{K}[x_1, \ldots, x_n]/I(V)\Big) = \Big\{\frac{f + I(V)}{g + I(V)} / f, g \in \mathbb{K}[\underline{x}], g \notin I(V)\Big\}/\sim,$$

*donde la relación de equivalencia* $\sim$ *viene dada por*

$$\frac{f + I(V)}{g + I(V)} \sim \frac{f' + I(V)}{g' + I(V)} \Leftrightarrow fg' - f'g \in I(V).$$

*Para simplificar, en muchas ocasiones utilizaremos* $\bar{f}$ *para denotar* $f + I(V)$*.*

**Definición 1.13.** *Una función racional* $\varphi \in \mathbb{K}(V)$ ***está definida*** *en* $P \in V$ *si admite una representación de la forma* $\varphi = \bar{f}/\bar{g}$ *con* $g(P) \neq 0$*. En tal caso decimos que* $f(P)/g(P)$ *es el* ***valor*** *de la función en el punto* $P$*,* $\varphi(P)$*. Un punto* $P \in V$ *en que la función no esté definida se denomina* ***polo****.*

Observemos en primer lugar que el valor de una función racional está bien definido, pues si tenemos dos representaciones $\bar{f}/\bar{g}$ y $\bar{f}'/\bar{g}'$ de la misma función racional $\varphi$, con $g(P)$ y $g'(P)$ no nulos, entonces $fg' - f'g \in I(V)$ y por tanto $f(P)g'(P) - f'(P)g(P) = 0$.

Atendiendo al siguiente resultado (que puede verse en [Ful71], Cap. 2, Sec. 4), se tiene que las funciones racionales están definidas en todo un abierto (no vacío, pues si $\bar{f}/\bar{g}$ es una representación de $\varphi$, entonces $g \notin I(V)$ y existe al menos un punto de $V$ donde $\varphi$ está definida) en la topología de Zariski.

**Teorema 1.14.** *El conjunto de polos de una función racional* $\varphi \in \mathbb{K}(V)$ *es un conjunto algebraico.*

Las aplicaciones racionales extienden el concepto de función racional:

**Definición 1.15.** *Sean* $V \subset \mathbb{A}^n$*,* $W \subset \mathbb{A}^m$ *variedades. Una* ***aplicación racional*** $\varphi$ *de* $V$ *en* $W$ *es una* $m$*-upla* $\varphi = (\varphi_1, \ldots, \varphi_m)$ *de funciones racionales en* $\mathbb{K}(V)$ *de manera que, para todo punto* $P \in V$ *en que estén definidas todas las* $\varphi_i$*, se tiene que* $(\varphi_1(P), \ldots, \varphi_m(P)) \in W$*. Se dice que* $\varphi$ *está definida en* $P$ *si lo están todas las* $\varphi_i$

Como la unión finita de conjuntos algebraicos es algebraica, tenemos de nuevo que una aplicación racional está definida en todo un abierto no vacío de $V$ (el complementario de la unión de los conjuntos de polos de cada componente).

**Definición 1.16.** *Decimos que una aplicación racional* $\varphi : V \to W$ *es un* ***isomorfismo birracional*** *si existe una aplicación racional* $\psi : W \to V$ *de manera que, allá donde estén definidas las composiciones,* $\psi \circ \varphi = id_V$ *y* $\varphi \circ \psi = id_W$*, y* $\varphi(V), \psi(W)$ *son densos en* $W, V$*, respectivamente (esto es, su clausura Zariski es el total). En estas condiciones decimos que* $V$ *y* $W$ *son* ***birracionalmente equivalentes*** *o* ***birracionalmente isomorfos****.*

El siguiente teorema es al que nos hemos referido al inicio de la sección, y puede verse en [SWPD08],Chapter 2, Th 2.38:

**Teorema 1.17.** *Dos variedades* $V \subset \mathbb{A}^n$ *y* $W \subset \mathbb{A}^m$ *son birracionalmente equivalentes si y sólo si sus cuerpos de funciones* $\mathbb{K}(V)$ *y* $\mathbb{K}(W)$ *son isomorfos.*

## 1.3. Anillos locales. Anillos de valoración discreta

Uno de las conceptos esenciales para estudiar el comportamiento de una curva en un punto es el de "anillo local". En esta sección estudiaremos la noción de anillo local de una variedad en un punto, demostraremos que tal nomenclatura no ha sido escogida de manera arbitraria y analizaremos algunas de sus propiedades. Los anillos locales nos permitirán dar más adelante una definición de multiplicidad de un punto en una curva independiente de coordenadas, así como de multiplicidad de intersección de dos curvas en un punto.

Los anillos de valoración discreta son anillos locales que verifican ciertas condiciones adicionales. Veremos en el segundo capítulo que los puntos simples (de multiplicidad 1) de una curva tienen asociados anillos locales que son de valoración discreta, y es precisamente por ello que nos interesa estudiarlos detalladamente.

**Definición 1.18.** *Para todo $P \in V$, se define el* ***anillo local de V en P*** *como*

$$\mathcal{O}_P(V) = \{\varphi \in \mathbb{K}(V)/\varphi \text{ está definida en } P\}.$$

Obsérvese que $\mathcal{O}_P(V)$ es un subanillo de $\mathbb{K}(V)$ que contiene al anillo de coordenadas $\Gamma(V)$. Más aún, tal y como se muestra en [Ful71], Cap. 2, Sec. 4,

**Teorema 1.19.** *Una función racional $\varphi \in \mathbb{K}(V)$ definida en todo punto de $V$ es una función polinómica, y por tanto*

$$\Gamma(V) = \bigcap_{P \in V} \mathcal{O}_P(V).$$

Puesto que $\Gamma(V)$ es un dominio noetheriano, se deduce que $\mathcal{O}_P(V)$ también lo es:

**Teorema 1.20.** *$\mathcal{O}_P(V)$ es un dominio noetheriano.*

*Demostración.* Por un lado, $\mathcal{O}_P(V)$ es un dominio por ser subanillo de $\mathbb{K}(V)$.

Por otro lado, si $I$ es un ideal de $\mathcal{O}_P(V)$, entonces $I \cap \Gamma(V)$ es un ideal de $\Gamma(V)$, y por tanto está generado por un número finito de elementos $\bar{f}_1, \ldots, \bar{f}_r$. Además, si $\varphi \in I$, entonces podemos escribir $\varphi = \bar{f}/\bar{g}$ con $g(P) \neq 0$, de modo que $\bar{g}\varphi \in \Gamma(V)$. De acuerdo con lo anterior, existen $\bar{a}_1, \ldots, \bar{a}_r \in \Gamma(V)$ tales que $\bar{g}\varphi = \sum \bar{a}_i \bar{f}_i$, esto es, $\varphi = \sum \frac{\bar{a}_i}{\bar{g}} f_i$. En definiva, $I = (f_1, \ldots, f_r)$. □

Convendrá también tener en cuenta que los cambios de coordenadas inducen isomorfismos entre estos anillos $\mathcal{O}_P$, pues esto nos dará libertad, por ejemplo, para suponer que trabajamos en el origen, lo que simplifica agradablemente la escritura.

**Proposición 1.21.** *Sea $V \subset \mathbb{A}^n$ una variedad, $P \in V$. Si $T : \mathbb{A}^n \to \mathbb{A}^n$ es un cambio de coordenadas con $T(Q) = P$, entonces los anillos $\mathcal{O}_P(V)$ y $\mathcal{O}_Q(T^{-1}(V))$ son isomorfos.*

*Demostración.* $T^{-1}(V)$ es una variedad al ser $T$ biyectiva, con lo que tiene sentido tal consideración. El isomorfismo $\varphi : \mathcal{O}_P(V) \to \mathcal{O}_Q(T^{-1}(V))$ viene dado por $\frac{\bar{f}}{\bar{g}} \mapsto \frac{\overline{f \circ T}}{\overline{g \circ T}}$, donde si $T = (T_1, \ldots, T_n)$, $f \circ T$ denota a $f(T_1, \ldots, T_n)$. □

Como mencionábamos, no denominamos a $\mathcal{O}_P(V)$ anillo local de manera azarosa. En general, un **anillo local** es un anillo $R$ que verifica cualquiera de las condiciones equivalentes siguientes:

- $R - R^*$ es un ideal, donde $R^*$ es el conjunto de unidades de $R$.
- $R$ posee un único ideal maximal que contiene a todo ideal propio de $R$.

La equivalencia entre ambas es clara: si $R - R^*$ es un ideal, entonces es maximal, pues un ideal que lo contenga contiene a una unidad y por tanto es el total. Además contiene a todo ideal propio de $R$. Recíprocamente, si $\mathfrak{m}$ es el único maximal de $R$ y contiene a todo ideal propio de $R$, entonces todo $y \in R - R^*$ está en $\mathfrak{m}$ (pues $(y) \subset \mathfrak{m}$); como $\mathfrak{m} \subset R - R^*$ siempre, se tiene la igualdad.

En nuestro caso particular, las unidades de $\mathcal{O}_P(V)$ son las funciones racionales que no se anulan en $P$: Si $\varphi = \bar{f}/\bar{g}$ está definida pero no se anula en $P$, entonces $f(P) \neq 0$ (luego $f \notin I(V)$) y tiene sentido considerar $\varphi^{-1} = \bar{g}/\bar{f}$. Las no unidades, estas son, las funciones racionales que se anulan en $P$, forman claramente un ideal de $\mathcal{O}_P(V)$, y por ello $\mathcal{O}_P(V)$ es, en sentido estricto, un anillo local.

**Lema 1.22.** *Si $P = (a_1, \ldots, a_n)$, entonces el maximal $\mathfrak{m}$ de $\mathcal{O}_P$ está generado por las clases de los $x_i - a_i$, para $i = 1, \ldots, n$,*

$$\mathfrak{m} = (\overline{x_1 - a_n}, \ldots, \overline{x_n - a_n})\mathcal{O}_P(V).$$

*Demostración.* En efecto, el contenido $\supset$ es claro, al anularse cada $x_i - a_i$ en $P$. El recíproco también, pues si $\frac{\bar{f}}{\bar{g}} \in \mathfrak{m}$, entonces $f(P) = 0$. Así, dividiendo $f$ por los $x_i - a_i$ obtenemos que $f = (x_1 - a_1)f_1 + \cdots + (x_n - a_n)f_n + r$ donde $f_i \in \mathbb{K}[x_1, \ldots, x_n]$ y $r$ debe ser constante. Como $f(P) = 0$, necesariamente $r = 0$, y tomando clases

$$\frac{\bar{f}}{\bar{g}} = (\overline{x_1 - a_1})\frac{\bar{f}_1}{\bar{g}} + \cdots + (\overline{x_n - a_n})\frac{\bar{f}_n}{\bar{g}} \in (\overline{x_1 - a_n}, \ldots, \overline{x_n - a_n})\mathcal{O}_P(V).$$

□

Puede resultarnos útil notar que este caso coincide con la construcción algebraica más general de localización de $\Gamma(V)$ por el ideal primo $I(P)$ (ver [AM69], Cap. 3, Ejemplo 1): En efecto, los elementos de $\Gamma(V)_P := \Gamma(V)_{I(P)}$ son, por definición, los $\bar{f}/\bar{g}$ donde $f, g \in \mathbb{K}[x_1, \ldots, x_n], g \notin I(V)$ y $g(P) \neq 0$. Además, dado que trabajamos en un dominio, la relación de equivalencia asociada a la localización es precisamente la definida sobre $\mathbb{K}(V)$. Así pues, $\Gamma(V)_P = \mathcal{O}_P(V)$.

Esto nos permite hacer uso de las propiedades y resultados de construcción de anillos de fracciones ([AM69], Cap. 3). Por ejemplo, sobre $R$-módulos en general, el operador $S^{-1}$ conmuta con sumas, intersecciones, módulos cociente, y si $N_1, N_2$ son submódulos de $M$ con $N_2$ finitamente generado, entonces $S^{-1}(N1 : N2) = (S^{-1}N1 : S^{-1}N2)$.

Tenemos además que, para ideales $I$ y $J$ de $R$:

**Propiedades 1.23.**

1. *Los ideales de $S^{-1}R$ son de la forma $S^{-1}I$ donde $I$ es ideal de $R$.*
2. *Sea $I$ ideal de $R$. Entonces $S^{-1}I = (1)$ si y sólo si $I \cap S \neq \emptyset$.*
3. *Existe una correspondencia 1-1 entre ideales primos de $S^{-1}R$ e ideales primos de $R$ con $R \cap S = \emptyset$.*
4. *$S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$ y $S^{-1}(\sqrt{I}) = \sqrt{S^{-1}(J)}$.*

*Obsérvese que de 2. se deduce que al localizar $R$ en un ideal primo $\mathfrak{p}$ eliminamos (pasan a ser el total) todos los ideales de $R$ salvo los que están contenidos en $\mathfrak{p}$.*

Atendiendo a estos resultados, podemos probar sin excesivos problemas la siguiente proposición:

**Proposición 1.24.** *Sea $V \subset \mathbb{A}^n$ una variedad, $P \in V$, $J$ ideal de $\mathbb{K}[x_1, \ldots, x_n]$ que contiene a $I(V)$. Entonces, si $\bar{J}$ es la imagen de $J$ en $\Gamma(V)$, se tiene que el cociente $\mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n)$ es isomorfo a $\mathcal{O}_P(V)/\bar{J}\mathcal{O}_P(V)$. En particular, se deduce que $\mathcal{O}_P(\mathbb{A}^n)/(I(V)\mathcal{O}_P(\mathbb{A}^n))$ es isomorfo a $\mathcal{O}_P(V)$.*

*Demostración.* Observemos que $\Gamma(\mathbb{A}^n) = \mathbb{K}[x_1, \ldots, x_n]$. Como $J$ es un ideal de $\mathbb{K}[x_1, \ldots, x_n]$ que contiene a $I(V)$, el Tercer Teorema de Isomorfía nos dice que

$$\Gamma(\mathbb{A}^n)/J \cong (\Gamma(\mathbb{A}^n)/I(V))/(J/I(V)) = \Gamma(V)/\bar{J}.$$

Ahora, teniendo en cuenta que el anillo local de una variedad en un punto es la localización de su anillo de coordenadas en el ideal asociado al punto, y que tal localización conmuta con cocientes, tenemos que

$$\mathcal{O}_P(\mathbb{A}^n)/J\mathcal{O}_P(\mathbb{A}^n) \cong (\Gamma(\mathbb{A}^n)/J)_P \cong (\Gamma(V)/\bar{J})_P \cong \mathcal{O}_P(V)/\bar{J}\mathcal{O}_P(V),$$

como queríamos demostrar. □

Los anillos $\mathcal{O}_P(V)$ cuyo ideal maximal es principal constituyen lo que se denomina un anillo de valoración discreta y poseen además ciertas particularidades interesantes. De manera general,

**Proposición 1.25.** *Sea $R$ un dominio que no sea un cuerpo. Son equivalentes:*

1. *$R$ es local noetheriano y con ideal maximal $\mathfrak{m}$ principal.*
2. *Existe un elemento irreducible $t \in R$ de manera que, si $a \in R$ es no nulo, entonces se puede expresar de forma única como $a = ut^n$, donde $u \in R^*$, $n$ entero no negativo.*

*Un anillo que verifique estas condiciones se denomina* ***anillo de valoración discreta****, y todo elemento como en 2. recibe el nombre de* ***parámetro de uniformización****.*

*Demostración.* [Ful71], Cap.2, Proposición 2.4. □

En particular, se demuestra que un anillo de valoración discreta es un dominio de ideales principales, siendo sus ideales de la forma $(t^n)$ para $t$ parámetro de uniformización y $n$ entero no negativo (cf. Teorema 1.29).

Observemos también que el parámetro de uniformización es único salvo producto por unidades. Efectivamente, si $t$ y $s$ son parámetros de uniformización, podemos escribir $t = us^n$ y $s = vt^m$ para ciertos $u, v \in R^*$. De esta forma $t = uv^n t^{mn}$ y por tanto $mn = 1$. Pero $m$ y $n$ son enteros no negativos, luego $m = n = 1$ y $t = us$.

En virtud de lo anterior, si $\mathbb{L}$ es el cuerpo de fracciones de $R$, todo $z \in \mathbb{L}$ no nulo admite una expresión única de la forma $z = ut^n$, donde $u \in R^*$ y $n \in \mathbb{Z}$. Esto es claro, pues existirán $a, b \in R$ tales que $z = a/b$. Como $R$ es anillo de valoración discreta, $a = vt^n$,$b = wt^m$ y, en conclusión, $z = vw^{-1}t^{n-m}$, con $uw^{-1} \in R^*$ y $n-m \in \mathbb{Z}$. Además,

acabamos de probar que este exponente, llamado **orden de z**, es independiente del parámetro $t$. Por tanto, tenemos una aplicación bien definida

$$\begin{array}{rccc} ord: & \mathbb{L} & \longrightarrow & \mathbb{Z}\cup\{\infty\} \\ & z\neq 0 & \longmapsto & n \\ & 0 & \longmapsto & \infty \end{array}$$

que se denomina función orden, y que verifica:

**Proposición 1.26.**

1. $ord(z)=\infty \Leftrightarrow z=0$.
2. $ord(zz')=ord(z)+ord(z')$, *para todo* $z,z'\in\mathbb{L}$.
3. *Si* $z,z'\in\mathbb{L}$, *entonces* $ord(z+z')\geq \min\{ord(a),ord(b)\}$. *Más aún, si* $ord(z)<ord(z')$, *entonces* $ord(z+z')=ord(z)$.
4. *Sean* $z_1,\ldots,z_n\in\mathbb{L}$. *Si existe* $i$ *tal que* $ord(z_i)<ord(z_j)$ *para todo* $j\neq i$, *entonces* $z_1+\cdots+z_n\neq 0$.

*Demostración.* El apartado *1.* se tiene por propia definición y el apartado *2.* es claro. Para ver *3.*, supongamos que $z=ut^n$, $z'=vt^m$ con $n\leq m$. Entonces $z+z'=ut^n+vt^m=(u+vt^{m-n})t^n\in(t^n)$ y por tanto $ord(z+z')=k\geq n$. Además, si $n<m$, entonces $k=n$, porque de lo contrario

$$wt^k=z+z'=ut^n+vt^m\Rightarrow u=wt^{k-n}-v^tm-n\in(t),$$

lo que es absurdo. El apartado *4.* es consecuencia de *3.*: Supongamos que $i=1$. La primera parte de *3.* nos dice que $ord(a_2+\cdots+a_n)\geq ord(a_2)>ord(a_1)$, y la segunda parte nos dice que $ord(a_1+(a_2+\cdots+a_n))=ord(a_1)\neq\infty$. En definitiva, se concluye que $a_1+\cdots+a_n\neq 0$. □

$R$ se identifica, pues, con los elementos de $\mathbb{L}$ de orden no negativo. De este modo, es claro que, para todo $z\in\mathbb{L}$, o bien $z\in R$ o bien $z^{-1}\in R$.

La siguiente proposición enuncia que disponemos de un análogo a los desarrollos tipo Taylor para los elementos de $R$:

**Proposición 1.27.** *Sea* $R$ *un anillo de valoración discreta con maximal* $\mathfrak{m}=(t)$ *y supongamos que un cierto cuerpo* $\mathbb{K}$ *es subanillo de* $R$ *isomorfo a* $R/\mathfrak{m}$. *Entonces, para todo* $z\in R$ *y todo* $n\geq 0$, *existen unos únicos* $\lambda_0,\ldots,\lambda_n\in\mathbb{K}$ *y* $z_{n+1}\in R$ *tales que*

$$z=\lambda_0+\lambda_1t+\cdots+\lambda_nt^n+z_{n+1}t^{n+1}.$$

*Demostración.* Sea $z\in R$. La demostración se realizará por inducción sobre $n$. Si $n=0$, entonces debemos probar que existen unos únicos $\lambda_0\in\mathbb{K}$,$z_1\in\mathfrak{m}$ tales que $z=\lambda_0+z_1t$. En efecto, como $R/\mathfrak{m}\cong\mathbb{K}$, entonces existe un único $\lambda_0$ con $z+\mathfrak{m}\leftrightarrow\lambda_0$. De esta manera, $z-\lambda_0\in\mathfrak{m}$, y existe $z_1\in R$ tal que $z-\lambda_0=z_1t$, como queríamos ver.

Supongamos este hecho cierto hasta $n-1$, y veámoslo para $n$. Por hipótesis tenemos que existen unos únicos $\lambda_0,\ldots,\lambda_{n-1}\in\mathbb{K}$, $z_n\in R$ tales que

$$z=\lambda_0+\lambda_1t+\cdots+\lambda_{n-1}t^{n-1}+z_nt^n.$$

Por lo visto en el paso inicial, existen unos únicos $\lambda_n \in \mathbb{K}$,$z_{n+1} \in K$ tales que $z_n = \lambda_n + z_{n+1}t$, y por tanto

$$z = \lambda_0 + \lambda_1 t + \cdots + \lambda_{n-1}t^{n-1} + \lambda_n t^n + z_{n+1}t^{n+1}.$$

Durante el propio procedimiento hemos visto que $\lambda_0, \ldots, \lambda_n$ y $z_{n+1}$ son los únicos en las condiciones anteriores: si existiera otra descomposición de la forma $z = \mu_0 + \mu_1 t + \cdots + \mu_{n-1}t^{n-1} + \mu_n t^n + z'_{n+1}t^{n+1}$, entonces obtendríamos que $z = \mu_0 + \mu_1 t + \cdots + \mu_{n-1}t^{n-1} + (\mu_n + z'_{n+1}t)t^n$, y por definición de los $\lambda_i$ y $z_n$ se tiene que $\lambda_i = \mu_i$ para $i = 1, \ldots, n-1$ y $\mu_n + z'_{n+1}t = z_n$. Como esta última descomposición de $z_n$ también es única, necesariamente $\mu_n = \lambda_n$ y $z_{n+1} = z'_{n+1}$. □

Si trabajamos en una variedad $V \subset \mathbb{A}^n$, el cuerpo de fracciones de los anillos $\mathcal{O}_P(V)$ es el cuerpo de funciones racionales $\mathbb{K}(V)$. Cuando $\mathcal{O}_P(V)$ sea de valoración discreta, denotaremos a su función orden asociada por $ord_P$, y hemos visto que $\mathcal{O}_P(V)$ se identifica con las funciones racionales con orden no negativo en $P$. De esta manera, si $\varphi \in \mathbb{K}(V)$ es una función racional no definida en $P$, es decir, si $P$ es un polo de $\varphi$, decimos que el entero positivo $-ord_P(\varphi)$ es el **orden del polo** $P$ **de** $\varphi$. Análogamente, si $P$ es un cero de $\varphi$, entonces decimos que el entero positivo $ord_P(\varphi)$ es el **orden del cero** $P$ **de** $\varphi$.

Observemos que, por la propiedad *2.* de $ord_P$, $ord_P(\frac{\bar{f}}{\bar{g}}) = ord_P(\bar{f}) - ord_P(\bar{g})$, es decir, que basta estudiar por separado numerador y denominador de una función racional (ambos en $\mathcal{O}_P$ y por tanto de orden no negativo). Como debe ser, el orden de una función racional es independiente del representante escogido para determinarlo, dado que si $\varphi = \bar{f}/\bar{g} = \bar{f}'/\bar{g}'$, entonces $\bar{f}\bar{g}' - \bar{f}'\bar{g} = 0$, luego $ord_P(\bar{f}\bar{g}' - \bar{f}'\bar{g}) = \infty$. De acuerdo con la propiedad *4.* de la función de orden, esto implica que $ord_P(\bar{f}\bar{g}') = ord_P(\bar{f}'\bar{g})$, y de nuevo por la propiedad *2.*, $ord_P(\bar{f}) - ord_P(\bar{g}) = ord_P(\bar{f}') - ord_P(\bar{g}')$. Si $f \in \mathbb{K}[x_1, \ldots, x_n]$, definiremos $ord_P(f) := ord_P(\bar{f})$, siendo $\bar{f}$ la clase de $f$ en $\Gamma(V)$. Cerraremos la sección con un teorema que nos proporciona formas equivalentes de definir y/o calcular $ord_P$. Para ello, necesitaremos el siguiente resultado general, que enunciaremos en forma de lema para futuras referencias:

**Lema 1.28.** *Sean $I, J$ ideales comaximales de un anillo $R$, esto es, $I + J = R$. Entonces, para todo $n, m$ enteros positivos, $I^n$ y $J^m$ son ideales comaximales.*

*Demostración.* Bastará probar que, para todo $n \geq 1$, $I^n + J = R$. En efecto, como $I, J$ son comaximales, existen $a \in I, b \in J$ tales que $1 = a + b$. Así,

$$1 = (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k = a^n + \left(\sum_{k=1}^{n} \binom{n}{k} a^{n-k}b^{k-1}\right) b \in I^n + J$$

y por tanto $I^n + J = R$. □

**Teorema 1.29.** *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado, $V$ una variedad de $\mathbb{A}^n(\mathbb{K})$ y $P = (a_1, \ldots, a_n) \in V$ tal que $\mathcal{O}_P(V)$ es un anillo de valoración discreta con maximal $\mathfrak{m} = (t)$. Dados $g \in \mathbb{K}[x_1, \ldots, x_n]$, $m \geq 0$ entero, son equivalentes:*

1. *$\bar{g} = ut^m$, $u$ unidad de $\mathcal{O}_P$.*
2. *$\bar{g} \in (t^m)$, $\bar{g} \notin (t^{m+1})$.*
3. *$(\bar{g}) = (t^m)$.*

*4.* $m = dim_{\mathbb{K}}\Big(\mathcal{O}_P(V)/(\bar{g})\mathcal{O}_P(V)\Big)$.

*5.* $m = dim_{\mathbb{K}}\Big(\mathbb{K}[x_1,\ldots,x_n]/(I(V)+(g))\Big)_{I(P)}$.

*6.* $g \in (x_1-a_1,\ldots,x_n-a_n)^m + I(V)$, $g \notin (x_1-a_1,\ldots,x_n-a_n)^{m+1} + I(V)$.

*Demostración.* La equivalencia entre los tres primeros apartados es clara y ha sido demostrada a lo largo de la sección. Comencemos viendo que son equivalentes a *4.*: Por un lado, si $(\bar{g}) = (t^m)$, entonces la Proposición 1.27 nos dice que $\{1, t, \ldots, t^{m-1}\}$ forma una base de $\mathcal{O}_P(V)/(\bar{g})$ como $\mathbb{K}$-espacio vectorial, y por tanto

$$m = dim_{\mathbb{K}} \frac{\mathcal{O}_P(V)}{(\bar{g})}.$$

El recíproco también es cierto, pues todo ideal de $\mathcal{O}_P(V)$ es de la forma $(t^k)$ para algún $k$, y por tanto la única manera de que $m$ sea la dimensión de $\mathcal{O}_P/(\bar{g})$ es que $g = (t^m)$.

La equivalencia entre *4.* y *5.* se prueba teniendo en cuenta la Proposición 1.24, que la operación $S^{-1}$ conmuta con cocientes, y que la imagen de $I(V)+(g)$ en $\Gamma(V)$ es $(\bar{g})$. Así,

$$\left(\frac{\mathbb{K}[x_1,\ldots,x_n]}{I(V)+g}\right)_{I(P)} \cong \frac{\mathcal{O}_P(\mathbb{A}^n)}{(I(V)+g)\mathcal{O}_P(\mathbb{A}^n)} \cong \frac{\mathcal{O}_P(V)}{(\bar{g})\mathcal{O}_P(V)}$$

y sus dimensiones son iguales.

Veamos finalmente la equivalencia *2.* $\Leftrightarrow$ *6.*. Sea $\pi : \mathbb{K}[x_1,\ldots,x_n] \to \Gamma(V)$ la proyección natural en el cociente, e $i : \Gamma(V) \to \mathcal{O}_P(V)$ el monomorfismo dado por $\bar{f} \mapsto \bar{f}/\bar{1}$. Como sabemos por el Lema 1.22, $\mathfrak{m} = (\overline{x_1-a_1},\ldots,\overline{x_n-a_n})\mathcal{O}_P(V)$. Observemos que $i^{-1}(\mathfrak{m}) = (\overline{x_1-a_1},\ldots,\overline{x_n-a_n})$ [si $\bar{f} \in i^{-1}(\mathfrak{m})$, entonces $f(P) = 0$ y por tanto $f \in I(P) = (x_1-a_1,\ldots,x_n-a_n)$. Por ello $\bar{f} \in (\overline{x_1-a_1},\ldots,\overline{x_n-a_n})$. El otro contenido es claro]. Más aún, vamos a probar que $i^{-1}(\mathfrak{m}^k) = (\overline{x_1-a_1},\ldots,\overline{x_n-a_n})^k$:

"$\supseteq$" Se da siempre (en general para contracciones de ideales).

"$\subseteq$" Como $\mathfrak{m}^k = (\overline{x_1-a_1},\ldots,\overline{x_n-a_n})^k\mathcal{O}_P(V)$, si $\bar{f} \in i^{-1}(\mathfrak{m}^k)$ entonces se puede expresar como combinación de los generadores de $\mathfrak{m}^k$ por elementos de $\mathcal{O}_P(V)$, y limpiando denominadores, tenemos que existe un $v \in \mathbb{K}[x_1,\ldots,x_n]$, con $v(P) \neq 0$, tal que $\bar{v}\bar{f} \in (\overline{x_1-a_1},\ldots,\overline{x_n-a_n})^k$. Ahora bien, $\bar{v} \notin (\overline{x_1-a_1},\ldots,\overline{x_n-a_n})$, que es maximal, y por tanto

$$(\bar{v}) + (\overline{x_1-a_1},\ldots,\overline{x_n-a_n}) = \Gamma(V).$$

De esta manera, tal como fue demostrado en el lema anterior,

$$(\bar{v}) + (\overline{x_1-a_1},\ldots,\overline{x_n-a_n})^k = \Gamma(V)$$

y, en particular, podemos escribir $\bar{1} = k\bar{v} + \bar{g}$, con $k \in \Gamma(V)$ y $\bar{g} \in (\overline{x_1-a_1}, \ldots, \overline{x_n-a_n})^k$. Multiplicando por $\bar{f}$, $\bar{f} = k\bar{v}\bar{f} + \bar{g}\bar{f}$. Como $\bar{v}\bar{f}, \bar{g} \in (\overline{x_1-a_1}, \ldots, \overline{x_n-a_n})^k$, tenemos el resultado.

Por otra parte, ciertamente

$$\pi^{-1}((\overline{x_1-a_1},\ldots,\overline{x_n-a_n})^k) = (x_1-a_1,\ldots,x_n-a_n)^k + I(V).$$

Así pues, queda probado que, para todo $g \in \mathbb{K}[x_1,\ldots,x_n]$,

$$g \in (x_1-a_1,\ldots,x_n-a_n)^k + I(V) \Leftrightarrow \bar{g} \in \mathfrak{m}^k = (t^k),$$

con lo que queda finalizada la demostración. $\square$

## 1.4. Descomposición primaria

La descomposición primaria servirá a un doble propósito en este trabajo: en primer lugar, constituye una herramienta para demostrar ciertas propiedades de interés sobre los anillos locales; en segundo lugar, nos permitirá llevar a cabo cálculos (en el tercer capítulo) de manera simbólica y sin tener que recurrir a cuerpos de extensión (típicamente trabajaremos en $\mathbb{Q}$).

En esta sección, aquellos resultados que se presentan sin demostración podrán encontrarse en [AM69] Cap.4.

Para comenzar, un **ideal primario** $\mathfrak{q}$ de un anillo $R$ es un ideal $\mathfrak{q} \neq R$ tal que, si $x, y \in R$ son tales que $xy \in \mathfrak{q}$, entonces $x \in \mathfrak{q}$ o $y \in \sqrt{\mathfrak{q}}$. De este modo, por ejemplo, los ideales primos son ideales primarios, y la contracción de un ideal primario vuelve a ser primaria.

Si $\mathfrak{q}$ es un ideal primario, entonces $\mathfrak{p} = \sqrt{\mathfrak{q}}$ es un ideal primo: si $xy \in \sqrt{\mathfrak{q}}$, entonces existe $n > 0$ tal que $(xy)^n \in \mathfrak{q}$. Por definición, o bien $x^n \in \mathfrak{q}$ o bien existe $m > 0$ tal que $y^{nm} \in \mathfrak{q}$. En cualquier caso, $x \in \sqrt{\mathfrak{q}}$ o $y \in \sqrt{\mathfrak{q}}$.

Más aún, como el radical de un ideal es la intersección de todos los primos que contienen a ese ideal, $\mathfrak{p} = \sqrt{\mathfrak{q}}$ es el menor primo que contiene a $\mathfrak{q}$. Decimos que $\mathfrak{q}$ es un ideal $\mathfrak{p}$-primario.

Destacamos el comportamiento de ideales primarios con cocientes de ideales:

**Proposición 1.30.** *[AM69] Sea $\mathfrak{q}$ un ideal $\mathfrak{p}$-primario, $x$ un elemento de $R$. Entonces*

- *Si $x \in \mathfrak{q}$, entonces $(\mathfrak{q} : x) = (1)$.*
- *Si $x \notin \mathfrak{q}$, entonces $(\mathfrak{q} : x)$ es $\mathfrak{p}$-primario.*
- *Si $x \notin \mathfrak{p}$, entonces $(\mathfrak{q} : x) = \mathfrak{q}$.*

Una **descomposición primaria** de un ideal $I$ de $R$ es una expresión de $I$ como intersección finita de ideales primarios. Decimos que una de tales descomposiciones $I = \bigcap \mathfrak{q}_i$ es **minimal** cuando los ideales $\sqrt{\mathfrak{q}_i}$ son todos distintos y, para todo $i = 1, \ldots, n$, se verifica que $\cap_{j \neq i} \mathfrak{q}_j \nsubseteq \mathfrak{q}_i$.

En caso de existencia de descomposición, siempre se puede conseguir una descomposición minimal teniendo en cuenta que la intersección de ideales $\mathfrak{p}$-primarios es $\mathfrak{p}$-primaria y eliminando las componentes redundantes.

Las descomposiciones primarias minimales verifican dos teoremas de unicidad. Por un lado, si $I = \bigcap \mathfrak{q}_i$ es una descomposición minimal y llamamos $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$, entonces estos primos $\mathfrak{p}_i$ son independientes de la descomposición y se denominan **ideales asociados** (o pertenecientes) **a I**. Los elementos minimales del conjunto $\{\mathfrak{p}_i\}$ son llamados **primos aislados**, y el resto son denominados **primos inmersos**. El segundo teorema de unicidad nos dice que las componentes primarias asociadas a primos aislados también son independientes de la descomposición.

Hacemos especial hincapié en el comportamiento de la operación de crear módulos de fracciones $S^{-1}$ con ideales y descomposiciones primarias. Cuando se hable de contracción nos referiremos a la contracción a través del homomorfismo $f : R \to S^{-1}R$ dado por $r \mapsto r/1$. De [AM69]:

**Proposición 1.31.** *Sea $S$ un subconjunto multiplicativamente cerrado de $R$, $\mathfrak{q}$ ideal $\mathfrak{p}$-primario. Entonces:*

- *Si $S \cap \mathfrak{p} \neq \emptyset$, entonces $S^{-1}\mathfrak{q} = S^{-1}R$.*

- *Si $S \cap \mathfrak{p} = \emptyset$, entonces $S^{-1}\mathfrak{q}$ es $S^{-1}\mathfrak{p}$-primario y $(S^{-1}\mathfrak{q})^{-1} = \mathfrak{q}$.*

**Proposición 1.32.** *Sea $S \subseteq R$ multiplicativamente cerrado e $I = \bigcap_{i=1}^{n} \mathfrak{q}_i$ una descomposición minimal del ideal $I$ de $R$. Sea $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Entonces*

$$S^{-1}I = \bigcap_{i=1}^{n} S^{-1}\mathfrak{q}_i, \quad (S^{-1}I)^{\mathfrak{c}} = \bigcap_{S\cap\mathfrak{p}_i=\emptyset} \mathfrak{q}_i,$$

*donde $(S^{-1}I)^{\mathfrak{c}}$ es la contracción de $S^{-1}I$. Además, estas son descomposiciones primarias minimales.*

El Teorema de Lasker-Noether establece que en un anillo noetheriano todo ideal posee descomposición primaria, luego podemos aplicar todo lo anterior a nuestro caso particular, $\mathbb{K}[x_1, \ldots, x_n]$. Finalizamos la sección haciendo uso de este hecho y de los siguientes resultados generales para probar que si $I$ es un ideal de $\mathbb{K}[\underline{x}]$ con $V(I) = \{P_i\}_i$ finito y $\mathbb{K}$ algebraicamente cerrado, entonces $\mathbb{K}[\underline{x}]/I$ es isomorfo a $\prod_i \mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n)$ (caso particular del Teorema de Estructura para anillos de Artin).

**Lema 1.33.** *En un anillo noetheriano $R$, todo ideal contiene a una potencia de su radical.*

*Demostración.* [AM69], Cap.7, Proposición 7.14. □

**Lema 1.34.** *Sean $I_1, \ldots, I_n$ ideales de un anillo $R$, y $\mathfrak{p}$ un ideal primo con $\cap I_i \subset \mathfrak{p}$. Entonces existe $i$ tal que $I_i \subset \mathfrak{p}$.*

*Demostración.* [AM69], Cap. 1, Proposición 1.11. □

**Teorema 1.35.** *Sea $\mathbb{K}$ algebraicamente cerrado, $I$ ideal de $\mathbb{K}[x_1, \ldots, x_n]$, y supongamos que $V(I) = \{P_1, \ldots, P_r\}$ es finito. Entonces, $\mathbb{K}[x_1, \ldots, x_n]/I$ es isomorfo a $\prod \mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n)$.*

*Demostración.* Sea $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k$ una descomposición primaria minimal de $I$, y denotemos $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Como radicales e intersecciones conmutan, tenemos por un lado que

$$\sqrt{I} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k,$$

y por otro lado que, en virtud del Teorema de los Ceros de Hilbert,

$$\sqrt{I} = IV(I) = I(\{P_1, \ldots, P_r\}) = I(P_1) \cap \cdots \cap I(P_r).$$

Podemos deducir de ambas que $k = r$ y para todo $i$ existe $j$ tal que $\mathfrak{p}_i = I(P_j)$. En efecto, observemos que $\bigcap_j I(P_j) \subset \mathfrak{p}_i$ para cada $i$, y que por tanto, según el Lema 1.34, existe $j$ tal que $I(P_j) \subset \mathfrak{p}_i$. De la maximalidad de $I(P_j)$ se obtiene la igualdad. Tal $j$ debe ser único porque los $I(P_i)$ son maximales distintos, por lo que $k = r$. Asumamos que $I(P_i) = \mathfrak{p}_i$.

Tenemos en particular que los $\mathfrak{p}_i$ son dos a dos comaximales, y que por tanto (Lema 1.28) cualesquiera de sus potencias también lo son. Atendiendo al Lema 1.33, existe una potencia $n_i$ tal que $\mathfrak{p}_i^{n_i} \subset \mathfrak{q}_i$, por lo que los $\mathfrak{q}_i$ son dos a dos comaximales.

De esta manera, podemos emplear el Teorema Chino de los Restos para obtener un isomorfismo

$$\mathbb{K}[x_1,\ldots,x_n]/I \xrightarrow{\cong} \prod_{i=1}^{n} \mathbb{K}[x_1,\ldots,x_n]/\mathfrak{q}_i.$$

El siguiente paso es la localización. Fijémonos en primer lugar en que $\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{q}_i$ y $\left(\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{q}_i\right)_{I(P_i)}$ son isomorfos. En efecto, al localizar por el radical de $\mathfrak{q}_i$ consideramos fracciones de la forma $\bar{f}/\bar{g}$ donde $\bar{f},\bar{g} \in \mathbb{K}[x_1,\ldots,x_n]/\mathfrak{q}_i$ y $g \notin I(P_i)$. Ahora bien, tenemos entonces que $(g)+I(P_i)=(1)$, y por el Lema 1.28, que $(g)+\mathfrak{q}_i = (1)$. Por tanto, existen $h \in \mathbb{K}[x_1,\ldots,x_n]$, $q \in \mathfrak{q}_i$ tales que $1 = gh + q$, y tomando clases, $\bar{1} = \bar{g}\bar{h}$. Así, tales fracciones tienen denominadores que ya son unidades de $\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{q}_i$ y, por tanto, son elementos de $\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{q}_i$.

Además, como la localización conmuta con cocientes, tenemos también que

$$\left(\mathbb{K}[x_1,\ldots,x_n]/\mathfrak{q}_i\right)_{I(P_i)} \cong \mathcal{O}_{P_i}(\mathbb{A}^n)/\mathfrak{q}_i\mathcal{O}_{P_i}(\mathbb{A}^n).$$

Finalmente, faltaría por comprobar que $\mathcal{O}_{P_i}(\mathbb{A}^n)/\mathfrak{q}_i\mathcal{O}_{P_i}(\mathbb{A}^n) \cong \mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n)$. Efectivamente, sea $S_i = \mathbb{K}[x_1,\ldots,x_n] - I(P_i)$. Localizar en $I(P_i)$ es realizar la operación $S_i^{-1}$. Como la localización conmuta con intersecciones,

$$S_i^{-1}I = S_i^{-1}\mathfrak{q}_1 \cap \cdots \cap S_i^{-1}\mathfrak{q}_k.$$

Ahora, $S_i \cap \mathfrak{p}_j \neq \emptyset$ para todo $j \neq i$ (más aún, como los $\mathfrak{p}_i$ son comaximales dos a dos, $S_i \cap \mathfrak{p}_j = S_i$), y como vimos al estudiar el comportamiento de la localización con los ideales primarios, esto implica que $S_i^{-1}\mathfrak{q}$ es el total. Por tanto,

$$I\mathcal{O}_{P_i}(\mathbb{A}^n) = S_i^{-1}I = S_i^{-1}\mathfrak{q}_i = \mathfrak{q}_i\mathcal{O}_{P_i}(\mathbb{A}^n),$$

con lo que damos por terminada la demostración. □

**Corolario 1.36.** *Sea $\mathbb{K}$ algebraicamente cerrado, $I$ ideal de $\mathbb{K}[x_1,\ldots,x_n]$ con $V(I) = \{P_1,\ldots,P_r\}$ finito. Si $I = \bigcap_{j=1}^{k} \mathfrak{q}_j$ es descomposición primaria minimal de $I$, entonces $k = r$, podemos suponer que $\sqrt{\mathfrak{q}_i} = I(P_i)$, y*

$$\mathcal{O}_{P_i}(\mathbb{A}^n)/I\mathcal{O}_{P_i}(\mathbb{A}^n) \cong \mathbb{K}[x_1,\ldots,x_n]/\mathfrak{q}_i.$$

*Demostración.* Ha sido probado a lo largo de la demostración del teorema anterior. □

# Capítulo 2

# Curvas algebraicas planas

A lo largo del primer capítulo hemos analizado de manera general las herramientas algebraicas que necesitaremos. A partir de ahora nos centraremos en el estudio de las curvas algebraicas planas. Como adelantamos en la introducción, comenzaremos presentando la noción de curva algebraica plana y los conceptos asociados de multiplicidad de un punto o tangente a una curva, junto con los resultados básicos referentes a éstos. Acto seguido, pasaremos a trabajar con curvas en el plano proyectivo, extendiendo a este caso algunos de los objetos introducidos en el caso afín, lo que nos permitirá posteriormente introducir la multiplicidad de intersección y establecer el Teorema de Bézout. Tras esto, discutiremos la existencia de modelos no singulares de curvas planas y explicaremos cómo obtener, mediante transformaciones cuadráticas del plano proyectivo, curvas birracionalmente equivalentes a una curva dada pero en que las singularidades sean todas ordinarias. Finalmente pasaremos a desarrollar la teoría de divisores de curvas no singulares, lo que culminará con la demostración del Teorema de Riemann y la definición del género.

En el resto de la memoria supondremos que $\mathbb{K}$ es un cuerpo algebraicamente cerrado y de característica cero, siendo así aplicables todos los resultados previamente expuestos.

## 2.1. Curvas algebraicas planas afines

**Definición 2.1.** *Una* ***curva algebraica plana afín*** $\mathcal{C}$ *sobre* $\mathbb{K}$ *es el subconjunto algebraico de* $\mathbb{A}^2$ *definido por un polinomio no constante* $f \in \mathbb{K}[x,y]$*, es decir,*

$$\mathcal{C} = V(f) = \{(a,b) \in \mathbb{A}^2 / f(a,b) = 0\}.$$

Observemos que, con esta definición y puesto que trabajamos en un cuerpo de característica cero (en particular, infinito), dos polinomios $f, g$ definen la misma curva si y sólo si $g = \lambda f$ para cierto $\lambda \in \mathbb{K}$ no nulo,esto es, el polinomio que define una curva está unívocamente determinado salvo producto por constantes. En ocasiones abusaremos de notación y nos referiremos por $f$ a la curva definida por el polinomio $f \in \mathbb{K}[x,y]$.

El **grado** de una curva es el grado total del polinomio que la define.

Si $f = \prod_{i=1}^{n} f_i^{n_i}$ es la descomposición de $f$ en factores irreducibles, diremos que cada curva $f_i$ es una **componente irreducible** de $f$ de **multiplicidad** $n_i$. Decimos

que $\mathcal{C}$ es una curva **irreducible** si el polinomio que la define es irreducible (en cuyo caso $\mathcal{C}$ es una variedad).

**Definición 2.2.** *Sea $\mathcal{C}$ una curva algebraica afín de grado $d$ definida por $f \in \mathbb{K}[x,y]$, $P = (0,0)$. Escribamos $f = f_m + f_{m+1} + \cdots + \cdots + f_d$ donde $f_i \in \mathbb{K}[x,y]$ es un polinomio homogéneo de grado $i$ y $f_m, f_d \neq 0$. Decimos que $m$ es la* ***multiplicidad de*** *$(0,0)$* ***en*** *$\mathcal{C}$.*

*Extendemos la definición a cualquier otro punto $P = (a,b)$ de la siguiente manera: consideramos el polinomio $f(X+a, Y+b)$ (aplicamos una transformación que lleva el origen en $P$), y lo descomponemos en suma de homogéneos como antes,*

$$f(X+a, Y+b) = f'_{m'} + f'_{m'+1} \cdots + f'_d.$$

*Decimos que $m'$ es la* ***multiplicidad de*** *$P = (a,b)$* ***en*** *$\mathcal{C}$ o multiplicidad de $\mathcal{C}$ en $P$, y la denotamos por $m_P(C)$. En particular, $m_P(\mathcal{C}) = 0$ si y sólo si $P \notin \mathcal{C}$.*

*Como todo polinomio homogéneo en dos variables se descompone en factores lineales (en $\mathbb{K}$ algebraicamente cerrado), tenemos que en la notación anterior,*

$$f'_{m_P(\mathcal{C})} = \prod (a_i X + b_i Y)^{e_i},$$

*donde los $a_i X + b_i Y$ son rectas distintas. Se dice que cada recta*

$$L_i = a_i(X-a) + b_i(Y-b)$$

*es una* ***recta tangente a*** *$\mathcal{C}$* ***en*** *$P$ de* ***multiplicidad*** *$e_i$.*

Decimos que un punto $P \in \mathcal{C}$ es **simple** si $m_P(\mathcal{C}) = 1$, y **singular** en caso contrario. Decimos que un punto singular $P$ es **ordinario** si todas las tangentes a $\mathcal{C}$ en $P$ son diferentes, y **no ordinario** en otro caso.

La multiplicidad de un punto en una curva puede estudiarse a través de las derivadas parciales del polinomio que la define:

**Proposición 2.3.** *Sea $\mathcal{C}$ una curva plana afín definida por $f$. Un punto $P \in \mathcal{C}$ tiene multiplicidad $r$ si y sólo si todas las derivadas parciales de $f$ hasta grado $r-1$ se anulan en $P$, y al menos una de grado $r$ no se anula en $P$. En particular, un punto es simple si y sólo si $(f_X(P), f_Y(P)) \neq (0,0)$.*

*Demostración.* Sea $d = deg(f)$. El resultado se deduce directamente del desarrollo de Taylor en un entorno de $(0,0)$

$$f(x+a, y+b) = \sum_{k=0}^{d} \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} \frac{\partial^k f}{\partial x^i \partial y^{k-i}}(P) x^i y^{k-i}.$$

Así, la componente homogénea $f_k$ de la descomposición $f(x+a, y+b) = f_0 + f_1 + \cdots + f_d$ coincide precisamente con

$$f_k = \frac{1}{k!} \sum_{i=0}^{k} \binom{k}{i} \frac{\partial^k f}{\partial x^i \partial y^{k-i}}(P) x^i y^{k-i}.$$

La multiplicidad viene dada por el menor $k$ tal que $f_k \neq 0$, con lo que efectivamente la multiplicidad es $r$ si y sólo si todas las derivadas parciales de $f$ hasta grado $r-1$ se anulan en $P$, y al menos una de grado $r$ es no nula en $P$. □

De la propia demostración obtenemos que las tangentes a $\mathcal{C}$ en un punto $P = (a, b)$ de multiplicidad $r$ son los factores irreducibles de

$$\sum_{i=0}^{r} \binom{r}{i} \frac{\partial^r f}{\partial x^i \partial y^{r-i}}(P)(x-a)^i(y-b)^{r-i}.$$

La multiplicidad en un punto goza de la siguiente propiedad deseable:

**Proposición 2.4.** *Sea $\mathcal{C}$ una curva plana afín definida por $f \in \mathbb{K}[x, y]$, y supongamos que $f = \prod_{i=1}^{n} f_i^{n_i}$ es la descomposición de $f$ en factores irreducibles. Entonces*

$$m_P(\mathcal{C}) = \sum_{i=1}^{n} n_i m_P(f_i)$$

*y, si $L$ es tangente a $f_i$ en $P$ de multiplicidad $s_i$, entonces es tangente a $\mathcal{C}$ de multiplicidad $\sum n_i s_i$.*

*Demostración.* Sea $P = (a, b)$, $m_i = m_P(f_i)$, $d_i = deg(f_i)$. Escribamos cada $f_i(x + a, y + b)$ como suma de homogéneos: $f_i(x + a, y + b) = f_{i,m_i} + \cdots + f_{i,d_i}$. Como $f(x + a, y + b) = \prod f_i(x + a, y + b)^{n_i}$, es claro que el polinomio homogéneo de menor grado en $f(x + a, y + b)$ es exactamente $\prod f_{i,m_i}^{n_i}$. Por tanto su grado, es decir, la multiplicidad de $P$ en $\mathcal{C}$, es $\sum n_i m_i$, y si $L$ es tangente a $f_i$ en $P$ de multiplicidad $s_i$, entonces aparece como factor de $\prod f_{i,m_i}^{n_i}$ de multiplicidad $\sum n_i s_i$. □

A continuación demostraremos que una curva plana afín irreducible tiene sólo un número finito de singularidades. Para ello, nos basaremos en las propiedades de la resultante de dos polinomios.

**Proposición 2.5.** *El número de puntos singulares de una curva plana afín irreducible es finito.*

*Demostración.* Sea $\mathcal{C}$ una curva plana afín irreducible definida por el polinomio $f$. El conjunto de puntos singulares es $V(f, f_X, f_Y)$. Como $f$ no es constante, al menos una de sus derivadas parciales, pongamos $f_X$, es no nula. Sean $R_X = Res_X(f, f_X)$, $R_Y = Res_Y(f, f_X)$ sus resultantes respecto a cada variable. Si ambas son no nulas, el número de posibles ceros comunes a $f$ y $f_X$ es finito y hemos acabado. Si una es idénticamente nula, $f$ y $f_X$ comparten una componente irreducible en común, lo cual es imposible porque $f$ es irreducible y no puede ser componente de $f_X$. □

A tenor del siguiente resultado, la proposición anterior sigue siendo válida para curvas planas definidas por polinomios libres de cuadrados, dado que la Proposición 2.4 implica que en este caso los puntos múltiples de $\mathcal{C}$ son los puntos múltiples de cada una de sus componentes y los puntos de intersección de dos componentes.

**Proposición 2.6.** *Si $\mathcal{C}$ y $\mathcal{C}'$ son dos curvas sin componentes en común, entonces su intersección es un número finito de puntos.*

*Demostración.* Sean $f$ y $f'$, respectivamente, los polinomios que definen a $\mathcal{C}$ y $\mathcal{C}'$, y consideremos la resultante de ambos con respecto a cada variable, $R_X = Res_X(f, f') \in \mathbb{K}[Y]$, $R_Y = Res_Y(f, f') \in \mathbb{K}[X]$. Como $f$ y $f'$ no tienen componentes en común, tenemos que $R_X$ y $R_Y$ son polinomios no nulos, y que, si $(x, y) \in V(f, f')$, entonces $x$ es raíz de $R_Y$ e $y$ es raíz de $R_X$. Como el número de raíces de ambos polinomios es finito, las posibles combinaciones también y se tiene el resultado. □

Veamos que el concepto de multiplicidad de un punto en una curva puede estudiarse en términos de los anillos locales $\mathcal{O}_{\mathcal{P}}$ asociados a cada una de sus componentes irreducibles (recordemos que los anillos locales se definen sobre variedades). Así obtenemos, dada la Proposición 1.21, que la multiplicidad es independiente de las coordenadas escogidas.

**Teorema 2.7.** *Sea $P$ un punto de una curva irreducible $\mathcal{C}$, y sea $\mathfrak{m}_P$ el ideal maximal del anillo local $\mathcal{O}_P(\mathcal{C})$. Entonces, para todo $n$ suficientemente grande ($n \geq m_P(\mathcal{C})$),*

$$m_P(\mathcal{C}) = dim_{\mathbb{K}}(\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}).$$

*Demostración.* Para todo $n$, la aplicación $\varphi : \mathcal{O}_P/\mathfrak{m}_P^{n+1} \longrightarrow \mathcal{O}_P/\mathfrak{m}_P^n$ dada por $\phi(z + \mathfrak{m}_P^{n+1}) = z + \mathfrak{m}_P^n$ está bien definida pues $\mathfrak{m}_P^{n+1} \subset \mathfrak{m}_P^n$ y constituye un epimorfismo con núcleo $ker\varphi = \mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}$. De este modo, por el Teorema de rango-nulidad,

$$dim_{\mathbb{K}}(\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}) = dim_{\mathbb{K}}(\mathcal{O}_P/\mathfrak{m}_P^{n+1}) - dim_{\mathbb{K}}(\mathcal{O}_P/\mathfrak{m}_P^n),$$

y lo que probaremos será que existe una constante $c \in \mathbb{Z}$ tal que, para todo $n \geq m_P(\mathcal{C})$, $dim_{\mathbb{K}}(\mathcal{O}_P/\mathfrak{m}_P^n) = nm_P(\mathcal{C}) + c$. Si $P = (a, b)$, sabemos que $\mathfrak{m}_P = (\overline{x-a}, \overline{y-b})\mathcal{O}_P$. Como $V(\mathfrak{m}_P^n) = \{P\}$, se tiene aplicando el Teorema 1.35 y la Proposición 1.24 que

$$\mathbb{K}[x, y]/(I^n, f) \cong \mathcal{O}_P(\mathbb{A}^2)/(I^n, f)\mathcal{O}_P(\mathbb{A}^2) \cong \mathcal{O}_P(\mathcal{C})/\mathfrak{m}_P^n,$$

donde $I = (x-a, y-b)$. De este modo debemos calcular la dimensión de $\mathbb{K}[x, y]/(I^n, f)$. Denotemos $m = m_P(\mathcal{C})$. Consideremos el epimorfismo natural $\varphi : \mathbb{K}[x, y]/I^n \to \mathbb{K}[x, y]/(I^n, f)$, y observemos que su núcleo es isomorfo a $\mathbb{K}[x, y]/I^{n-m}$ vía

$$\psi : \mathbb{K}[x, y]/I^{n-m} \longrightarrow ker\varphi$$

dada por $\psi(\bar{g}) = \bar{f}\bar{g}$. Para ver que $\psi$ está bien definido tengamos en cuenta que por definición de multiplicidad en $(a, b)$, $f(x + a, y + b) = f_m +$ formas de mayor grado y, por tanto, $f(x, y) = f_m(x-a, y-b) +$ formas en $x - a$, $y - b$ de mayor grado $\in I^m$ de modo que $fg \in I^n$ para todo $g \in I^{n-m}$. Esto implica que la definición es independiente del representante escogido. Además, $\psi(\bar{g}) \in ker\varphi$ porque $fg \in (I^n, f)$. Es claro que es un homomorfismo, luego falta demostrar que es inyectiva y sobre:

La aplicación es inyectiva, pues si $\bar{g}, \bar{g'}$ son tales que $\bar{f}\bar{g} = \bar{f}\bar{g'}$, entonces $\overline{f(g - g')} \in I^n$. Como $f \in I^m$ (y $f \notin I^{m+1}$), necesariamente $\overline{g - g'} \in I^{n-m}$, esto es, $\bar{g} = \bar{g'}$. También es sobre, pues si $\bar{h} \in ker\varphi$, entonces $h \in (I^n, f)$ y existen $g \in \mathbb{K}[x, y]$, $q \in I^n$ tales que $h = q + fg$. Esto quiere decir que $\bar{h} = \psi\bar{g}$.

Por el Teorema del rango-nulidad, $dim_{\mathbb{K}}(\mathbb{K}[x, y]/(I^n, f)) = dim_{\mathbb{K}}(\mathbb{K}[x, y]/I^n) - dim_{\mathbb{K}}(\mathbb{K}[x, y]/I^{n-m})$. Ahora, como $\mathbb{K}[x, y]/I^k$ tiene por base $\{x^i y^j\}_{i+j<k}$, tiene dimensión $k(k + 1)/2$, y por tanto

$$dim_{\mathbb{K}}(\mathbb{K}[x, y]/(I^n, f)) = \frac{n(n+1)}{2} - \frac{(n-m)(n-m+1)}{2} = nm - \frac{m(m-1)}{2},$$

como queríamos ver [$m(m - 1)/2$ es la constante independiente de $n$]. □

Además, de la proposición que presentamos a continuación se deduce una nueva caracterización de los puntos simples en términos de anillos locales:

**Proposición 2.8.** *Sea $P$ un punto de una curva irreducible $\mathcal{C}$, y sea $\mathfrak{m}_P$ el ideal maximal del anillo local $\mathcal{O}_P(\mathcal{C})$. Entonces, para todo $0 \leq n < m_P(\mathcal{C})$,*

$$n + 1 = dim_{\mathbb{K}}(\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}).$$

*Demostración.* Como en la demostración anterior, sigue siendo cierto que

$$dim_{\mathbb{K}}(\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}) = dim_{\mathbb{K}}(\mathcal{O}_P/\mathfrak{m}_P^{n+1}) - dim_{\mathbb{K}}(\mathcal{O}_P/\mathfrak{m}_P^n),$$

y que $\mathcal{O}_P(\mathcal{C})/\mathfrak{m}_P^n \cong \mathbb{K}[x,y]/(I^n, f)$. Sin embargo, como $n < m_P(\mathcal{C})$, se tiene en esta ocasión que $f \in I^{m_P(\mathcal{C})} \subset I^n$, y por tanto $\mathbb{K}[x,y]/(I^n, f) = \mathbb{K}[x,y]/(I^n)$. Puesto que la dimensión de este último es $n(n+1)/2$, obtenemos que

$$dim_{\mathbb{K}}(\mathfrak{m}_P^n/\mathfrak{m}_P^{n+1}) = \frac{(n+1)(n+2)}{2} - \frac{n(n+1)}{2} = n+1.$$

□

**Corolario 2.9.** *Un punto $P$, de una curva irreducible $\mathcal{C}$, es simple, si y sólo si $dim_{\mathbb{K}}(\mathfrak{m}_P/\mathfrak{m}_P^2) = 1$*

*Demostración.* Si $m_P(\mathcal{C}) = 1$, aplicamos el Teorema 2.7 con $n = m_P(\mathcal{C})$ para obtener el resultado. Si $m_P(\mathcal{C}) > 1$, la Proposición 2.8 para $n = 1$ nos dice que $dim_{\mathbb{K}}(\mathfrak{m}_P/\mathfrak{m}_P^2) = 2$. □

Concluimos la sección viendo que además, los puntos simples tienen asociados anillos locales que son de valoración discreta, y el recíproco es también cierto. Para ello, será necesario el siguiente resultado elemental de la geometría afín:

**Lema 2.10.** *Sean $P, P' \in \mathbb{A}^2$, $L_1, L_2$ dos rectas distintas que pasan por $P$, y $L_1', L_2'$ dos rectas distintas que pasan por $P'$. Entonces existe un cambio de coordenadas $T$ tal que $T(P) = P'$ y $T(L_i) = L_i'$.*

**Teorema 2.11.** *Un punto $P$ de una curva irreducible $\mathcal{C}$ es simple si y sólo si $\mathcal{O}_P(\mathcal{C})$ es un anillo de valoración discreta. Además, para toda recta $L$ que pase por $P$ y no sea tangente a $\mathcal{C}$ en $P$, se tiene que $\bar{L}$ es parámetro de uniformización.*

*Demostración.* "⇐" Sea $\mathfrak{m} = (t)$ el ideal maximal de $\mathcal{O}_P(\mathcal{C})$. Claramente, tenemos que $dim_{\mathbb{K}}(\mathfrak{m}/\mathfrak{m}^2) = dim_{\mathbb{K}}(t)/(t^2) = 1$ luego, por el Corolario 2.9, $P$ es simple.

"⇒" Como la multiplicidad de un punto es independiente de coordenadas, y en virtud del Lema 2.10, podemos suponer que $P = (0,0)$, $L = x$ y la recta tangente es $L' = y$. Sea $f$ el polinomio que define a $\mathcal{C}$. Ya que la tangente en $(0,0)$ coincide con la forma de menor grado en la descomposición de $f$ como $f = f_0 + \cdots + f_d$, podemos escribir $f = y +$ formas de mayor grado $= yg - x^2h$, para ciertos $g, h \in \mathbb{K}[x,y]$, $g = 1 +$ términos de grado superior. Así, $\bar{g}$ es unidad en $\mathcal{O}_P(\mathcal{C})$, y $\bar{y} = \bar{x}^2\bar{h}\bar{g}^{-1} \in (\bar{x})\mathcal{O}_P(\mathcal{C})$ De esta manera, $\mathfrak{m} = (\bar{x}, \bar{y})\mathcal{O}_P(\mathcal{C}) = (\bar{x})\mathcal{O}_P(\mathcal{C})$ es principal, y en definitiva $\mathcal{O}_P$ es de valoración discreta. □

## 2.2. Curvas algebraicas planas proyectivas

En la sección anterior vimos que dos curvas sin componentes en común tienen intersección finita. Buscaremos definir una noción de multiplicidad de un punto de intersección de manera que se verifiquen ciertas propiedades deseables, y como adelantábamos al inicio del capítulo, la forma de conseguirlo requiere trabajar en el plano proyectivo $\mathbb{P}^2$.

**Definición 2.12.** *Una* ***curva proyectiva plana*** $\mathcal{C}$ *sobre* $\mathbb{K}$ *es el conjunto (proyectivo) de ceros de un polinomio homogéneo* $F \in \mathbb{K}[x,y,z]$*, esto es,*

$$\mathcal{C} = V_{\mathbb{P}^2}(F) = \{(a:b:c) \in \mathbb{P}^2 / F(a,b,c) = 0\}.$$

*Denotaremos en ocasiones* $\mathcal{C}$ *por el polinomio que lo define (que es único salvo producto por escalares).*

Todas los conceptos introducidos en el caso de curvas afines, como el grado o las componentes irreducibles de una curva, se extienden de forma natural al caso proyectivo. Si $\mathcal{C}$ es una curva proyectiva irreducible también podemos definir, no sin antes tomar las precauciones correspondientes, su cuerpo de funciones o su anillo local en un punto. Para ello, sea $\Gamma(\mathcal{C}) = \mathbb{K}[x,y,z]/I(\mathcal{C})$, donde $I(\mathcal{C})$ es la extensión de la noción de ideal asociado a un subconjunto de $\mathbb{P}^2$, esto es, el conjunto de los polinomios $G \in \mathbb{K}[x,y,z]$ tales que para todo $P \in \mathcal{C}$ y para toda elección $(a:b:c)$ de las coordenadas homogéneas de $P$, $G(a,b,c) = 0$. De la misma manera que ocurre en el afín, $\mathcal{C}$ es irreducible si y sólo si $I(\mathcal{C})$ es primo, luego $\Gamma(\mathcal{C})$ es un dominio y podemos considerar su cuerpo de fracciones $\mathcal{K}$. Sin embargo, los elementos $\bar{G}/\bar{H}$ de $\mathcal{K}$ no son en general funciones, pues si escogemos dos representaciones distintas $(a,b,c)$, $(a',b',c')$ de un mismo punto de $\mathbb{P}^2$ ,en general $G(a,b,c)/H(a,b,c) \neq G(a',b',c')/H(a',b',c')$. Así, el **cuerpo de funciones racionales** de $\mathcal{C}$ se define como el subcuerpo de $\mathcal{K}$ formado por los elementos $\bar{G}/\bar{H}$ donde $G, H$ son formas del mismo grado $d$, pues en ese supuesto si $(a:b:c) = (a':b':c')$ no anulan a $H$, pongamos $(a,b,c) = \lambda(a',b',c')$, entonces

$$\frac{G(a,b,c)}{H(a,b,c)} = \frac{G(\lambda(a',b',c'))}{H(\lambda(a',b',c'))} = \frac{\lambda^d G(a',b',c')}{\lambda^d H(a',b',c')} = \frac{G(a',b',c')}{H(a',b',c')}.$$

Lo denotaremos por $\mathbb{K}(\mathcal{C})$. Diremos que un elemento $\varphi \in \mathbb{K}(\mathcal{C})$ **está definido en** $P \in \mathcal{C}$ si $\varphi = \bar{G}/\bar{H}$, con $G, H$ formas de mismo grado y $H(P) \neq 0$, y que su **valor** es $G(P)/H(P)$, que no depende del representante escogido. De esta manera definimos el **anillo local** $\mathcal{O}_P(\mathcal{C})$ como el conjunto de funciones racionales definidas en $P$, que tiene por maximal al conjunto de funciones racionales que se anulan en $P$.

Todo isomorfismo lineal $T : \mathbb{A}^3 \to \mathbb{A}^3$ lleva rectas que pasan por el origen a rectas que pasan por el origen, y por tanto define una biyección $T : \mathbb{P}^2 \to \mathbb{P}^2$ que denominamos **cambio proyectivo de coordenadas**. Si el isomorfismo viene determinado por la matriz $[a_{ij}]$, y $\mathcal{C}$ es una curva proyectiva plana, entonces $T^{-1}(\mathcal{C})$ es la curva proyectiva $V_{\mathbb{P}^2}(F(a_{11}x + a_{12}y + a_{13}z, a_{12}x + a_{22}y + a_{23}z, a_{31}x + a_{32}y + a_{33}z))$. Del mismo modo que en la Proposición 1.21, si $T$ es un cambio de coordenadas proyectivo y $T(Q) = P$, entonces se induce un isomorfismo $\mathcal{O}_P(\mathcal{C}) \cong \mathcal{O}_Q(T^{-1}(\mathcal{C}))$.

Para $F \in \mathbb{K}[x,y,z]$, denotamos por $F_{*,z}$ (o simplemente $F_*$) a la deshomogeneización de $F$ por la variable $z$, o sea, $F(x,y,1)$. Recíprocamente, dado $f = f_0 + f_1 + \cdots + f_d \in \mathbb{K}[x,y]$, $f_i$ homogéneo de grado $i$, denotamos $f^{*,z}$ (o simplemente $f^*$) al polinomio homogeneizado $f_0 z^d + f_1 z^{d-1} + \cdots + f_d$. Se tiene inmediatamente que para todo $f \in \mathbb{K}[x,y]$, $(f^*)_* = f$ y, para todo $F \in \mathbb{K}[x,y,z]$, $Z^d(F_*)^* = F$, donde $Z^d$ divide a $F$ y $Z^{d+1}$ no. En particular, si $F$ es irreducible, $(F_*)^* = F$.

Así pues, si $\mathcal{C}$ es una curva proyectiva plana irreducible definida por la forma irreducible $F \in \mathbb{K}[x,y,z]$ y si $P = (a:b:1) \in \mathcal{C}$, tenemos un isomorfismo de $\mathcal{O}_P(\mathcal{C})$ en $\mathcal{O}_{(a,b)}(F_*)$ dado por $\overline{F}/\overline{G} \mapsto \overline{F_*}/\overline{G_*}$ con inversa dada por $\overline{f}/\overline{g} \mapsto \overline{f^*}/\overline{g^*}$. Definimos así la **multiplicidad de una curva proyectiva** plana $F$ **en un punto** $P = (a : b : 1)$ como la multiplicidad de $F_*$ en $(a,b)$, y de forma análoga (deshomogeneizando

con respecto a la variable adecuada) para puntos $(a : 1 : c)$ o $(1 : b : c)$. Esta definición es independiente de cambios de coordenadas proyectivos y de la variable con respecto a la cual deshomogeneizamos (caso de tener más de una posibilidad) dado que la noción en el caso afín sólo depende de anillos locales (para el caso reducible, estudiando cada componente irreducible) y los cambios de coordenadas proyectivos inducen isomorfismos entre éstos.

Si $G$ es un polinomio homogéneo de $\mathbb{K}[x, y, z]$ y $P = (a : b : 1)$ es un punto simple de una curva irreducible $F$, definiremos su orden como $ord_P(G) := ord_P(\bar{G}_*)$ en $\mathcal{O}_{(a,b)}(F_*)$.

Esto nos proporciona un método para calcular multiplicidades trabajando directamente con la curva proyectiva:

**Lema 2.13.** *Sea $F$ un polinomio homogéneo de $\mathbb{K}[x, y, z]$ de grado $d$. Entonces:*

- *(Fórmula de Euler) $xF_X + yF_Y + zF_Z = d \cdot F$.*
- *$\frac{\partial^{i+j} F_*}{\partial x^i \partial y^j} = \left(\frac{\partial^{i+j} F}{\partial x^i \partial y^j}\right)_*$. En particular, $\frac{\partial^{i+j} F_*}{\partial x^i \partial y^j}(a, b) = \frac{\partial^{i+j} F}{\partial x^i \partial y^j}(a, b, 1)$.*

**Proposición 2.14.** *Sea $F$ una curva proyectiva plana de grado $d$. Un punto $P = (a : b : c) \in \mathbb{P}^2$ tiene multiplicidad al menos $r$ $(r \leq d)$ si y sólo si todas las derivadas parciales (r-1)-ésimas de $F$ se anulan en $P$, esto es,*

$$\frac{\partial^{i+j+k} F}{\partial x^i \partial y^j \partial z^k}(P) = 0, \text{ para todo } i, j, k \text{ con } i + j + k = r - 1,$$

*donde se entiende $F(P) := F(a, b, c)$.*

*Demostración.* Es una aplicación directa e iterada de la fórmula de Euler. □

De forma similar, las **tangentes a $F$ en $P = (a : b : 1)$** se obtienen como resultado de homogeneizar las tangentes a $F_*$ en $(a, b)$. Así, por ejemplo,

**Proposición 2.15.** *Si $P \in \mathbb{P}^2$ es un punto simple de una curva proyectiva plana $F$, entonces la tangente a $F$ en $P$ viene dada por*

$$xF_X(P) + yF_Y(P) + zF_Z(P).$$

*Demostración.* En efecto, si $P = (a : b : 1)$, entonces la tangente proviene de homogeneizar la tangente a $F_*$ en $(a, b)$. Como consecuencia de la Proposición 2.3 vimos que la tangente a un punto simple $(a, b)$ es

$$(x - a)\frac{\partial f}{\partial x}(a, b) + (y - b)\frac{\partial f}{\partial y}(a, b),$$

y por tanto homogeneizando y teniendo en cuenta *2.* del Lema 2.13, obtenemos que la tangente en el caso proyectivo es

$$(x - az)F_X(P) + (y - bz)F_Y(P) = xF_X(P) + yF_Y(P) + z(-aF_X(P) - bF_Y(P)).$$

Pero por la fórmula de Euler evaluada en $P = (a : b : 1)$, este último sumando es exactamente $zF_Z(P)$. □

También existe un análogo de la Proposición 2.6 para el caso proyectivo:

**Proposición 2.16.** *Si $F$ y $G$ son curvas proyectivas planas sin componentes en común, entonces su intersección es finita.*

*Demostración.* Como $F$ y $G$ no tienen componentes en común, podemos suponer que $Z$ no divide a $F$. Así, $F$ sólo tiene un número finito de puntos en el infinito y, por tanto, existe un número finito de puntos de intersección en el infinito.

El resto de puntos serán de la forma $(a : b : 1)$ y por tanto estarán asociados a $(a, b) \in F_* \cap G_*$. Ahora bien, $F_*$ y $G_*$ no tienen componentes en común (si no, las tendrían $F$ y $G$), luego la Proposición 2.6 aplica y hemos acabado. □

Concluimos la sección contemplando que, del mismo modo que toda curva proyectiva tiene asociadas diversas (infinitas) curvas afines, toda curva afín tiene asociada, de manera natural, una curva proyectiva a la que denominamos su clausura proyectiva.

**Definición 2.17.** *Sea $\mathcal{C}$ una curva proyectiva afín definida por el polinomio $f \in \mathbb{K}[x, y]$. Llamamos* ***clausura proyectiva de $\mathcal{C}$ en $\mathbb{P}^2$*** *a la curva proyectiva $\mathcal{C}^*$ definida por el polinomio homogeneizado $f^*$.*

Así pues, los puntos $(a, b)$ de $\mathcal{C}$ se corresponden con los puntos $(a : b : 1)$ de $\mathcal{C}^*$, y el resto de puntos en $\mathcal{C}^*$ son los puntos en el infinito (coordenada $z = 0$). Si $f = f_0 + \cdots + f_d$, con $f_i$ homogéneo de grado $i$, entonces estos puntos adicionales son los que anulan a $f_d$, y como $f_d$ se descompone en factores lineales, puede haber a lo sumo $d$ puntos en el infinito.

Tal y como hemos ido analizando, existe total compatibilidad entre las definiciones en $\mathcal{C}$ y en su clausura proyectiva. En adelante, siempre que trabajemos sobre una curva plana afín pensaremos implícitamente en su clausura proyectiva.

## 2.3. Multiplicidad de intersección

Existen diversas maneras de introducir la multiplicidad de intersección, bien a través de axiomas "deseables" que la determinan de forma unívoca, o bien mediante herramientas o propiedades de objetos matemáticos como pueden ser las resultantes o las dimensiones de ciertos espacios vectoriales. Dado que las relaciones entre las diferentes definiciones en este último caso no son, en general, evidentes sin pasar por la definición axiomática y carecen en ocasiones de una justificación intuitiva asociada, presentaremos la multiplicidad con tales axiomas y nos referiremos luego a la amplia literatura existente para acreditar los otros métodos de cálculo.

Las referencias principales en esta sección serán [Vai96] y [Ful71].

**Definición 2.18.** *Sean $F$ y $G$ dos curvas proyectivas planas, $P \in \mathbb{P}^2$. Llamamos* ***multiplicidad de intersección de $F$ y $G$ en $P$*** *al número $mult_P(F, G)$ que verifica:*

1. *$mult_P(F, G)$ es un número entero no negativo o $\infty$.*
2. *$mult_P(F, G) = 0 \Leftrightarrow P \notin F \cap G$.*
3. *$mult_P(F, G) = \infty \Leftrightarrow P$ pertenece a una componente común de $F$ y $G$.*
4. *$mult_P(F, G) = mult_P(G, F)$.*
5. *Si $T$ es un cambio de coordenadas proyectivo y $T(Q) = P$, entonces $mult_P(F, G) = mult_Q(T^{-1}(F), T^{-1}(G))$.*

6. $mult_P(F,G) \geq m_P(F)m_P(G)$, *con igualdad si y sólo si* $F$ *y* $G$ *no poseen tangentes en común en* $P$.

7. $mult_P(F, G + AF) = mult_P(F,G)$ *para todo polinomio homogéneo* $A$ *de grado* $deg(G) - deg(F)$.

8. $mult_P(F, G_1G_2) = mult_P(F,G_1) + mult_P(F,G_2)$.

Esta definición es consistente, esto es, existe un único número $mult_P(F,G)$ verificando las propiedades anteriores para todos $F$, $G$ y $P$:

**Proposición 2.19.** *Sean* $F$ *y* $G$ *dos curvas proyectivas planas,* $P \in \mathbb{P}^2$. *El número* $mult_P(F,G)$ *queda completamente determinado por las propiedades anteriores.*

*Demostración.* [Vai96], Cap. 6, Prop. 6. □

**Corolario 2.20.** $mult_P(F,G)$ *depende únicamente de las componentes de* $F$ *y* $G$ *que pasan por* $P$.

*Demostración.* Consecuencia directa de *8.* y *2.*. □

Cualquier método "explícito" que respete los axiomas anteriores nos brinda una nueva posibilidad para calcular $mult_P(F,G)$. Mencionaremos dos de estas opciones:

### 2.3.1. Cálculo mediante resultantes

La primera de las posibilidades que comentamos viene recogida detalladamente en [Vai96], Cap. 5 y 6. Sean $F$ y $G$ dos curvas planas sin componentes en común, y por tanto con un número finito de puntos de intersección.

**Definición 2.21.** *Supongamos que* $F \cap G = \{P_1, \ldots, P_n\}$. *Decimos que* $F$ *y* $G$ *están* ***muy bien posicionadas*** *si* $P_0 = (0:1:0)$ *no está en* $F \cap G$ *ni en ninguna recta que conecte dos puntos de intersección* $P_i$ *y* $P_j$.

Comenzamos observando que esta última condición equivale a decir que, si $P_i = (x_i : y_i : z_i)$, $P_j = (x_j : y_j : z_j)$ son dos puntos distintos de $F \cap G$, entonces $(x_i : z_i) \neq (x_j : z_j)$. En efecto, $(x_i : z_i) = (x_j : z_j)$ si y sólo si existe $\lambda \in \mathbb{K}$ tal que $(x_i, z_i) = \lambda(x_j, z_j)$, esto es, si $(0:1:0) = (0 : y_i - \lambda y_j : 0) = P_i - \lambda P_j$ está en la recta que une $P_i$ con $P_j$.

Además, si $F$ y $G$ tienen grados $m$ y $n$, respectivamente, y escribimos

$$F = aY^m + \text{ términos de grado } <\text{m en Y}$$
$$G = bY^n + \text{ términos de grado } <\text{n en Y},$$

la condición $(0:1:0) \notin F \cap G$ asegura que $(a,b) \neq (0,0)$ y, por tanto, su resultante $R_Y = R_Y(F,G)$ respecto de $y$ es un polinomio homogéneo en $\mathbb{K}[x,z]$ de grado $mn$ ([Vai96], Cap. 2, Lema 16) tal que para todo $(x:z) \in \mathbb{P}^1$,

$$R_Y(x,z) = 0 \Leftrightarrow \exists | y \text{ tal que } (x:y:z) \in F \cap G$$

(la unicidad de $y$ se debe a la segunda condición). Por tanto, bajo hipótesis de muy buen posicionamiento, $R_Y = k\prod_{i=1}^{r}(z_iX - x_iZ)^{m_i}$, donde $k \in \mathbb{K}$ es no nulo, los puntos $(x_i : y_i : z_i)$ son los puntos de $F \cap G$ y $\sum m_i = mn$. Definimos la **multiplicidad de**

**intersección de $F$ y $G$** en $P_i = (x_i : y_i : z_i)$ como $mult_{P_i}(F,G) = m_i$, y como 0 en los puntos que no están en la intersección.

Si tenemos dos curvas genéricas $F$ y $G$ definimos la multiplicidad a través de un cambio de coordenadas que las deje en muy buen posicionamiento, y si $F$ y $G$ tienen componentes en común, extendemos la definición diciendo que la multiplicidad de un punto es $\infty$ si pertenece a $H = mcd(F,G)$, o la multiplicidad de $F/H$ y $G/H$ (que no tienen componentes en común) en caso contrario.

En [Vai96], Cap.5 y 6, se demuestra que esta definición verifica los axiomas de multiplicidad (en particular es independiente del cambio de coordenadas para lograr la buena posición), y por tanto la resultante constituye una herramienta alternativa para el cálculo de multiplicidad de intersección. Además, la ventaja de utilizar esta definición es que obtenemos automáticamente la validez del Teorema de Bézout:

**Teorema 2.22** (Teorema de Bézout)**.** *Si $F$ y $G$ son dos curvas proyectivas planas de grados $m$ y $n$, respectivamente, sin componentes en común, entonces*

$$\sum_{P \in F \cap G} mult_P(F,G) = mn.$$

*Demostración.* Basta ver la descomposición de la resultante $R_Y(F,G)$ antes dada. □

### 2.3.2. Cálculo mediante anillos locales

Esta segunda aproximación puede encontrarse en [Ful71],Cap. 3 y 5, y hace uso de anillos locales. De manera más precisa, se define la **multiplicidad de intersección** de dos curvas proyectivas planas $F$ y $G$ en un punto $P = (a : b : 1)$ (de forma análoga en el resto de casos) como

$$mult_P(F,G) = dim_{\mathbb{K}} \mathcal{O}_{(a,b)}(\mathbb{A}^2)/(F_*, G_*)\mathcal{O}_{(a,b)}(\mathbb{A}^2).$$

De nuevo, se verifican los axiomas dados, y obtenemos propiedades interesantes como consecuencia de esta definición.

**Proposición 2.23.** *Sean $F$, $G$ curvas proyectivas sin componentes en común, $P = (a : b : 1) \in F \cap G$. Entonces,*

$$mult_P(F,G) = dim_{\mathbb{K}} \mathbb{K}[x,y]/\mathfrak{q},$$

*donde $\mathfrak{q}$ es la componente $(x-a, y-b)$-primaria del ideal $(F_*, G_*)$.*

*Demostración.* Consecuencia inmediata del Corolario 1.36. □

**Proposición 2.24.** *Si $P = (a : b : 1)$ es un punto simple de una curva proyectiva irreducible $F$, entonces $mult_P(F,G) = ord_P(G)$ en $\mathcal{O}_{a,b}(F_*)$.*

*Demostración.* Hemos definido $ord_P(G) := ord_{(a,b)}(\bar{G}_*)$, y por el Teorema 1.29, esto equivale a la dimensión de $\mathcal{O}_{(a,b)}(F_*)/(\bar{G}_*)\mathcal{O}_{(a,b)}(F_*)$. Por la Proposición 1.24, este espacio es isomorfo a $\mathcal{O}_{(a,b)}(\mathbb{A}^2)/(F_*, G_*)\mathcal{O}_{(a,b)}(\mathbb{A}^2)$, luego se tiene el resultado. □

En particular, el Teorema 1.29 nos muestra diferentes maneras de calcular la multiplicidad de intersección para puntos que son simples sobre una de las curvas.

**Proposición 2.25.** *Si $F$ y $G$ son curvas proyectivas planas sin componentes en común, entonces*

$$\sum_{P \in F \cap G} mult_P(F,G) = dim_{\mathbb{K}} \mathbb{K}[x,y]/(F_*, G_*).$$

*Demostración.* Como $F$ y $G$ no tienen componentes en común su intersección es finita. Podemos suponer, sin pérdida de generalidad, que todos los puntos de $F \cap G$ son de la forma $P_i = (a_i : b_i : 1)$, es decir, que no hay puntos de intersección sobre la recta del infinito $z = 0$ (siempre es posible escoger una recta que no pase por ninguno de los puntos de intersección, luego podríamos tomar esa como recta del infinito). De esta forma $F_* \cap G_* = \{P_{*,i} = (a_i, b_i)\}_i$ y el Teorema 1.35 nos proporciona un isomorfismo

$$\mathbb{K}[x,y]/(F_*, G_*) \cong \prod_{P \in F \cap G} \mathcal{O}_{P_*}(\mathbb{A}^2)/(F_*, G_*)\mathcal{O}_{P_*}(\mathbb{A}^2).$$

Así, $dim_{\mathbb{K}} \mathbb{K}[x,y]/(F,G) = \sum_{P \in F \cap G} dim_{\mathbb{K}} \mathcal{O}_{P_*}(\mathbb{A}^2)/(F,G)\mathcal{O}_{P_*}(\mathbb{A}^2)$ siendo los sumandos del segundo miembro, por definición, $mult_P(F,G)$. □

## 2.4. Existencia de modelos birracionales no singulares

Como ha sido comentado, a través del Teorema de Riemann se introduce la noción del género de una "curva arbitraria no singular". Este concepto resulta depender únicamente del cuerpo de funciones de la curva, y por tanto se puede extender a curvas singulares que sean birracionalmente isomorfas a una curva no singular.

En esta sección debatiremos la existencia de modelos no singulares de curvas, es decir, de curvas no necesariamente planas birracionalmente equivalentes a una curva plana dada y en que las singularidades ya han sido "resueltas". En resumidas cuentas, toda curva proyectiva es birracionalmente isomorfa a otra no singular, lo que nos permite definir el género de una curva irreducible. No obstante, no será necesario hallar explícitamente un modelo no singular para hallar el género, sino que bastará con encontrar curvas birracionalmente equivalentes a la curva de interés y en que todas las singularidades sean ordinarias, cuestión que puede resolverse sin salir del plano proyectivo.

Obsérvese que hasta el momento sólo hemos introducido el concepto de curva plana, luego en primer lugar debemos especificar qué se entiende por una curva arbitraria, y luego definir la multiplicidad de un punto.

Si $V$ es una variedad, entonces su cuerpo de funciones $\mathbb{K}(V)$ es una extensión finitamente generada de $\mathbb{K}$, y por tanto, se puede hablar de su grado de trascendencia sobre $\mathbb{K}$. Decimos que una variedad $V$ no vacía es una **curva** si $\mathbb{K}(V)$ tiene grado de trascendencia uno sobre $\mathbb{K}$.

Sobre $\mathbb{A}^2$ (y $\mathbb{P}^2$), esta definición coincide con la de curva plana irreducible (ver [Ful71], Cap 6, § 5). En particular para toda curva plana irreducible $\mathcal{C}$ se tiene que $\mathbb{K}(\mathcal{C})$ es una extensión algebraica de (un cuerpo isomorfo a) $\mathbb{K}(x)$ (ver [Ful71], Cap. 6, Proposición 9).

La noción general de multiplicidad es la siguiente: se dice que un punto $P$ en una curva $\mathcal{C}$ es **simple** si $\mathcal{O}_P(\mathcal{C})$ es un anillo de valoración discreta, definición que coincide con las que hemos visto para curvas planas en virtud del Teorema 2.11. Así, una **curva no singular** es una curva cuyos puntos son todos simples.

Llamamos **modelo no singular** de una curva plana $\mathcal{C}$ a toda curva no singular $X$ (no necesariamente plana) birracionalmente equivalente a $\mathcal{C}$. La demostración de la existencia de modelos no singulares de curvas proyectivas que se presenta en [Ful71] consta de tres etapas:

(1) Toda curva proyectiva es birracionalmente equivalente a una curva proyectiva plana irreducible.

(2) Toda curva proyectiva plana irreducible es birracionalmente equivalente a una curva proyectiva plana irreducible cuyas singularidades son puntos ordinarios.

(3) Toda curva proyectiva plana irreducible cuyas singularidades son puntos ordinarios es birracionalmente equivalente a una curva proyectiva no singular.

Además, si $\varphi : X \to \mathcal{C}$ es el isomorfismo birracional y $\varphi^{-1}(P) = \{Q_1, \ldots, Q_n\}$, el cálculo de multiplicidades de intersección con $\mathcal{C}$ en $P$ está intimamente relacionado con el cálculo de órdenes en los anillos $\mathcal{O}_{Q_i}$. De manera más precisa, para toda curva plana $\mathcal{C}'$ definida por $G$,

$$mult_P(\mathcal{C}, G) = \sum_{i=1}^{n} ord_{Q_i}(G). \tag{2.1}$$

Dado que en la práctica trabajaremos únicamente con curvas planas y que, como adelantábamos, el cálculo del género puede hacerse de manera sencilla sobre curvas cuyas singularidades son ordinarias, dedicaremos el resto de la sección al segundo de los puntos expuestos.

Para obtener una curva ordinaria a partir de otra con singularidades no ordinarias se hará uso de transformaciones cuadráticas del plano proyectivo. A este procedimiento por el cual eliminamos una singularidad no ordinaria se le conoce como explosión de la singularidad.

**Definición 2.26.** *Llamamos* ***transformación estándar de Cremona*** *a la transformación $\mathcal{Q}$ de $\mathbb{P}^2$ dada por $(x : y : z) \mapsto (yz : xz : xy)$. Llamamos* ***transformación cuadrática*** *a la composición de $\mathcal{Q}$ con un cambio de coordenadas proyectivo.*

Observemos que $\mathcal{Q}$ no está definida en los puntos $(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)$, que denominaremos **puntos fundamentales**. Por otro lado, los puntos de $V(xyz)$, es decir, los puntos de las rectas $x = 0$, $y = 0$ y $z = 0$, que llamaremos **rectas excepcionales**, van a parar a los puntos $(1 : 0 : 0), (0 : 1 : 0)$ y $(0 : 0 : 1)$, respectivamente. Además, si $(a, b, c) \notin V(xyz)$, entonces

$$\mathcal{Q}(\mathcal{Q}(a : b : c)) = (acab : bcab : bcac) = (a : b : c),$$

es decir, $\mathcal{Q} = \mathcal{Q}^{-1}$ sobre el abierto $\mathbb{P}^2 - V(xyz)$, y por tanto $\mathcal{Q}$ es un isomorfismo birracional de $\mathbb{P}^2$ en sí mismo.

**Definición 2.27.** *Sea $F$ una curva proyectiva. Entonces,*

$$G(x, y, z) := F(yz, xz, xy)$$

*se denomina* ***transformado algebraico de*** *$F$. Eliminando en $G$ los factores que son potencias de $x$, $y$ y $z$, obtenemos un polinomio homogéneo $F'$ que se denomina* ***transformado cuadrático*** *de $F$.*

Se enumeran y comentan a continuación algunas de las propiedades de los transformados cuadráticos (ver [Ful71], Cap.7, § 4 para los detalles). Llamemos intersecciones no fundamentales a las intersecciones distintas de los puntos fundamentales de una curva con una recta excepcional.Sea $F$ una curva irreducible de grado $d$. Supongamos que $P_1 = (1:0:0)$, $P_2 = (0:1:0)$, $P_3 = (0:0:1)$ son puntos de multiplicidad $r_1, r_2, r_3$ y que las rectas excepcionales no son tangentes a ninguno de ellos. Si $F'$ es el transformado cuadrático de $F$, entonces:

*1.* Si $F$ es irreducible, $F'$ también (como consecuencia de que $\mathcal{Q}$ sea su propia inversa).

*2.* $F' = F(yz, xz, xy)/x^{r_1}y^{r_2}z^{r_3}$.

$\diamond$ Por definición, debemos ver que $z^{r_3}$ es la mayor potencia de $z$ que divide a $F(yz, xz, xy)$ (análogo para $x$, $y$). En efecto, recordemos que $m_{P_3}(F) = m_{(0,0)}(F_*)$. Así, si $r_3 = m_{(0,0)}(F_*)$, $F_* = F_{r_3} + \cdots + F_d$, con $F_i \in \mathbb{K}[x,y]$ homogéneo de grado $i$. Como $F$ es irreducible, $F = (F_*)^* = F_{r_3}z^{d-r_3} + \cdots + F_{d-1}z + F_d$, de donde

$$\begin{aligned} F(yz, xz, xy) &= z^{r_3}F_{r_3}(y,x)(xy)^{d-r_3} + \cdots + z^{d-1}F_{d-1}(y,x)xy + F_d(y,x) \\ &= z^{r_3}(F_{r_3}(y,x) + \dots). \end{aligned}$$

*3.* Existe una correspondencia uno a uno entre tangentes a $F$ en $P_1$ (resp. $P_2$, $P_3$) e intersecciones no fundamentales de $F'$ con $x = 0$ (resp. $y = 0, z = 0$) que preserva multiplicidades (donde entendemos en el primer caso multiplicidad de la tangente y en el segundo multiplicidad de intersección).

$\diamond$ Aprovechando la expresión anterior,

$$\begin{aligned} F' = {} & x^{d-r_3-r_1}y^{d-r_3-r_2}F_{r_3}(y,x) + \cdots + z^{d-r_3-1}x^{1-r_1}y^{1-r_2}F_{d-1}(y,x) \\ & + z^{d-r_3}x^{-r_1}y^{-r_2}F_d(y,x). \end{aligned}$$

Veamos el resultado para $P_3$. La intersecciones de $F'$ con $z = 0$ vienen dadas por las raíces de $F'(x,y,0) = x^{d-r_1-r_3}y^{d-r_2-r_3}F_{r_3}(y,x)$. Por tanto, las intersecciones no fundamentales y sus multiplicidades de intersección vienen dadas por los factores en que se descompone $F_{r_3}$, que son las tangentes a $F$ en $P_3$, y sus multiplicidades.

*4.* Los puntos de $F$ que no estén sobre las rectas excepcionales se transforman en puntos de $F'$ preservando su multiplicidad y la de sus tangentes. Esto es consecuencia de que la transformación estándar de Cremona constituya un isomorfismo de $\mathbb{P}^2 - V(xyz)$ (puntos fuera de las rectas excepcionales) en sí mismo, y que las multiplicidades de puntos y tangentes se preserven por isomorfismos.

*5.* $F'$ tiene multiplicidad $d - r_2 - r_3$ en $P_1$ (análogo para $P_2, P_3$), y sus tangentes, que corresponden a las intersecciones no fundamentales de $F$ con $x = 0$ (resp. $y = 0$, $z = 0$), son distintas de las rectas excepcionales.

$\diamond$ Estudiémoslo brevemente en $P_3$. La multiplicidad de $F'$ en $P_3$ viene dada por $m_{(0,0)}(F'_*)$. Con la expresión anterior de $F'$,

$$\begin{aligned} F'_* = {} & x^{d-r_3-r_1}y^{d-r_3-r_2}F_{r_3}(y,x) + \cdots + x^{1-r_1}y^{1-r_2}F_{d-1}(y,x) \\ & + x^{-r_1}y^{-r_2}F_d(y,x), \end{aligned}$$

luego el polinomio homogéneo de menor grado es $x^{-r_1}y^{-r_2}F_d(y,x)$, de grado $d-r_1-r_2$, como queríamos ver. Además, ni $x$ ni $y$ dividen a $x^{-r_1}y^{-r_2}F_d(y,x)$ pues en caso contrario dividirían a $F'$, lo cual no es posible por definición. Por tanto, las tangentes a $P_3$ son distintas de las rectas excepcionales. Por su parte, las intersecciones no fundamentales de $F$ con la recta $z = 0$ surgen de descomponer precisamente $F(x,y,0) = F_d(x,y)$.

En función de estos resultados, tenemos el siguiente método, tal y como se expone en [SWPD08], Chapter 3, § 2, para resolver las singularidades no ordinarias de $F$:

- Mediante un cambio de coordenadas movemos una de las singularidades no ordinarias a $(0:0:1)$ de manera que ninguna de las tangentes sea una recta excepcional, y que no haya más puntos singulares sobre una recta excepcional.
- Obtener la transformada cuadrática $F'$ de $F$.

  Por *4.*, fuera de las rectas excepcionales se mantienen multiplicidades de puntos y tangentes.

  Por *5.*, se podrían crear nuevas singularidades en los puntos fundamentales; no obstante, al asegurar en *1.* que los puntos (no fundamentales) sobre las rectas excepcionales son simples se puede comprobar que las tangentes a dichos puntos también son simples, esto es, son ordinarios. Como $(1:0:0)$ y $(0:1:0)$ son simples en $F$, en virtud de (2) $F'$ no tiene puntos múltiples en las rectas $x=0$ e $y=0$, pero podría tener singularidades, incluso no ordinarias, en la recta $z=0$.
- Aplicar *1.* y *2.* hasta que no haya singularidades no ordinarias. En [Ful71], Cap. 7, § 4 se demuestra que, si denotamos

$$g^*(F) = \frac{(deg(F)-1)(deg(F)-2)}{2} - \sum_{P\in F} \frac{m_P(F)(m_P(F)-1)}{2},$$

  que es un entero no negativo, entonces tras cada iteración o bien se elimina una singularidad no ordinaria, o bien $g^*(F') < g^*(F)$, de manera que el procedimiento es finito.

## 2.5. El Teorema de Riemann

Ya estamos en condiciones de comenzar a trabajar en la dirección del Teorema de Riemann. El primer paso consiste en desarrollar la teoría de divisores de una curva proyectiva no singular.

Sea $X$ una curva proyectiva no singular (irreducible).

**Definición 2.28.** *Un **divisor de** $X$ es una suma formal*

$$D = \sum_{P\in X} r_P P, r_P \in \mathbb{Z},$$

*donde todos los $r_P$ son nulos salvo un número finito. El **grado** de $D$ se define como $deg(D) = \sum_{P\in X} r_P$, y es claramente aditivo (el grado de una suma de divisores es la suma de los grados). Se dice que $D$ es **efectivo** o positivo cuando todos los $r_P$ son no negativos, y se denota $D \succ 0$. Escribimos $D \succ D'$ si $D - D' \succ 0$.*

Sea $\mathcal{C}$ una curva plana irreducible con modelo no singular $X$, y sea $\mathbb{K}(C) \cong \mathbb{K}(X)$ su cuerpo de funciones.

**Definición 2.29.** *Si $G$ es una curva plana que no contiene a $\mathcal{C}$, llamamos **divisor de** $G$ a*

$$div(G) = \sum_{P\in X} ord_P(G)P,$$

*que es un divisor de grado $deg(\mathcal{C})deg(G)$, pues sumando la ecuación 2.1 para todo punto de $\mathcal{C}$ y aplicando el Teorema de Bézout,*

$$deg(div(G)) = \sum_{P \in X} ord_P(G) = \sum_{Q \in \mathcal{C}} mult_Q(\mathcal{C}, G) = deg(\mathcal{C})deg(G).$$

Esta definición se puede extender a todo elemento no nulo $\varphi \in \mathbb{K}(\mathcal{C})$. Para ello, debemos tener en cuenta que $\varphi$ sólo tiene un número finito de ceros y polos: En efecto, si $\varphi = \bar{G}/\bar{H}$, con $G$, $H$ formas de mismo grado, entonces $\mathcal{C}$ no es componente de $G$ (pues $\varphi$ es no nulo) ni de $H$ (pues $H \notin I(\mathcal{C})$). Ahora, es suficiente observar que los ceros y polos de $\varphi$ forman un subconjunto de $\mathcal{C} \cap G$ y $\mathcal{C} \cap H$, respectivamente, y que éstos son finitos. De esta manera, tiene sentido la siguiente definición:

**Definición 2.30.** *Sea $\varphi \in \mathbb{K}(\mathcal{C})$ no nulo. Llamamos **divisor de** $\varphi$ a*

$$div(\varphi) = \sum_{P \in X} ord_P(\varphi)P.$$

*El divisor de $\varphi$ puede desglosarse en dos partes: el **divisor de los ceros** y el **divisor de los polos**, que son, respectivamente,*

$$(\varphi)_0 = \sum_{\substack{P \in X: \\ ord_P(\varphi) > 0}} ord_P(\varphi)P, (\varphi)_\infty = \sum_{\substack{P \in X: \\ ord_P(\varphi) < 0}} -ord_P(\varphi)P.$$

Por la Proposición 1.26 de la función de orden, $div(\varphi\varphi') = div(\varphi) + div(\varphi')$ y $div(\varphi^{-1}) = -div(\varphi)$. De esta manera,

**Proposición 2.31.** *El divisor de todo $\varphi \in \mathbb{K}(\mathcal{C})$ no nulo tiene grado cero. Esto quiere decir que, contados con sus órdenes, una función racional tiene tantos ceros como polos. Además, el divisor es cero si y sólo si $\varphi \in \mathbb{K}$.*

*Demostración.* Si $\varphi = \bar{G}/\bar{H}$, con $G, H$ formas de mismo grado, entonces, por todo lo comentado

$$deg(div(\varphi)) = deg(div(G)) - deg(div(H)) = deg(G)deg(\mathcal{C}) - deg(H)deg(\mathcal{C}) = 0.$$

La segunda parte es clara: si el divisor es cero, entonces $\varphi$ no tiene ceros ni polos. Si $\varphi$ fuera no constante y tomásemos cualquier $P \in X$, entonces $\varphi - \varphi(P)$ es una función no nula con un cero en $P$ y sin polos, lo que es imposible. □

**Corolario 2.32.** *El divisor de una función racional no nula la caracteriza salvo producto por constantes.*

*Demostración.* Atendiendo a la Proposición 2.31,

$$div(\varphi) = div(\varphi') \Leftrightarrow div(\varphi\varphi'^{-1}) = 0 \Leftrightarrow \varphi\varphi'^{-1} \in \mathbb{K} \Leftrightarrow \varphi = \lambda\varphi'.$$

□

**Definición 2.33.** *Decimos que dos divisores $D$ y $D'$ son **linealmente equivalentes** y escribimos $D \equiv D'$ si difieren en el divisor de una función racional, esto es, si existe $\varphi \in \mathbb{K}(\mathcal{C})$ no nula con $D' = D + div(\varphi)$.*

Claramente, $\equiv$ es relación de equivalencia, y si $D \equiv D'$, entonces $deg(D) = deg(D')$ por la Proposición 2.31.

A todo divisor $D = \sum r_P P$ le vamos a asociar un espacio vectorial $L(D)$ formado por las funciones racionales cuyo orden en los puntos $P \in X$ es al menos $-r_P$. Esto obliga a que la función sólo pueda tener polos en los puntos $P$ con $r_P$ positivo y de orden a lo sumo $-r_P$, y a que tenga ceros de orden $-r_P$ o superior en los puntos $P$ con $r_P$ negativo. Formalmente,

$$\begin{aligned} L(D) &= \{\varphi \in \mathbb{K}(\mathcal{C})/ord_P(\varphi) \geq -r_P, P \in X\} \\ &= \{\varphi \in \mathbb{K}(\mathcal{C})/div(\varphi) + D \succ 0 \text{ ó } \varphi = 0\}. \end{aligned}$$

He aquí algunas propiedades de los espacios $L(D)$, donde $l(D)$ denota a su dimensión como $\mathbb{K}$-espacio vectorial.

**Proposición 2.34.**

1. *Si $D \prec D'$, entonces $L(D) \subset L(D')$ y $dim_{\mathbb{K}}(L(D')/L(D)) \leq deg(D' - D)$.*
2. *$L(D)$ es de dimensión finita. Más aún:*
   - *Si $deg(D) < 0$, entonces $L(D) = 0$.*
   - *Si $deg(D) \geq 0$, entonces $l(D) \leq deg(D) + 1$. En particular, $L(0) = \mathbb{K}$.*
3. *Si $D \prec D'$, entonces $deg(D) - l(D) \leq deg(D') - l(D')$.*
4. *Si $D \equiv D'$, entonces $l(D) = l(D')$.*

*Demostración.*

*1.* Si $D = \sum r_P P$ y $D \prec D'$, entonces existen $P_1, \ldots, P_r$ tal que $D' = D + P_1 + \cdots + P_r$. La demostración será por inducción sobre $r$. Veamos el caso $r = 1$: Sea $\mathfrak{m}$ el maximal de $\mathcal{O}_P(X)$, $t$ parámetro de uniformización, y consideremos

$$\begin{array}{rccc} f: & L(D+P) & \to & \mathbb{K} \\ & \varphi & \mapsto & (t^{r_P+1}\varphi)(P). \end{array}$$

Si $\varphi \in L(D+P)$, entonces $ord_P(\varphi) \succ -r_P - 1$, luego $t^{r_P+1}\varphi$ está definida en $P$ y tiene sentido considerar $f$, que es claramente una aplicación lineal. Su núcleo es $L(D)$, pues si $(t^{r_P+1}\varphi)(P) = 0$, entonces $t^{r_P+1}\varphi \in \mathfrak{m} = (t)$, de donde $\varphi = ut^{-r}$ para cierto $u \in \mathcal{O}_{\mathcal{P}}$, y en definitiva $ord_P(\varphi) \geq -r$. El Primer Teorema de Isomorfía nos dice que $L(D+P)/L(D) \cong im(f)$, luego en particular tiene dimensión $\leq 1 = deg(D+P-D)$.

Para el caso general basta tener en cuenta que por el Tercer Teorema de Isomorfía

$$\frac{L(D+P_1+\cdots+P_r)/L(D)}{L(D+P_1+\cdots+P_{r-1})/L(D)} \cong L(D+P_1+\cdots+P_r)/L(D+P_1+\cdots+P_{r-1}),$$

y que por el paso inductivo $L(D+P_1+\cdots+P_{r-1})/L(D)$ tiene dimensión $\leq r-1$ y el miembro derecho tiene dimensión $\leq 1$. De esta manera, $L(D+P_1+\cdots+P_r)/L(D)$ tiene dimensión finita y $\leq r$, como queríamos ver.

*2.* El primer punto es claro, pues para que $D + \varphi \succ 0$, esto es, para que haya un elemento no nulo en $L(D)$, debe ocurrir que

$$0 \leq deg(D) + deg(\varphi) = deg(D).$$

Por su parte, si $deg(D) \geq 0$, tomemos un divisor efectivo $D'$ con $deg(D') = deg(D)+1$. Entonces por lo anterior $L(D - D') = 0$, y por *1.*,

$$dim_{\mathbb{K}} L(D) = dim_{\mathbb{K}} L(D)/L(D - D') \leq deg(D') = deg(D) + 1.$$

*3.* Ahora que sabemos que los $L(D)$ tienen dimensión finita, el resultado se sigue directamente de *1.*

*4.* Supongamos que $D = D' + div(\varphi)$ para cierto $\varphi \in \mathbb{K}(\mathcal{C})$ no nulo, y consideremos

$$\begin{array}{rccc} f: & L(D) & \to & L(D') \\ & \psi & \mapsto & \psi\varphi. \end{array}$$

$f$ está bien definida, pues si $\psi \in L(D)$ es no nulo, entonces

$$D' + div(\psi\varphi) = D' + div(\varphi) + div(\psi) = D + div(\psi) \succ 0$$

y es un isomorfismo con inversa $g : L(D') \to L(D)$ definida por $\eta \mapsto \eta\varphi^{-1}$.

□

Para demostrar el Teorema de Riemann necesitaremos los siguientes resultados:

**Lema 2.35.** *Sea $R$ un dominio con cuerpo de fracciones $\mathbb{L}$ y $\mathbb{F}$ una extensión algebraica finita de $\mathbb{L}$. Para todo $v \in \mathbb{F}$ existe un $b \in R$ no nulo tal que $bv$ es entero sobre $R$.*

*Demostración.* Como $v$ es algebraico sobre $\mathbb{L}$, existe $f \in \mathbb{L}[x]$, que podemos suponer de la forma $f = x^n + a_{n-1}x^{n-1} + \cdots + a_0, a_i = \frac{b_i}{b}, b_i, b \in R$, de manera que $f(v) = 0$. Multiplicando por $b^n$,

$$b^n v^n + b^{n-1}b_{n-1}v^{n-1} + b^{n-1}b_{n-2}v^{n-2} + \cdots + b^{n-1}b_0 = 0,$$

luego $g(x) = x^n + b_{n-1}x^{n-1} + bb_{n-2}x^{n-2} + \cdots + b^{n-1}b_0$ es un polinomio mónico en $R[x]$ que se anula en $bv$, es decir, $bv$ es entero. □

**Lema 2.36.** *Sean $P_1, \ldots, P_r \in X$, $m_1, \ldots, m_r \in \mathbb{Z}$. Entonces, existe un $\varphi \in \mathbb{K}(X)$ tal que $ord_{P_i}(\varphi) = m_i$*

*Demostración.* Pongamos que $X$ es el modelo no singular de una curva plana irreducible $\mathcal{C}$ y sea $f : X \to \mathcal{C}$ el isomorfismo birracional. Podemos suponer que $\mathcal{C}$ sólo tiene puntos ordinarios aplicando el método de la sección anterior, y también que los $f(P_i)$ son puntos simples: si no fuera así, aplicamos de nuevo el método de la sección anterior sobre cada $f(P_i)$, de manera que cada uno de ellos pase a "identificarse" con puntos simples (uno por tangente). Para toda curva plana $G$, la ecuación 2.1 se lee, en virtud de la Proposición 2.24 para cada $f(P_i)$ como

$$ord_{f(P_i)}(G) = ord_{P_i}(G).$$

Cojamos ahora, para cada $i$, una recta $L_i$ que pase por $f(P_i)$ pero no por $f(P_j)$, $j \neq i$, y que no sea la tangente a $\mathcal{C}$ en $f(P_i)$. Esto quiere decir que $\bar{L}_i$ es una unidad en cada $\mathcal{O}_{f(P_j)}$, $j \neq i$, y un parámetro de uniformización en $\mathcal{O}_{f(P_i)}$ en virtud del Teorema 2.11. Tomemos una recta adicional $L$ que no pase por ningún $P_i$. Entonces, la $\varphi$ que buscamos es

$$\varphi = \frac{\prod_{i=1}^{r} \bar{L}_i^{m_i}}{\bar{L}^{\sum m_i}}.$$

□

Sea $S$ un subconjunto de $X$, $D = \sum r_P P$ un divisor de $X$. Denotaremos $gr^S(D) = \sum_{P\in S} r_P$ y $L^S(D) = \{\varphi \in \mathbb{K}(\mathcal{C})/ord_P(\varphi) \geq -r_P, \text{ si } P \in S\}$.

**Lema 2.37.** *Si $D \prec D'$, entonces $L^S(D) \subset L^S(D')$, y si $S$ es finito,*

$$dim_{\mathbb{K}}(L^S(D')/L^S(D)) = gr^S(D' - D).$$

*Demostración.* El procedimiento es el mismo que el visto en la demostración de *1.* de la Proposición 2.34, sólo que ahora hay que demostrar la igualdad en el primer paso, esto es, hay que probar que

$$\begin{array}{rccc} f: & L^S(D+P) & \to & \mathbb{K} \\ & \varphi & \mapsto & (t^{r_P+1}\varphi)(P) \end{array}$$

es sobre. Para ello, basta dar un elemento no nulo en la imagen. Como $ker(f) = L^S(D)$, debemos demostrar que existe $\varphi \in L^S(D+P) - L^S(D)$, esto es, $\varphi$ con $ord_P(\varphi) = -r_P - 1$ y $ord_Q(\varphi) \geq -r_Q$ para todo $Q \in S$, lo cual es siempre posible por el Lema 2.36. □

**Proposición 2.38.** *Sea $x \in \mathbb{K}(X)$ no constante, y $n = [\mathbb{K}(X) : \mathbb{K}(x)]$. Entonces:*

1. *Existe una constante $\tau$ tal que $l(r(x)_0) \geq rn - \tau$ para todo $r$.*
2. *$deg((x)_0) = n$.*

*Demostración.*

*1.* Sean $D = (x)_0 = \sum r_P P$, $m = deg(D)$ y $S = \{P \in X/r_P > 0\}$. Como $[\mathbb{K}(X) : \mathbb{K}(x)] = n$ y según el Lema 2.35, podemos coger una base $v_1, \ldots, v_n$ de $\mathbb{K}(X)$ sobre $\mathbb{K}(x)$ de manera que $v_i$ satisface una ecuación de la forma

$$v_i^{n_i} + a_{i1}v_i^{n_i-1} + \cdots + a_{in_i} = 0, a_{ij} \in \mathbb{K}[x^{-1}].$$

Así, $ord_P(a_{ij}) \geq 0$ si $P \notin S$. Asimismo, $ord_P(v_i) \geq 0$ si $P \notin S$, pues si no se tendría que $ord_P(v_i^{n_i}) < ord_P(a_{ij}v_i^{n_i-j})$ lo que implicaría por la Proposición 1.26 que $v_i^{n_i} + a_{i1}v_i^{n_i-1} + \cdots + a_{in_i} \neq 0$. Por tanto, como los únicos puntos donde $ord_P(v_i)$ puede ser negativo están en $S$, se tiene que para $t$ suficientemente grande, $div(v_i) + tD \succ 0, i = 1, \ldots, n$. Esto es, $v_i \in L(tD)$. Observemos que entonces para todo $r$ y para todo $j \leq r$, $v_i x^{-j} \in L((r+t)D)$: en efecto, como $div(x) = D - (x)_\infty$,

$$div(v_i x^{-j}) + (t+r)D = (div(v_i) + tD) + (r-j)D + j(x)_\infty \geq 0.$$

Como los $v_i$ son independientes sobre $\mathbb{K}(x)$ y $1, x^{-1}, \ldots, x^{-r}$ lo son sobre $\mathbb{K}$, obtenemos que $\{v_i x^{-j}\}$ es un conjunto de $n(r+1)$ elementos independientes sobre $\mathbb{K}$, es decir, $l((r+t)D) \geq n(r+1)$. Empleando ahora la Proposición 2.34(3), $l((r+t)D) \leq l(rD) + tm$ y, en definitiva, $l(rD) \geq n(r+1) - tm = rn + (n - tm) = rn - \tau$ con $\tau = tm - n$ independiente de $r$, como queríamos.

*2.* Por un lado, en la notación del apartado anterior, y utilizando el segundo punto de la Proposición 2.34,

$$rn - \tau \leq l(rD) \leq rm + 1,$$

de donde si $r > 0$, $n \leq m + (1+\tau)/r$. Tomando $r$ suficientemente grande, $n \leq m$.

Para la otra desigualdad, atendiendo al Lema 2.37, $L^S(0)/L^S(-D)$ tiene dimensión $m$, y por tanto podemos tomar $w_1, \ldots, w_m \in L^S(0)$ tal que $\{\bar{w}_i\}$ forma base del

cociente. Afirmamos que los $w_i$ son independientes sobre $\mathbb{K}(x)$. De lo contrario, limpiando denominadores si hace falta, existen $g_1, \ldots, g_m \in \mathbb{K}[x]$ tales que $\sum g_i w_i = 0$. Podemos escribir $g_i = \lambda_i + xh_i$ y suponer que no todos los $\lambda_i$ son nulos (pues si no sacamos la potencia de $x$ correspondiente de la relación y sigue siendo válida). Así, $\sum \lambda_i w_i$ es un elemento de $L^S(-D)$, pues

$$ord_P(\sum \lambda_i w_i) = ord_P(-x \sum h_i v_i) \geq ord_P(x), \text{si } P \in S.$$

Pero entonces $\sum \lambda_i \bar{w}_i = 0$, lo que es absurdo. En definitiva $m \leq n$ y se tiene el resultado. □

Es importante observar que la constante obtenida $\tau = tm - n = n(t-1)$ sólo depende del cuerpo de funciones de la curva.

**Teorema 2.39** (Teorema de Riemann)**.** *Existe una constante $g$ tal que, para todos los divisores $D$ de $X$, $l(D) \geq deg(D) + 1 - g$. La menor de esas constantes se denomina* ***género*** *de $X$.*

*Demostración.* Consideremos $S(D) = deg(D)+1-l(D)$. Buscamos $g$ tal que $S(D) \leq g$ para todo $D$. Por la Proposición 2.34(2.), $S(0) = 0$ ( luego necesariamente $g \geq 0$) y si $D \equiv D'$ entonces $S(D) = S(D')$. Además, de la Proposición 2.34(3.) se tiene que si $D \prec D'$, entonces $S(D) \leq S(D')$.

Sea $x \in \mathbb{K}(X)$ no constante, y $\tau$ el entero de la Proposición 2.38(1) más pequeño. Se tiene entonces que para todo $r$, $S(r(x)_0) = deg(r(x)_0) + 1 - l(r(x)_0) \leq \tau + 1$ luego, como $r(x)_0 \prec (r+1)(x)_0$, deducimos de lo anteriormente dicho que $S(r(x)_0) = \tau + 1$ para todo $r > 0$ suficientemente grande.

Tomemos $g = \tau + 1$. Vamos a probar que, para todo divisor $D = \sum r_P P$, existe un divisor $D'$ y un entero $r \geq 0$ tal que $D' \equiv D$ y $D' \prec r(x)_0$, de donde se tendrá el resultado. En efecto, pongamos $(x)_0 = s_P P$. Queremos encontrar $\varphi$ tal que $D' = D - div(\varphi)$ y $r_P - ord_P(\varphi) \leq rs_P$ para todo $P$. Sea $y = x^{-1}$, $T = \{P \in X / r_P > 0 \wedge ord_P(y) \geq 0\}$, y consideremos $\varphi = \prod_{P \in T} (y - y(P))^{r_P}$. Entonces, si $ord_P(y) \geq 0$, entonces $P$ es cero de $\varphi$ de orden al menos $r_P$, y por tanto $r_P - ord_P(\varphi) \leq 0$. Por otro lado, i $ord_P(y) < 0$, entonces $s_P = ord_P(x) > 0$. Por tanto, un $r$ suficientemente grande hará que se satisfaga la condición deseada. □

Como $\tau$ sólo depende del cuerpo de funciones, el género también y por tanto es un invariante birracional. De esta manera, definimos el género de una curva $\mathcal{C}$ cualquiera como el género de un modelo no singular $X$ de $\mathcal{C}$.

**Corolario 2.40.** *Si $l(D_0) = deg(D_0) + 1 - g$ y $D \equiv D' \succ D_0$, entonces $l(D) = deg(D) + 1 - g$.*

*Demostración.* En la notación de la demostración anterior, $S(D) = S(D')$ y $S(D') \geq S(D_0)$. Por tanto, $deg(D)+1-l(D) \geq deg(D_0)+1-l(D_0) = g$. Como por el Teorema de Riemann se tiene la desigualdad contraria, hemos terminado. □

**Corolario 2.41.** *Si $x \in \mathbb{K}(X)$ es no constante, entonces para $r$ suficientemente grande*

$$g = gr(r(x)_0) - l(r(x)_0) + 1.$$

*Demostración.* Como en la demostración del Teorema de Riemann, para $r$ suficientemente grande, $S(r(x)_0) \geq \tau + 1 = g$. □

**Corolario 2.42.** *Existe $N$ tal que, para todo divisor $D$ con $deg(D) > N$, $l(D) = deg(D) + 1 - g$.*

*Demostración.* Por el corolario anterior, podemos tomar $D_0$ tal que $l(D_0) = deg(D_0) + 1 - g$. Sea $N = deg(D_0) + g$. Entonces, si $D$ tiene $deg(D) \geq N$, $deg(D - D_0) + 1 - g \geq N - deg(D_0) + 1 - g = 1$ y, por el Teorema de Riemann, $l(D - D_0) > 0$. De esta manera, existe un $\varphi \in L(D - D_0)$ no nulo, es decir, tal que $D - D_0 + div(\varphi) \succ 0$. Por tanto, $D \equiv D + div(\varphi) \succ D_0$, y se aplica el primer corolario. □

Aunque no es nuestro objetivo, cabe mencionar que la diferencia entre $l(D)$ y $deg(D) + 1 - g$ en el Teorema de Riemann es cuantificable a través de una clase especial de divisores denominados divisores canónicos, y que se definen a través de la noción de diferencial de una curva. Si $W$ es cualquiera de tales divisores canónicos, entonces lo que resta para la igualdad es el término $l(W - D)$. El teorema que establece este resultado se denomina Teorema de Riemann-Roch.

# Capítulo 3

# Cálculo simbólico y ejemplos

En los capítulos anteriores hemos tratado los aspectos teóricos necesarios para alcanzar la definición de género. Tal y como fue comentado en la introducción, en la práctica debemos buscar una alternativa que nos permita extraer la información deseada de una curva plana proyectiva de manera simbólica (no podemos trabajar en $\mathbb{C}$).

En este capítulo trabajaremos con curvas definidas por polinomios con coeficientes racionales, y afrontaremos la problemática anterior mediante el estudio conjunto de puntos "conjugados" y/o recurriendo a extensiones algebraicas de $\mathbb{Q}$. Relacionar el comportamiento en $\mathbb{C}$ y en $\mathbb{Q}$ conllevará en muchas ocasiones la utilización de propiedades de contracción y extensión de ideales, para las que nos referiremos salvo especificación particular a [AM69].

Expondremos en primer lugar la teoría que justifica la implementación realizada y posteriormente estudiaremos algunos ejemplos concretos para ilustrar la manera en que funciona. Dado que no se dispone de herramientas adecuadas para factorizar sobre extensiones de $\mathbb{Q}$, jugará un rol muy importante la descomposición primaria.

Para evitar confusiones en el cuerpo considerado en cada caso, denotaremos por $I^e$ a la extensión de un ideal $I$ de $\mathbb{Q}[x,y]$ a $\mathbb{C}[x,y]$, y por $J^c$ a la contracción de un ideal $J$ de $\mathbb{C}[x,y]$ a $\mathbb{Q}[x,y]$.

## 3.1. Estudio simbólico de curvas planas

A tenor del Nullstellensatz sabemos que todo punto de $\mathbb{C}^2$ queda completamente determinado a través de un ideal maximal de $\mathbb{C}[x,y]$. Más concretamente, a un punto $(a,b)$ le corresponde un ideal maximal $(x-a, y-b)$ y todos los maximales de $\mathbb{C}[x,y]$ son de esta forma. En la práctica no podemos trabajar directamente con ideales sobre $\mathbb{C}[x,y]$, y lo que haremos será definir puntos a través de ideales maximales en $\mathbb{Q}[x,y]$, que como veremos a continuación están asociados a un conjunto de puntos conjugados que comparten el mismo comportamiento como elementos de una curva. Explotaremos este hecho y, en nuestro algoritmo, identificaremos un punto algebraico $(a,b) \in \mathbb{C}^2$ junto con todos sus conjugados por el ideal que los define en $\mathbb{Q}[x,y]$.

A fin de estudiar la forma de los ideales en $\mathbb{Q}[x_1,\ldots,x_n]$ necesitaremos recordar el Lema de Zariski ([AM69], Cap. 7, Proposición 9):

**Teorema 3.1** (Lema de Zariski). *Sea $\mathbb{K}$ un cuerpo y $A$ una $\mathbb{K}$-álgebra finitamente*

*generada, es decir, $A = \mathbb{K}[a_1, \ldots, a_n]$. Si $A$ es un cuerpo, entonces $A$ es una extensión algebraica de $\mathbb{K}$.*

**Teorema 3.2.** *Un ideal $I \subseteq \mathbb{Q}[x_1, \ldots, x_n]$ es maximal si y sólo si*

$$I = (f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots, x_n)),$$

*donde $f_1(x_1)$ es irreducible sobre $\mathbb{Q}[x_1]$ con una raíz compleja $\alpha_1$ y, si hemos definido de manera recursiva $\alpha_1, \ldots, \alpha_{j-1}$, tenemos que $f_j(\alpha_1, \ldots, \alpha_{j-1}, x_j)$ es irreducible sobre $\mathbb{Q}(\alpha_1, \ldots, \alpha_{j-1})[x_j]$ y $\alpha_j$ es una raíz de $f_j(\alpha_1, \ldots, \alpha_{j-1}, x_j)$.*

*Demostración.* Lo demostraremos por inducción, siendo el caso $n = 1$ conocido.

Para probar la suficiencia, por inducción tenemos que

$$\mathbb{L} = \mathbb{Q}[\overline{x_1}, \ldots, \overline{x_{n-1}}] = \mathbb{Q}[x_1, \ldots, x_{n-1}]/(f_1, \ldots, f_{n-1})$$

es un cuerpo. Ahora $f_n(\overline{x_1}, \ldots, \overline{x_{n-1}}, x_n)$ es irreducible en $\mathbb{L}[x_n]$, por lo que $\mathbb{L}[x_n]/(f_n)$ es un cuerpo. Pero, por el Tercer Teorema de Isomorfía, $\mathbb{L}[x_n]/(f_n) \cong \mathbb{Q}[x_1, \ldots, x_{n-1}]/I$, por lo que $I$ es maximal.

Para probar la necesidad, supongamos $I$ maximal. Entonces $\mathbb{Q}[x_1, \ldots, x_n]/I$ es cuerpo, y del Lema de Zariski deducimos que es una extensión algebraica finita de $\mathbb{Q}$. De esta manera, como $\bar{x}_1$ es algebraico sobre $\mathbb{Q}$, existe un polinomio mónico irreducible $f_1(x_1) \in \mathbb{Q}[x_1]$ tal que $f_1(\bar{x}_1) = 0$. Puesto que $\overline{f_1(x_1)} = f_1(\bar{x}_1) = 0$, se tiene que $f_1(x_1) \in I$. Ahora, dado que $\bar{x}_2$ es algebraico sobre $\mathbb{Q}[\bar{x}_1]$, podemos encontrar $g_2(x_2) \in \mathbb{Q}[\bar{x}_1][x_2]$ mónico e irreducible tal que $g_2(\bar{x}_2) = 0$. Sustituyendo $\bar{x}_1$ por $x_1$ en $g_2$ se obtiene $f_2(x_1, x_2)$ tal que $\overline{f_2(x_1, x_2)} = f_2(\bar{x}_1, \bar{x}_2) = g_2(\bar{x}_2) = 0$, esto es, $f_2 \in I$. Iterando el proceso, encontramos polinomios en la forma del enunciado tales que $(f_1, \ldots, f_n) \subset I$.

Nos falta comprobar que $(f_1, \ldots, f_n) \supset I$. Sea $h(x_1, \ldots, x_n) \in I$. Como $f_n$ es mónico en $x_n$, podemos dividir $h$ entre $f_n$ respecto de la variable $x_n$, obteniendo $h = f_n g_n + r_{n-1}(x_1, \ldots, x_{n-1})$. Dividimos ahora $r_{n-1}$ entre $f_{n-1}$ respecto de $x_{n-1}$, obteniendo $r_{n-1} = f_{n-1}g_{n-1} + r_{n-2}(x_1, \ldots, x_{n-2}$. Iterando el proceso, podemos escribir $h = f_n g_n + \ldots f_1 r_1 + r_0$ con $r_0 \in \mathbb{Q}$. Pasando al cociente, obtenemos $0 = r_0$ y $h \in (f_1, \ldots, f_n)$. □

Cabe mencionar que la existencia de esta estructura "escalonada" de polinomios generadores puede verse como consecuencia de la aplicación del Lema de Normalización de Noether a este caso. Así, en particular, los ideales de $\mathbb{Q}[x, y]$ son de la forma $I = (f_1(x), f_2(x, y))$, con $f_1$ y $f_2$ como han sido descritos arriba. Por tanto, un punto $(a, b)$ con coordenadas algebraicas sobre $\mathbb{Q}$ puede representarse (además, de manera única) a través del ideal $I \subset \mathbb{Q}[x, y]$ definido por el polinomio mínimo de $a$ en $\mathbb{Q}$ y el polinomio mínimo de $b$ en $\mathbb{Q}[a]$, pero este ideal también define a todos los puntos conjugados de $(a, b)$.

Ahora, sea $P_1 = (a, b)$ y sea $P_2 = (a', b')$ uno de tales conjugados. Si $\mathbb{L} = \mathbb{Q}(a, b)$ y $\sigma$ es un $\mathbb{Q}$-isomorfismo de $\mathbb{C}$ que lleva $(a, b)$ en $(a', b')$, obtenemos un isomorfismo entre $\mathbb{L}$ y su cuerpo conjugado $\sigma(\mathbb{L})$ que deja fijo a $\mathbb{Q}$ y de manera que toda "operación" sobre $\mathbb{L}$ en términos de $a, b$ se transforma en una sobre $\sigma(\mathbb{L})$ en términos de $a', b'$, y viceversa.

De este modo, si $f \in \mathbb{Q}[x, y]$ (por tanto, invariante por conjugación) es el polinomio que define una curva afín -si se quiere, resultado de deshomogeneizar adecuadamente una curva proyectiva para estudiar el punto $P_1$-, la extensión de $\sigma$ a

$\mathbb{C}$ nos genera un $\mathbb{Q}$-isomorfismo entre los anillos locales $\mathcal{O}_{P_1}(f) = (\mathbb{C}[x,y]/(f))_{P_1}$ y $\mathcal{O}_{P_2}(f) = (\mathbb{C}[x,y]/(f))_{P_2}$ dado por $\bar{g}/\bar{h} \mapsto \overline{\sigma(g)}/\overline{\sigma(h)}$. Como la multiplicidad de un punto depende únicamente de su anillo local, esto quiere decir que todos los puntos conjugados tienen la misma multiplicidad (más aún, las tangentes a los puntos están relacionadas a través de la conjugación adecuada). Asimismo, si $g$ es otra curva con coeficientes en $\mathbb{Q}$, entonces la multiplicidad de intersección de $f$ y $g$ en cada uno de los conjugados coincide, pues de nuevo la conjugación nos proporciona un isomorfismo $\mathcal{O}_{P_1}(\mathbb{C}) \cong \mathcal{O}_{P_2}(\mathbb{C})$ en el que el ideal $(f,g)$ se preserva, de manera que $\mathcal{O}_{P_1}(\mathbb{C})/(f,g) \cong \mathcal{O}_{P_2}(\mathbb{C})/(f,g)$.

Esto explica por qué podemos estudiar un punto cualquiera de $\mathbb{C}^2$ a través de su ideal maximal asociado $I$ en $\mathbb{Q}[x,y]$.

Las consideraciones en el espacio proyectivo no suponen mayor problema, pues si un punto proyectivo (que podrá asociarse a un ideal maximal homogéneo de $\mathbb{Q}[x,y,z]$) vive en una carta determinada entonces todos sus conjugados también y podemos estudiar el comportamiento de ese punto en dicha carta.

### 3.1.1. Grado de un punto

Hemos visto que los ideales maximales de $\mathbb{Q}[x,y]$ están asociados a un punto y a sus conjugados (vía los polinomios que definen el ideal). Podemos calcular el número de puntos conjugados (grado del punto) en un ideal $I \in \mathbb{Q}[x,y]$ 0-dimensional sin salirnos de $\mathbb{Q}$ como

$$dim_{\mathbb{Q}}\mathbb{Q}[x,y]/I.$$

La justificación de este hecho es la siguiente: si $G$ es una base de Gröbner de $I$ sobre $\mathbb{Q}$, entonces también lo es sobre $\mathbb{C}$, y los monomios $m \notin Lt(I)$ constituyen una base tanto de $\mathbb{Q}[x,y]/I$ como de $\mathbb{C}[x,y]/I^e$. Por tanto, sus dimensiones son iguales, y coinciden, por ser $\mathbb{C}$ algebraicamente cerrado, con el número de puntos en $V(I^e)$:

$$dim_{\mathbb{Q}}\mathbb{Q}[x,y]/I = dim_{\mathbb{C}}\mathbb{C}[x,y]/I^e = \#V(I^e).$$

Si describimos los puntos a través de ideales homogéneos $I$ de $\mathbb{Q}[x,y,z]$, basta tener en cuenta que un punto y sus conjugados viven en la misma carta afín (pongamos $z=1$), y que por tanto el cálculo del número de conjugados puede realizarse como $dim_{\mathbb{Q}}\mathbb{Q}[x,y,z]/(I+(z-1))$.

### 3.1.2. Carta afín

Si $P = (a:b:c) \in \mathbb{P}^2$, entonces podemos obtener su ideal homogéneo asociado en $\mathbb{C}[x,y,z]$ como $I(P) = (bx-ay, cx-az, cy-bz)$.

Si una de las coordenadas de $P$, pongamos $c$ (resp. $a, b$), fuera nula, entonces obtendríamos que $z \in I(P)$ (resp. $x, y$). Podemos determinar una carta afín para $P$ escogiendo una variable que no pertenezca a $I(P)$.

Si lo que tenemos es el ideal homogéneo $I$ asociado a varios puntos conjugados $P_1, \ldots, P_n$, entonces $I = I(P_1) \cap \cdots \cap I(P_n)$. Si uno de ellos tuviera una coordenada nula, pongamos $c$, todos sus conjugados también la tendrían, y por lo anterior $z \in \bigcap P_i = I$. Así, nos vale la misma estrategia para seleccionar carta.

### 3.1.3. Cálculo de multiplicidades

Un recurso (ver Proposición 2.3 y su demostración) para obtener la multiplicidad de un punto $P$ en una curva afín $f$ consiste en calcular todas las derivadas parciales de $f$ de un cierto orden (empezando por la propia $f$, luego sus parciales de orden $1,\cdots$), evaluarlas en $P$ y comprobar si todas se anulan (en cuyo caso debemos pasar a las derivadas de orden siguiente) o no (en cuyo caso el orden es la multiplicidad). Si $P=(a,b)$, entonces $I(P)=(x-a,y-b)$, y en términos del desarrollo

$$f(x,y)=\sum_{k=0}^{d}\frac{1}{k!}\sum_{i=0}^{k}\binom{k}{i}\frac{\partial^k f}{\partial x^i\partial y^{k-i}}(P)(x-a)^i(y-b)^{k-i}$$

es claro que esto equivale a ir comprobando si $f\in I(P)^k$ para cada $k=1,2,\ldots,$ de manera que la multiplicidad es el menor $k$ tal que $f\notin I(P)^{k+1}$.

Como discutimos al principio, los puntos conjugados tienen el mismo comportamiento en términos de multiplicidades, luego si $I$ es el ideal de varios puntos conjugados $P_i$, por lo anterior la multiplicidad de cada $P_i$ coincide con el menor $k$ tal que $f\notin I^{k+1}$.

Finalmente, si tanto $f$ como los $P_i$ son proyectivos, basta con utilizar una carta para reducir los cálculos al caso anterior. De manera más precisa, si los puntos viven en la carta $z=1$ podemos calcular su multiplicidad hallando el menor entero no negativo $k$ tal que $f\notin I^{k+1}+(z-1)$.

### 3.1.4. Multiplicidad de intersección

Recordemos que una manera de calcular la multiplicidad de intersección de dos curvas proyectivas $F$ y $G$ en un punto $P$ es la siguiente (ver Proposición 2.23):

$$mult_P(F,G)=dim_{\mathbb{C}}\mathbb{C}[x,y]/\mathfrak{q},$$

siendo $\mathfrak{q}$ la componente $P_*$-primaria de la descomposición primaria $(F_*,G_*)$ como ideal de $\mathbb{C}[x,y]$. Veamos cómo realizar este cálculo directamente sobre $\mathbb{Q}$. Denotemos $f=F_*$, $g=G_*$.

**Teorema 3.3.** *Sean $f,\ g\in\mathbb{Q}[x,y]$ dos polinomios. Sea $(f,g)=Q_1\cap\ldots\cap Q_s$ la descomposición primaria minimal de $(f,g)$ sobre $\mathbb{Q}[x,y]$. Para cada $Q_i$ sea $Q_i^e=\mathfrak{q}_1^i\cap\ldots\cap\mathfrak{q}_{k_i}^i$ la descomposición primaria minimal de $Q_i^e$ (sobre $\mathbb{C}$). Entonces*

- *$I^e=\cap_{i,j}\mathfrak{q}_j^i$ es la descomposición primaria minimal de $I^e$.*
- *$k_i=\dim_{\mathbb{Q}}\frac{Q[x,y]}{\sqrt{Q_i}}$.*
- *Si $f=F_*$, $g=G_*$ para ciertos polinomios homogéneos $F,G\in\mathbb{Q}[x,y,z]$ y $P_*$ es un punto de intersección de $f$ y $g$, su ideal es uno de los ideales $\sqrt{\mathfrak{q}_j^i}$ y $mult_P(F,G)=\frac{1}{k_i}dim_{\mathbb{Q}}\frac{\mathbb{Q}[x,y]}{Q_i}$.*

*Demostración.* Como fue visto durante la demostración del Teorema 1.35, si $f\cap g=\{P_*=P_1,\ldots,P_r\}$, entonces la descomposición primaria minimal de $(f,g)^e$ tiene la forma $(f,g)^e=\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_r$ donde $\sqrt{\mathfrak{q}_i}=I(P_i)$. Tal y como hemos comentado al inicio de la sección, puntos conjugados tienen mismas multiplicidades, luego en particular un punto está en $f\cap g$ si y sólo si sus conjugados son puntos de intersección. Esto nos

dice que podemos agruparlos en paquetes disjuntos de puntos conjugados, o en otras palabras, que podemos escribir

$$\sqrt{(f,g)^e} = I(P_1) \cap \cdots \cap I(P_r) = I_1 \cap \cdots \cap I_s,$$

donde cada $I_i = \bigcap I(P_j)$ para los $j$ tales que $P_j$ son conjugados. De las propiedades básicas de extensión y contracción de ideales ([AM69] Ej 1.18) y de las propiedades particulares en el caso de extensiones de cuerpos ([ZS75] Chapter VII, § 11), se obtiene

$$\sqrt{(f,g)} = \sqrt{(f,g)^{ec}} = \sqrt{(f,g)^e}^{\,c} = I_1^c \cap \cdots \cap I_s^c,$$

donde, por construcción, cada $I_i^c$ es maximal en $\mathbb{Q}[x,y]$. Como el punto del que partimos, $P_*$, está en $f \cap g$, podemos suponer que $I = I_1^c$ es su ideal asociado.

Por lo anterior, es fácil ver que la descomposición primaria minimal de $(f,g)$ en $\mathbb{Q}[x,y]$ tendrá la forma $(f,g) = Q_1 \cap \cdots \cap Q_s$, donde $\sqrt{Q_i} = I_i^c$, y de nuevo por propiedades de extensión de ideales sobre extensiones de cuerpos,$(f,g)^e = Q_1^e \cap \cdots \cap Q_s^e$. Queremos ver que si $I$ está asociado a $P_1,\ldots,P_k$, entonces $Q_1^e = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_k$. En efecto, para ello basta observar que, dado que los conjuntos de ideales maximales $I(P_j)$ asociados a cada $Q_i^e$ son disjuntos dos a dos, la descomposición primaria minimal $(f,g)^e = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ se obtiene intersecando las descomposiciones primarias minimales de cada $Q_i^e$. Así, en particular, la descomposición primaria minimal de $Q_1^e$ será la intersección de los $\mathfrak{q}_i$ cuyos radicales sean $I(P_1),\ldots,I(P_k)$, esto es, $Q_1^e = \bigcap_{i=1}^k \mathfrak{q}_i$, como queríamos ver.

De esta manera, aplicando el Teorema Chino de los Restos, empleando el mismo argumento dimensional que para el cálculo del grado de un punto y teniendo en cuenta que los puntos conjugados tienen iguales multiplicidades de intersección: $dim_{\mathbb{Q}}\mathbb{Q}[x,y]/Q_1 = dim_{\mathbb{C}}\mathbb{C}[x,y]/Q_1^e = \sum_{i=1}^k dim_{\mathbb{C}}\mathbb{C}[x,y]/\mathfrak{q}_i = k \cdot mult_P(F,G)$, esto es,

$$mult_P(F,G) = \frac{1}{k} dim_{\mathbb{Q}}\mathbb{Q}[x,y]/Q_1,$$

donde $Q_1$ es la componente primaria de la descomposición de $(f,g)$ que corresponde a $P_*$, y $k$ es el grado del punto $P$.

□

El paso que debemos dar a continuación es, dado que trabajaremos con curvas proyectivas, el de relacionar la descomposición primaria de $(F,G)$ con la de $(f,g)$, para lo cual utilizaremos los siguientes resultados generales válidos para anillos de polinomios con coeficientes en un cuerpo $\mathbb{K}$ (nosotros los utilizaremos sobre $\mathbb{Q}$):

**Lema 3.4.** *Sea $I$ un ideal homogéneo de $\mathbb{K}[x_1,\ldots,x_{n+1}]$. Entonces $I$ es primario si y solo si para todo $F$ y $G$ homogéneos, $FG \in I \Rightarrow F \in I$ o $G \in \sqrt{I}$.*

*Demostración.* Ver [ZS75], Chapter VII, § 2, Lemma 2. □

Para los siguientes dos lemas recordemos que $(f^*)_* = f$ para todo $f \in \mathbb{K}[x_1,\ldots,x_n]$, y que para $F \in \mathbb{K}[x_1,\ldots,x_{n+1}]$, $F = x_{n+1}^m (F_*)^*$ donde $m$ es la mayor potencia de $x_{n+1}$ que divide a $F$ (En particular, si $(F_*)^* \in I$ ideal, entonces $F \in I$). También será necesaria la siguiente

**Definición 3.5.** *Dados dos ideales $I, J$ de un anillo $R$, llamamos* ***saturación de I por J*** *al ideal*

$$(I : J^\infty) = \{x \in R / J^n x \subset I para\ algún\ n\} = \bigcup_{n\in\mathbb{N}} (I : f^n).$$

Finalmente, si $I$ es ideal de $\mathbb{K}[x_1, \ldots, x_n]$, denotaremos $I^h = (\{f^* / f \in I\}) \in \mathbb{K}[x_1, \ldots, x_{n+1}]$. Análogamente, si $J$ es ideal de $\mathbb{K}[x_1, \ldots, x_{n+1}]$, denotaremos $J_h$ al ideal $(\{F_* / F \in J\})$ de $\mathbb{K}[x_1, \ldots, x_n]$. Es claro que $(I^h)_h = I$.

**Lema 3.6.** *En los siguientes apartados, $I, I_1, I_2$ son ideales de $\mathbb{K}[x_1, \ldots, x_n]$, y $J_1, J_2$ son ideales de $\mathbb{K}[x_1, \ldots, x_{n+1}]$:*

1. *$I$primario $\Leftrightarrow$ $I^h$primario.*
2. *$(I_1 \cap I_2)^h = I_1^h \cap I_2^h$.*
3. *$\sqrt{I^h} = \sqrt{I}^h$.*
4. *$(J_1 \cap J_2)_h = (J_1)_h \cap (J_2)_h$.*

*Demostración. 1.* "$\Rightarrow$" Por el lema anterior basta probarlo para formas. Sean $F, G$ homogéneos tales que $FG \in I^h$ y $F \notin I^h$ (por lo que $F_* \notin I$). Entonces $(FG)_* = F_* G_* \in I$ y $F_* \notin I$. Como $I$ es primario, de aquí $G_* \in \sqrt{I}$, y por ello $G_*^m \in I$ para cierto $m$. De esta manera, $(G_*^m)^* = ((G_*)^*)^m \in I^h$, y si $G = x_{n+1}^k (G_*)^*$, entonces $x_{n+1}^{km}((G_*)^*)^m = G^m \in I^h$, como queríamos demostrar.
"$\Leftarrow$" Sean $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ tales que $fg \in I$ y supongamos que $f \notin I$. Entonces $f^* g^* \in I^h$ y $f^* \notin I^h$. Así pues $g^* \in \sqrt{I^h}$, esto es, existe $m$ con $(g^*)^m = (g^m)^* \in I^h$. Finalmente $g^m = ((g^m)^*)_* \in I$.
*2.* $F \in (I_1 \cap I_2)^h \Leftrightarrow F_* \in I_1 \cap I_2 \Leftrightarrow F \in I_1^h \cap I_2^h$.
*3.* $F \in \sqrt{I^h} \Leftrightarrow F^n \in I^h \Leftrightarrow (F^n)_* = (F_*)^n \in I \Leftrightarrow F_* \in \sqrt{I} \Leftrightarrow F \in \sqrt{I}^h$.
*4.* Observemos que, en general, si $f \in J_h$, entonces $f = F_*$ para cierto $F$ de $J$, y por tanto $f^* = (F_*)^* \in (J : x_{n+1}^\infty)$. De la misma manera, si $f^* \in (J : x_{n+1}^\infty)$, entonces existe $m$ con $x_{n+1}^m f^* \in J$, y deshomogeneizando, $f \in J_h$. Así pues, $f \in (J_1)_h \cap (J_2)_h \Leftrightarrow f^* \in (J_1 : x_{n+1}^\infty) \cap (J_2 : x_{n+1}^\infty) = (J_1 \cap J_2 : x_{n+1}^\infty) \Leftrightarrow f \in (J_1 \cap J_2)_h$. □

**Lema 3.7.** *Sean $F, G$ dos polinomios homogéneos de $\mathbb{K}[x_1, \ldots, x_{n+1}]$, y $f = F_*$, $g = G_* \in \mathbb{K}[x_1, \ldots, x_n]$. Entonces*

$$((F, G) : x_{n+1}^\infty) = (f, g)^h.$$

*Demostración.* "$\supseteq$" Sea $H \in (f, g)^h$. Entonces $H_* = af + bg$ para ciertos $a, b \in \mathbb{K}[x_1, \ldots, x_n]$. Homogeneizando la expresión anterior y multiplicando por una potencia $k$ de $x_{n+1}$ suficientemente grande, podemos escribir $x_{n+1}^k H = AF + BG \in (F, G)$, luego $H \in ((F, G) : x_{n+1}^\infty)$.
"$\subseteq$" Si $H \in ((F, G) : x_{n+1}^\infty)$, entonces existe $m$ con $x_{n+1}^m H = AF + BG$. Deshomogeneizando, $H_* \in (f, g)$, de donde $H \in (f, g)^h$. □

**Proposición 3.8.** *Si $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ es una descomposición primaria minimal, entonces $I^h = \mathfrak{q}_1^h \cap \cdots \cap \mathfrak{q}_r^h$ es una descomposición primaria minimal de $I^h$.*

*Demostración.* La igualdad $I^h = \mathfrak{q}_1^h \cap \cdots \cap \mathfrak{q}_r^h$ se sigue del Lema 3.6 *2.*. Además, cada $\mathfrak{q}_i^h$ es primario atendiendo al Lema 3.6 *1.*. Los primos asociados a cada $\mathfrak{q}_i^h$ son todos distintos, pues en virtud del Lema 3.6 *3.*,

$$\sqrt{\mathfrak{q}_i^h} = \sqrt{\mathfrak{q}_j^h} \Leftrightarrow \sqrt{\mathfrak{q}_i}^h = \sqrt{\mathfrak{q}_j}^h \Leftrightarrow \sqrt{\mathfrak{q}_i} = \sqrt{\mathfrak{q}_j}.$$

Para terminar, es minimal, pues si se tuviera $\mathfrak{q}_i^h \supseteq \bigcap_{j\neq i} \mathfrak{q}_j^h$, entonces por el Lema 3.6 *4.* $\mathfrak{q}_i \supseteq \bigcap_{j\neq i} \mathfrak{q}_j$. □

**Corolario 3.9.** *Sean $F, G$ formas en $\mathbb{K}[x_1, \ldots, x_{n+1}]$, $f = F_*$, $g = G_*$. Si se tiene que $(f, g) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ es una descomposición primaria minimal de $(f, g)$, entonces $((F, G) : x_{n+1}^\infty) = \mathfrak{q}_1^h \cap \cdots \cap \mathfrak{q}_r^h$ es una descomposición primaria minimal de $((F, G) : x_{n+1}^\infty)$.*

Centrémonos ahora en nuestro caso particular. Sean $F, G$ polinomios homogéneos de $\mathbb{Q}[x, y, z]$ sin componentes en común. Observemos en primer lugar que la única componente inmersa que podría aparecer en una descomposición minimal de $(F, G)$ es aquella que tiene por radical $(x, y, z)$ (correspondiente al punto $(0, 0, 0)$). El resto son componentes primarias aisladas: a grosso modo, razonando como en el caso afín, cada una de ellas está asociada a un conjunto distinto de puntos de intersección conjugados, esto es, sus radicales (tomando en cuenta la carta en la que viven los puntos) son todos maximales distintos.

En segundo lugar, es fácil comprobar (cf. Proposición 1.30) que, si $\mathfrak{q}$ es un ideal primario en un anillo $R$ y $r \in R$, se tiene que

- Si $r \in \sqrt{\mathfrak{q}}$, entonces $(\mathfrak{q} : r^\infty) = (1)$.
- Si $r \notin \sqrt{\mathfrak{q}}$, entonces $(\mathfrak{q} : r^\infty) = \mathfrak{q}$.

Así pues, si en nuestro caso $(F, G) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}_{r+1} \cap \cdots \cap \mathfrak{q}_s$ es descomposición minimal de $(F, G)$, con $z \notin \sqrt{\mathfrak{q}_i}, i = 1, \ldots, r$, y $z \in \sqrt{\mathfrak{q}_i}, i = r+1, \ldots, s$, entonces $((F, G) : z^\infty) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$ es una descomposición minimal de $((F, G) : z^\infty)$. De lo anterior, como $z \in (x, y, z)$, obtenemos que todas las componentes son aisladas, y por tanto, en virtud del segundo teorema de unicidad de descomposición primaria, que la descomposición es única. En particular, el Corolario 3.9 nos dice que si $(F_*, G_*) = Q_1 \cap \cdots \cap Q_r$, entonces estas componentes son exactamente las $\mathfrak{q}_i = Q_i^h$. Así, si $P = (a : b : 1) \in F \cap G$ y $Q$ es la componente primaria de $(F_*, G_*)$ asociada a $(a, b)$, entonces $\mathfrak{q} = Q^h$ es la componente asociada a $P$ de $((F, G) : z^\infty)$ y

$$mult_P(F, G) = \frac{1}{k} dim_{\mathbb{Q}} \mathbb{Q}[x, y]/Q = \frac{1}{k} dim_{\mathbb{Q}} \mathbb{Q}[x, y, z]/(\mathfrak{q} + (z - 1)).$$

En general, saturando $(F, G)$ por $(x, y, z)$ para eliminar la posible componente inmersa y teniendo en cuenta la identidad $((F, G) : (x, y, z)^\infty) = ((F, G) : x^\infty) \cap ((F, G) : y^\infty) \cap ((F, G) : z^\infty)$ deducimos que las componentes de $((F, G) : (x, y, z)^\infty)$ son homogeneizaciones de una componente adecuada de $(F_{*,x}, G_{*,x})$, $(F_{*,y}, G_{*,y})$ o $(F_{*,z}, G_{*,z})$, y que por tanto, para todo $P \in F \cap G$,

$$mult_P(F, G) = \frac{1}{k} dim_{\mathbb{Q}} \mathbb{Q}[x, y, z]/(\mathfrak{q} + carta(P)),$$

donde $\mathfrak{q}$ es la componente de $((F, G) : (x, y, z)^\infty)$ en $\mathbb{Q}[x, y, z]$ con $\sqrt{\mathfrak{q}} = I$ el ideal maximal del punto, y $carta(P)$ es el ideal $(x - 1)$,$(y - 1)$ o $(z - 1)$ en función de si $P$ vive en la carta $x = 1$, $y = 1$ o $z = 1$, respectivamente (en caso de varias posibilidades, es independiente de la elección de carta).

### 3.1.5. Puntos de intersección y singularidades

De la subsección anterior, para hallar los puntos de intersección de dos curvas proyectivas $F$ y $G$ basta calcular la descomposición primaria de $((F,G):(x,y,z)^\infty)$, de manera que los puntos vienen descritos por los radicales de cada componente.

El cálculo de puntos singulares de una curva proyectiva se hace de manera similar: Si $F$ es una curva proyectiva con coeficientes en $\mathbb{Q}$, sus puntos singulares quedan descritos por los ideales primos asociados a la descomposición de $((F_X,F_Y,F_Z):(x,y,z)^\infty)$, y podemos estudiar sus multiplicidades y número de conjugados como hemos explicado.

El análisis del carácter (ordinario o no) de cada punto requiere ya trabajar en extensiones de $\mathbb{Q}$. Sobre los complejos, estudiar el carácter de un punto afín $(a,b)$ de una curva $f$ conlleva examinar la factorización de la forma en $x-a, y-b$ de menor grado $f_r$ de $f$, cuyos factores son las tangentes. Más concretamente, si $f_r$ es libre de cuadrados en $\mathbb{C}[x,y]$, sus tangentes serán todas distintas y el punto será ordinario, y en caso contrario será no ordinario.

Si $P$ viene descrito por el ideal $I=(g_1(x),g_2(x,y))$ en $\mathbb{Q}[x,y]$, $f_r$ puede verse como polinomio de $\mathbb{Q}[x,y,a,b]/(g_1(a),g_2(a,b))=\mathbb{Q}(\alpha,\beta)[x,y]$. Además, usaremos el siguiente resultado:

**Lema 3.10.** *Sea $\mathbb{K}\subseteq\mathbb{C}$ un subcuerpo. Sea $f\in\mathbb{K}[x,y]$. Entonces $f$ es libre de cuadrados en $\mathbb{K}[x,y]$, si y solo si lo es en $\mathbb{C}[x,y]$.*

*Demostración.* Supongamos que sobre $\mathbb{C}[x,y]$ tenemos $f=p_1^2p_2$ con $p_1$ irreducible. Sea $\mathbb{H}$ la menor extensión de $\mathbb{K}$ que contiene a los coeficientes de $p_1$ y sea $\mathbb{H}^N$ su clausura normal. Para cada isomorfismo de conjugación $\sigma$ asociado a la extensiones $\mathbb{K}\subseteq\mathbb{H}^N$, tendremos que $\sigma(p_1)$ es un polinomio irreducible cuyo cuadrado divide a $f$, y por tanto el producto de todos ellos es un polinomio de $\mathbb{K}$ cuyo cuadrado divide a $f$. Con esto hemos probado que si $f$ es libre de cuadrados en $\mathbb{K}$ entonces lo es en $\mathbb{C}$. La otra implicación es evidente. □

De esta manera todo "se reduce a" factorizar en anillos de polinomios con coeficientes en una extensión algebraica de $\mathbb{Q}$. Puesto que el software empleado no dispone de tales algoritmos de factorización en el caso no primitivo de manera directa, usamos rutinas de descomposición primaria para alcanzar el mismo resultado:

**Teorema 3.11.** *Sea $m=(g_1(a),g_2(a,b))$ maximal en $\mathbb{Q}[a,b]$, $\mathbb{Q}(\alpha,\beta)=\mathbb{Q}[a,b]/m$. Sea*

$$\pi:\mathbb{Q}[x,y,a,b]\to\mathbb{Q}[x,y,a,b]/(g_1(a),g_2(a,b))=\mathbb{Q}(\alpha,\beta)[x,y]$$

*la proyección natural. Sea $G\in\mathbb{Q}(\alpha,\beta)[x,y]$. Entonces, módulo el producto por unidades, son equivalentes:*

1. *$G=G_1^{r_1}\dots G_s^{r_s}$ es la descomposición en irreducibles de $G$ en $\mathbb{Q}(\alpha,\beta)[x,y]$.*
2. *$(G)=(G_1^{r_1})\cap\dots\cap(G_s^{r_s})$ es la descomposición primaria minimal de $(G)$ en $\mathbb{Q}(\alpha,\beta)[x,y]$.*
3. *$(G)+m=[(G_1^{r_1})+m]\cap\dots\cap[(G_s^{r_s})+m]$ es la descomposición primaria minimal de $(G)+m$ en $\mathbb{Q}[a,b,x,y]$.*

*Demostración.* La equivalencia entre *1.* y *2.* es clara. Veamos la equivalencia con *3.*: dado que la contracción de ideales conmuta con intersecciones y radicales y preserva ideales primarios, tenemos que en $\mathbb{Q}[x,y,a,b]$

$$(G)+m=[(G_1^{r_1})+m]\cap\dots\cap[(G_s^{r_s})+m]$$

es descomposición primaria de $(G)+m$, y que $\sqrt{(G_i^{r_i})+m} = (G_i)+m$. Además, la descomposición es minimal, pues si $(G_i)+m = (G_j)+m$ entonces se tendría que $(G_i) = (G_j)$ en $\mathbb{Q}(\alpha,\beta)[x,y]$, y si $G_i^{r_i}+m \supset \bigcap_{j\neq i}[(G_j^{r_j})+m]$, que $G_i^{r_i}$ divide a $\prod_{j\neq i} G_j^{r_j}$.

Finalmente, la descomposición minimal de $(G)+m$ es única puesto que todas sus componentes son aisladas (si $(G_i)+m \subseteq (G_j)+m$, tendríamos que $G_j$ divide a $G_i$), luego hemos relacionado unívocamente factorización en $\mathbb{Q}(\alpha,\beta)[x,y]$ y descomposición primaria en $\mathbb{Q}[x,y,a,b]$ de ideales de la forma $(f)+m$. □

Por tanto, $G$ es libre de cuadrados en $\mathbb{Q}(\alpha,\beta)[x,y]$ si y sólo si $(G)+m$ es radical en $\mathbb{Q}[x,y,a,b]$ ($(G)+m$ es radical si y sólo si cada componente primaria lo es, precisamente por la unicidad de la descomposición).

Visto esto, pongamos que estamos estudiando la curva definida por $f$ y que $P$ es un punto de multiplicidad $r$ cuyas coordenadas vienen descritas por el ideal $m = (g_1(a), g_2(a,b))$. Para estudiar su carácter hallamos la forma $f_r$ en $x-a, y-b$ de grado $r$ en $f$, para lo cual simplemente debemos reducir $f$ módulo $(x-a, y-b)^{r+1}+m$, y comprobamos si $(f_r)+m$ es radical en $\mathbb{Q}[a,b,x,y]$.

Para el caso proyectivo es análogo, trabajando en $\mathbb{Q}[x,y,z,a,b]$ pero añadiendo a $m$ una carta en la que viva $P$.

### 3.1.6. Cálculo del género

La definición de género dada en la Sección 2.5 no resulta práctica para calcularlo. Afortunadamente, y como ya adelantáramos en 2.4, existe una expresión explícita y cómoda del género cuando trabajamos con una curva cuyas singularidades son ordinarias ([Ful71], Cap. 8, Prop. 5):

**Proposición 3.12.** *Sea $\mathcal{C}$ una curva plana de grado $d$ con tan solo singularidades ordinarias, y denotemos $m_P = m_P(\mathcal{C})$. Entonces el género de $\mathcal{C}$ viene dado por la fórmula*

$$g = \frac{(d-1)(d-2)}{2} - \sum_{P\in\mathcal{C}} \frac{m_P(m_P-1)}{2}.$$

Además, si $\mathcal{C}$ es una curva plana proyectiva irreducible, sabemos que empleando un número finito de transformaciones de Cremona podemos obtener otra curva $\mathcal{C}'$ cuyas singularidades son todas ordinarias, luego tenemos un primer método para el cálculo del género que, no obstante, no es el más eficiente posible.

En [SWPD08], Chapter 3, Sec. 2, se proporciona un método (que además es local) que permite calcular el género estudiando directamente las singularidades de $\mathcal{C}$ y tomando ciertas consideraciones sobre aquellas no ordinarias. De forma más precisa, sea $P$ un punto no ordinario de $\mathcal{C}$, movámoslo a $(0:0:1)$ en las condiciones del procedimiento descrito en 2.4 y apliquemos la tranformación de Cremona. Diremos que los puntos de corte no fundamentales $\{P_1,\dots,P_k\}$ del tranformado estricto $\mathcal{C}_1$ con la recta excepcional $z=0$ constituyen el **primer entorno** de $P$. Algunos de estos puntos podrían ser no ordinarios en $\mathcal{C}_1$, luego podemos definir de forma análoga sus primeros entornos. La unión de todos ellos constituyen el **segundo entorno** de $P$. De manera sucesiva definimos el **$i$-ésimo entorno** de $P$. Como toda singularidad no ordinaria puede resolverse en un número finito de pasos, para cierto $i$ los puntos en el $i$-ésimo entorno de $P$ son ordinarios, y por tanto este procedimiento se detiene. Llamaremos **entorno** de $P$ y denotaremos $N(P)$ a la unión de todos los entornos $i$-ésimos de $P$. Si el punto $P$ es ordinario definiremos $N(P) := \emptyset$.

**Teorema 3.13.** *Sea $\mathcal{C}$ una curva proyectiva irreducible de grado $d$ y sean $\{P_1, \ldots, P_s\}$ sus puntos singulares. Sea $S = \{P_1, \ldots, P_s\} \cup N(P_1) \cup \cdots \cup N(P_s)$, y para cada punto $P \in S$, $m_P$ su multiplicidad en la curva correspondiente. Entonces, su género $g$ puede calcularse mediante la fórmula*

$$g = \frac{(d-1)(d-2)}{2} - \sum_{P \in S} \frac{m_P(m_P - 1)}{2}.$$

Para cada punto singular $P$ de $\mathcal{C}$, este mismo procedimiento puede realizarse trabajando en una carta adecuada (en la que viva $P$) moviendo $P_*$ al origen y empleando las explosiones en el plano afín presentadas en [Ful71], Cap. 7, § 2. Algebraicamente, dada una curva plana afín $f$ con singularidad en el origen de multiplicidad $r$ y tal que $x$ no sea tangente a $f$ en $(0,0)$, se calcula el **transformado estricto** de $f$ mediante la explosión en el origen, $f' = f(x, xy)/x^r$. Si $x$ no es tangente a $f$ en $(0,0)$, entonces tras la explosión el punto $(0,0)$ ha dado lugar a $s$ puntos $\{P_1, \ldots, P_s\}$, uno por cada tangente a $f$ en $(0,0)$ distinta, y que son los puntos de corte de $f'$ con el **divisor excepcional** $E : x = 0$. Se construye así, repitiendo el proceso recursivamente con cada $P_i$, el análogo a $N(P)$ en el caso afín, que denotaremos $N_*(P)$. Afirmamos que el género puede calcularse de la misma manera que en el Teorema 3.13 sustituyendo las multiplicidades de los puntos de $N(P)$ por las de los puntos de $N_*(P)$. Para comprobarlo basta entender la relación existente entre una transformación de Cremona y las transformaciones que realizamos en el plano afín. Si tenemos un punto $(x : y : z)$ que vive en la carta $z = 1$, entonces mediante la tranformación en el plano afín lo que hacemos es

$$(x : y : z) \mapsto \left(\frac{x}{z}, \frac{y}{z}\right) \mapsto \left(\frac{x}{z}, \frac{xy}{z^2}\right).$$

Si invertimos la segunda variable (lo cual da lugar a un isomorfismo birracional del plano en sí mismo), retornamos al proyectivo y hacemos un intercambio entre las variables $x$ y $z$:

$$\left(\frac{x}{z}, \frac{xy}{z^2}\right) \mapsto \left(\frac{x}{z}, \frac{x}{y}\right) \mapsto (xy : xz : yz) \mapsto (yz : xz : xy),$$

que es justamente la imagen de $(x : y : z)$ por la transformación de Cremona. Esto quiere decir que, vistas proyectivamente, las transformaciones que hacemos en el afín y las transformaciones de Cremona dan lugar a curvas birracionalmente equivalentes, isomorfas fuera de las rectas excepcionales. Además, dado el último cambio de variable realizado, lo que ocurre con las intersecciones de la primera con $E : x = 0$ corresponde a lo que ocurre con las intersecciones no fundamentales de la segunda sobre $z = 0$ (pues esos puntos están en la clausura Zariski, y fuera de esas rectas las curvas se comportan igual). Por tanto el estudio de multiplicidades, que dependen únicamente del cuerpo de funciones racionales, es equivalente en ambas.

### 3.1.7. Implementación

En el código implementado, el usuario dispone de dos clases principales, **punto** y **curva**, cada una con los métodos oportunos para extraer la información deseada haciendo uso de la teoría expuesta en esta sección.

La clase **punto** permite trabajar con puntos del plano proyectivo dados a través de su ideal homogéneo sobre $\mathbb{Q}[x, y, z]$, y dispone de los métodos **ideal**, que devuelve

el ideal que define al punto, **carta**, que devuelve una de las cartas en las que vive el punto, y **grado**, que calcula el número de puntos conjugados.

La clase **curva**, por su parte, permite trabajar con curvas proyectivas planas con coeficientes en $\mathbb{Q}$ definiéndolas a través del polinomio homogéneo correspondiente. Dispone de los métodos **ec**, que devuelve el polinomio que la define, **contiene** y **mult**, que permiten comprobar si un punto está en la curva y cuál es su multiplicidad, respectivamente, **mult_int**, que calcula la multiplicidad de intersección con otra curva en un punto, **bezout**, que halla los puntos de intersección con otra curva, **sing**, que calcula y estudia las singularidades de la curva (incluyendo multiplicidad, número de conjugados y carácter del punto), **genero**, que devuelve el género de la curva y **mostrar_grafo**, que muestra el grafo asociado a las explosiones requeridas durante el cálculo del género.

Hagamos especial hincapié en estos dos últimos métodos. Para el cálculo del género utilizamos el Teorema 3.13 realizando explosiones afines locales mediante la función **blow_up**. De forma más precisa, tomamos cada singularidad $P$, calculamos una recta $L$ no tangente en $P$ mediante la función **no_tang** y aplicamos una traslación que lleve $P$ al origen y $L$ a la recta $x$, aplicamos la transformación estándar y hallamos los puntos de intersección del transformado estricto con el divisor excepcional, repitiendo el proceso con aquellos que sean múltiples. Aplicar las traslaciones nos obliga a considerar curvas cuyos coeficientes son elementos algebraicos sobre $\mathbb{Q}$. Es por ello que se dispone de dos clases secundarias **punto_alg** y **curva_alg** que nos permiten trabajar en extensiones de $\mathbb{Q}$ guardando las relaciones de los elementos algebraicos. La clase **punto_alg** tiene los métodos **ideal** y **grado_alg**, análogos a los de **punto**, y la clase **curva_alg** los métodos **ec, contiene_alg, mult_int, mult_int_alg** (análogos a los de **curva**) y **div_exc**, para el cálculo de los puntos de corte con el divisor excepcional.

Durante el método género se va calculando un grafo dirigido en el que cada componente conexa es un árbol que representa el entorno $N_*(P)$ de cada punto singular $P$ y sus conjugados. Así, las aristas unen la raíz con los puntos en su primer entorno, y a éstos a su vez con los puntos en su primer entorno, hasta que todos los puntos obtenidos sean simples. No obstante, representamos con un mismo nodo a un punto y a todos sus conjugados. Las funciones **busca_raices, rcolor, grafo_complejo, conjugados, lista_a_grafo** y **add_subgraph** tienen por objetivo obtener, a partir del grafo anterior, otro grafo en el que cada nodo está asociado a un único punto, y de manera que los subárboles al mismo nivel (de una misma componente conexa) y representados con idénticos colores están asociados a puntos conjugados. El método **mostrar_grafo** representa este grafo en pantalla (añadiendo un nodo raíz auxiliar cuya única función es unir cada componente conexa). Si de un punto sale una arista roja, entonces el punto es no ordinario, y el nodo de llegada de esa arista corresponde con una dirección tangente múltiple del mismo.

Finalmente, tenemos la clase **variable**, que provee de variables sin repetir, y las funciones **cambio** y **cambio1**, con finalidades auxiliares.

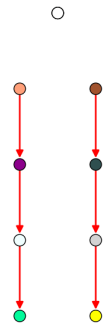
## 3.2. Ejemplos

**Ejemplo 1:** $x^2 - y^7$

Consideramos la curva $x^2z^5 - y^7$.

Tenemos los puntos singulares no ordinarios $(0 : 0 : 1)$, de multiplicidad 2, y

$(1:0:0)$, de multiplicidad 5. El género de la curva es 0. La Figura 3.1 siguiente es el grafo de explosiones realizadas para el cálculo del género,



Se deben realizar 3 explosiones en cada punto para resolver la singularidad. Hasta lograrlo, tras cada explosión surge un nuevo punto no ordinario.

Figura 3.1: grafo del Ejemplo 1

Por poner un ejemplo, los puntos de intersección de la curva con la parábola $y = x^2$ son: Puntos $(1:1:1)$ y $(-1:1:1)$ con multiplicidad 1; dos puntos conjugados con multiplicidad 1 $(\pm i:-1:1)$; cuatro puntos conjugados con multiplicidad 1 $(\mp\sqrt{\pm\alpha}:\pm\alpha:1)$, donde $\alpha$ es raíz de $y^2-y+1$; dos puntos conjugados $(-\beta-1:\beta:1)$ y otros dos puntos conjugados $(\beta+1:\beta:1)$ donde $\beta$ es raíz de $y^2+y+1$, todos con multiplicidad 1; y el origen $(0:0:1)$ con multiplicidad 2.

**Ejemplo 2:** El trébol de cuatro hojas

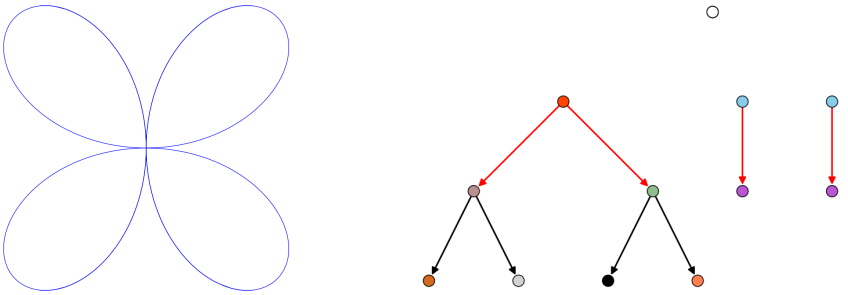


Figura 3.2: $(x^2+y^2)^3-4x^2y^2$ y su grafo

Consideramos ahora la curva $(x^2+y^2)^3-4x^2y^2z^2$. En este caso, el origen $(0:0:1)$ es un punto múltiple de dimensión 4, y además tenemos el par de puntos conjugados $(\pm i:1:0)$, cada uno de multiplicidad 2. Todos ellos son no ordinarios. El género es 0, y la Figura 3.2 muestra el proceso de explosiones realizadas. Tras la primera explosión todos los puntos pasan a ser ordinarios.

**Ejemplo 3:** Doble recubrimiento del trébol de cuatro hojas

La curva es ahora $f = (x^4+y^2z^2)^3-4x^4y^2z^6$. El doble recubrimiento de la figura trébol es de género 1 y sus singularidades son el origen $(0:0:1)$ y el punto del infinito $(0:1:0)$, ambos no ordinarios de multiplicidad 6. La Figura 3.3 representa el grafo de explosiones. Vemos por ejemplo que uno de los puntos (el origen) tiene una única tangente múltiple de multiplicidad 2, mientras que en el punto del infinito hay una única tangente de multiplicidad 6. Se observa además, que en el origen hay cuatro

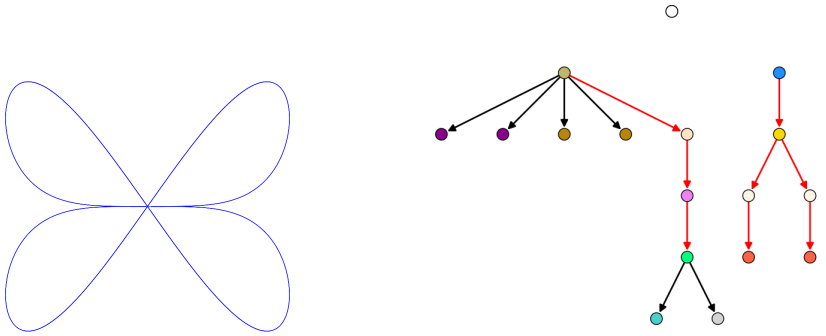


Figura 3.3: $(x^4+y^2)^3-4x^4y^2$ y su grafo

rectas tangentes ordinarias clasificadas en dos familias de dos rectas conjugadas sobre $\mathbb{Q}$ cada una.

**Ejemplo 4:** Ejemplo de curva reducible

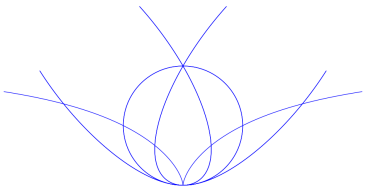


Figura 3.4: $(x^2+y^2-yz)(y^3+yx^2-zx^2)(y^4-2y^3z+y^2z^2-3yzx^2+2x^4)$

La siguiente curva algebraica aparece como ejemplo recogido en [SWPD08], Sec. 2.1.2, y es el resultado de la unión de una cónica, una cúbica y una cuártica.

Los puntos singulares son: El punto doble ordinario $(\frac{1}{2}:\frac{1}{2}:1)$; el punto doble ordinario $(-\frac{1}{2}:\frac{1}{2}:1)$;tres puntos dobles conjugados dados por $(-1:\alpha:1)$, donde $\alpha$ es raíz de $y^3+y-1$, y otros tres puntos dobles conjugados $(1:\alpha:1)$ con $\alpha$ como antes, todos ellos ordinarios; dos puntos dobles conjugados ordinarios $(\frac{1}{3\sqrt{2}}:\frac{1}{3}:1)$; dos puntos dobles conjugados ordinarios $(\pm i:1:0)$; el punto triple ordinario $(0:1:1)$ y el punto quíntuple no ordinario $(0:0:1)$.

Aunque se define el género para curvas que son irreducibles, existen generalizaciones al caso reducible que tienen en cuenta el número de componentes de la curva y de manera que sea consistente con sus propiedades sobre curvas irreducibles. La misma fórmula de género sigue siendo válida, pero se permite que el género sea negativo. De hecho, si una curva tiene género negativo entonces sabemos que es reducible.

# Bibliografía


[AM69] M.F. Atiyah and I.G. Macdonald. *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Ash02] R.B. Ash. *Abstract Algebra: The Basic Graduate Year.* 2002.

[Che51] C.Chevalley. *Introduction to the theory of Algebraic Functions of One Variable* A.M.S., 1951.

[CLO97] D.Cox, J.Little, and D.O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997.

[DBo61] J.H. De Boer. *Localization in a graded ring* Proceedings of the American Mathematical Society. Vol 12. No. 5 (Oct. 1961), pp. 764-772.

[Ful71] W.Fulton. *Curvas algebraicas: introducción a la geometría algebraica.* Barcelona [etc.]: Reverté, 1971. Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series.

[GrPf08] G.Greuel and G. Pfister. *A Singular Introduction to Commutative Algebra.* Springer, Second Edition, 2008.

[Pop11] P. Popescu-Pampu. *Qu'est-ce que le genre?.* Ed. École Polytechnique, Palaiseau, 2011. Dans Histoires de Mathématiques, Actes de Journées X-UPS 2011, 55-198.

[Sha77] I.R. Shafarevich. *Basic Algebraic Geometry Vol. 1.* Springer-Verlag, 1977

[St05] M. Stillman. *Tools for computing primary decompositions and applications to ideals associated to Bayesian networks.* From the book Solving Polynomial Equations, series Algorithms and Computation in Mathematics, Volume 14, 2005, pp. 203-239. Springer Berlin Heidelberg.

[SWPD08] J.R. Sendra, F.Winkler, and S.Pérez-Díaz. *Rational algebraic curves: A computer algebra approach*, volume22 of *Algorithms and Computation in Mathematics.* Springer, Berlin, 2008.

[Vai96] I.Vainsencher. *Introduçao às curvas algébricas planas.* Coleçao matemática universitária. Instituto de Matemática Pura e Aplicada, 1996.

[Wal50] R.J. Walker. *Algebraic Curves.* Springer-Verlag, 1950.

[ZS75] O.Zariski and P.Samuel. *Commutative algebra. Vol. II.* Springer-Verlag, New York, 1975. Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.

# Apéndice A

# Código

Se incluye a continuación una copia del código implementado.

```
K = QQ['x,y,z']
x,y,z = K.gens()

class variable():
    """
    Clase que permite crear variables. Requiere un argumento unico que es el nombre base de
    las variables.
    Ej: V = variable('a')
    """
    def __init__(self,s):
        self._s = str(s)
        self._count = 0
    def __repr__(self):
        return 'Generador de variables en ' + str(self._s)
    def devuelve(self,numvar):
        """
        Metodo que devuelve tantas variables como se indique. Se guarda el numero de
        variables que han sido creadas para evitar repeticiones.
        Ej: V.devuelve(2) devuelve ['a0','a1']
            V.devuelve(3) devuelve ahora ['a2','a3','a4']
        """
        L = [self._s+str(i) for i in range(self._count,self._count+numvar)]
        self._count = self._count+numvar
        return(L)

V = variable('a')

def cambio(I,x,y):
    """
    Funcion que realiza una copia del ideal sustituyendo las dos variables pasadas como
    argumento por nuevas variables, y devuelve tanto la copia como el ideal con los cambios
    realizados.
    Ej: cambio(ideal(x**2+1,y),x,y) devuelve (ideal(x-a0,y-a1),ideal(a0**2+1,a1))
    """
    R = I.ring()
    A = V.devuelve(2)
    B = list(R.gens())
    Kp = PolynomialRing(QQ,B+A)
    m = ideal(Kp(x)-Kp(A[0]),Kp(y)-Kp(A[1]))
    I = [i.substitute({x:Kp(A[0]),y:Kp(A[1])}) for i in I.gens()]*Kp
    return (m,I)

class punto():
    """
    Clase que permite trabajar con puntos del plano proyectivo dados a traves de su ideal
    homogeneo sobre el anillo de polinomios en tres variables con coeficientes racionales.
    Ej: El punto proyectivo (i:-i:1) se define como P = punto(ideal(x**2+z**2,x+y))
    """
    def __init__(self,I):
        self._ideal = ideal(I)
        self._var = ideal(I).ring().gens()

    def __repr__(self):
        return 'Punto definido por el ideal '+str(self._ideal)

    def ideal(self):
        """
        Devuelve el ideal que define al punto
        """
```

```
        return self._ideal

    def carta(self):
        """
        Devuelve una de las cartas en las que vive el punto.
        Ej: P.carta() devuelve z-1
        """
        if self._var[2] in self._ideal:
            if self._var[1] in self._ideal:
                return (self._var[0]-1)
            else:
                return (self._var[1]-1)
        else:
            return (self._var[2]-1)

    def grado(self):
        """
        Devuelve el numero de conjugados del punto definido, esto es, el numero de puntos
        de V(I) donde I es el ideal que define al punto.
        Ej: P.grado() devuelve 2 (corresponde a (i:-i:1) y (-i:i:1))
        """
        return (self._ideal+self.carta()).vector_space_dimension()

class curva():
    """
    Clase que permite definir curvas algebraicas proyectivas planas con coeficientes
    racionales.
    """
    def __init__(self,f):
        self._ec = f
        self._var = f.parent().gens()

    def __repr__(self):
        return 'Curva proyectiva plana de ecuacion '+str(self._ec)

    def ec(self):
        """
        Devuelve la ecuacion que define a la curva.
        """
        return self._ec

    def contiene(self,P):
        """
        Devuelve True si el punto P esta en la curva y False en caso contrario. P debe ser
        un elemento de la clase punto.
        """
        m = P.ideal()
        return self._ec in m

    def mult(self,P):
        """
        Devuelve la multiplicidad del punto P sobre la curva. P debe ser un elemento de la
        clase punto.
        """
        carta = P.carta()
        m = P.ideal()
        orden = 0
        while self.contiene(P):
            P = punto(P.ideal()*m+carta)
```

```
            orden = orden+1
        return orden

    def mult_int(self,g,P):
        """
        Devuelve la multiplicidad de interseccion de la curva y g en el punto P. P y g
        deben ser elementos de la clase punto y curva, respectivamente.
        """
        I = ideal(self._ec,g.ec())
        J = I.primary_decomposition()
        m = P.ideal()
        for j in J:
            if m == j.radical():
                conj = P.grado()
                mult = (j+P.carta()).vector_space_dimension()
                return mult/conj
        return 0

    def bezout(self,g):
        """
        Metodo que estudia la interseccion de la curva con g en caso de que no tengan
        componentes en comun. Devuelve una lista de tuplas, cada una de ellas con la
        siguiente informacion de un punto de interseccion:
        (Ideal, carta, multiplicidad de interseccion, numero de conjugados)
        """
        if gcd(self._ec,g.ec())<>1:
            raise Exception('Las curvas tienen componentes comunes')
            return
        I = ideal(self._ec,g.ec())
        I = I.saturation(ideal(self._var))[0]
        J = I.primary_decomposition()
        L = []
        for j in J:
            P = punto(j.radical())
            conj = P.grado()
            mult = (j+P.carta()).vector_space_dimension()
            mult = mult/conj
            L = L+[(P.ideal(),P.carta(),mult,conj)]
        return L

    def sing(self):
        """
        Metodo que devuelve las singularidades de una curva proyectiva dada.
        Devuelve una lista de tuplas, cada una de las cuales asociada a un punto y que
        contiene la siguiente informacion:(Ideal del punto (afin), relacion entre variables
        + carta, multiplicidad del punto, numero de conjugados, caracter), donde caracter
        vale True si el punto es ordinario y False en caso contrario.
        Ej: si el punto (i:-i:1) es de mult 2 ordinario, devuelve
        (ideal(x-a0,y-a1),ideal(a0**2+1,a0+a1,z-1),2,2,True)
        """
        I = ideal((self._ec).gradient())
        I = I.saturation(ideal(self._var))[0]
        J = I.primary_decomposition()
        L = []
        for j in J:
            P = punto(j.radical())
            m = P.ideal()
            conj = P.grado()
            r = self.mult(P)
```

```
            carta = P.carta()
            Pt = m+carta
            if conj > 1:
                if carta == self._var[2]-1:
                    Pt2 = cambio(Pt,self._var[0],self._var[1])
                else:
                    if carta == self._var[1]-1:
                        Pt2 = cambio(Pt,self._var[0],self._var[2])
                    else:
                        Pt2 = cambio(Pt,self._var[1],self._var[2])
                Kp = Pt2[0].ring()
                Gens = list(set((Pt2[0]**(r+1)).gens()))+list(Pt2[1].gens())
                Fr = (Kp(self._ec)).reduce(ideal(Gens).groebner_basis())
                if (Fr+Pt2[1])==(Fr+Pt2[1]).radical():
                    carac = True
                else:
                    carac = False
                L = L+[(Pt2[0],Pt2[1],r,conj,carac)]
            else:
                Gens = list(set((m**(r+1)).gens()))+[carta]
                Fr = (self._ec %carta).reduce(ideal(Gens).groebner_basis())
                if ideal(Fr)==ideal(Fr).radical():
                    carac = True
                else:
                    carac = False
                L = L+[(m,ideal(carta),r,conj,carac)]
        self._sing = L
        return L

    def genero(self):
        """
        Metodo que devuelve el genero de la curva.
        """
        Grafo = DiGraph()
        Dic = {}
        S = []
        d = (self._ec).degree()
        gen = (d-1)*(d-2)/2
        f = curva_alg(self._ec)
        try:
            Sing = self._sing
        except(AttributeError):
            Sing = self.sing()
        for sing in Sing:
            n = Grafo.add_vertex()
            #S es una lista con los puntos que faltan por explotar. Sus elementos son
            #tuplas, cada una con la siguiente informacion: (curva_alg, punto_alg,
            #multiplicidad, numero de conjugados, numero acumulado de conjugados, tg
            #multiple, numero de vertice), donde tg multiple indica si el punto esta
            #asociado a una direccion tg multiple de un punto no ordinario, y numero de
            #vertices indica su etiqueta en el grafo asociado a las explosiones.
            #Dic almacena la misma informacion en un diccionario.
            S = S+[(f,punto_alg(sing[0],sing[1]),sing[2],sing[3],sing[3],False,n)]
            Dic[n] = S[-1]
        while S<>[]:
            s=S.pop()
            gen = gen - s[4]*(s[2]*(s[2]-1)/2)
            bu = blow_up(s[0],s[1],s[2],s[4])
            f1 = bu[0]
```

```
            g = bu[1]
            # cada elemento de g contiene es una tupla con la siguiente informacion:
            #(punto_alg,multiplicidad, conjugados, tg multiple)
            for elm in g:
                n = s[-1]
                m = Grafo.add_vertex()
                Dic[m] = (f1,elm[0],elm[1],elm[2],s[4]*elm[2],elm[3],m)
                Grafo.add_edge((n,m))
                if elm[1]>1:
                    S = S+[(f1,elm[0],elm[1],elm[2],s[4]*elm[2],elm[3],m)]
        raices = busca_raices(Grafo)[0]
        Grafo.add_vertex(-1)
        for raiz in raices:
            Grafo.add_edge(-1,raiz)
        Dic[-1] = (0,0,0,1,0,0,0)
        #Se ha construido el grafo "sobre Q" asociado a las explosiones, esto es,
        #representando los puntos conjugados por un unico nodo
        self._grafo = (Grafo,Dic)
        return gen

    def mostrar_grafo(self):
        """
        Muestra el grafo dirigido asociado a las explosiones. Cada arista (negra o roja)
        une un punto con uno de los puntos que resultan al explotarlo (en esta direccion).
        Si de un nodo parte una arista roja, el punto correspondiente al nodo es no
        ordinario y el nodo de llegada corresponde a una de sus direcciones tangentes.
        Subgrafos al mismo nivel y con mismos colores corresponden a puntos conjugados.
        """
        try:
            Grafo,Dic = self._grafo
        except(AttributeError):
            g = self.genero()
            Grafo, Dic = self._grafo
        L = grafo_complejo(Grafo, Dic, -1)
        C,Color_vertices,Color_edges = lista_a_grafo(L)
        Color_vertices['white'] = [C.vertices()[-1]]
        return C.plot(vertex_labels = False, vertex_colors = Color_vertices,edge_colors =
        Color_edges, layout = 'tree')



def busca_raices(Grafo):
    """
    Funcion que devuelve las raices de un grafo.
    """
    L = []
    for vert in Grafo.vertices():
        if Grafo.neighbors_in(vert)==[]:
            L = L+[vert]
    return [tuple(L)]

C = [c for c in colors.values() if c != 'white']

def rcolor():
    """
    Generador de colores
    """
    return C[ZZ.random_element(148)].rgb()
```

```
def grafo_complejo(Grafo,Dic,vertice):
    """
    Funcion que construye la estructura -como lista de listas que representan un nodo y sus
    hijos- del grafo asociado a las explosiones en una curva teniendo en cuenta el numero
    de puntos conjugados en cada caso, esto es, con un nodo por cada punto complejo.
    """
    N = Grafo.neighbors_out(vertice)
    if not N:
        if vertice != -1:
            return [(rcolor(),'red' if Dic[vertice][5] else 'black'), []]
        else:
            return [(rcolor(),'white'), []]
    else:
        A = sum([[grafo_complejo(Grafo,Dic,i)]*conjugados(Grafo,Dic,i) for i in N],[])
        if vertice != -1:
            return [(rcolor(),'red' if Dic[vertice][5] else 'black'), A]
        else:
            return [(rcolor(),'white'), A]


def conjugados(G,D,i):
    """
    Devuelve la entrada de D correspondiente al numero de conjugados de un punto
    """
    return ZZ(D[i][3])

def lista_a_grafo(L):
    """
    Permite construir un grafo a partir de una lista en la que cada elemento está formado
    por un nodo y otra lista con sus hijos.
    """
    G = DiGraph()
    Color_vertices = {}
    Color_edges = {}
    hijos = []
    for i in L[1]:
        hijos.append( add_subgraph(G, i, Color_vertices, Color_edges ))
    n = G.add_vertex()
    for i in hijos:
        G.add_edge(n,i)
        try:
            Color_vertices[L[0][0]].append(n)
        except(KeyError):
            Color_vertices[L[0][0]] = [n]
        try:
            Color_edges[L[0][1]].append((n,i))
        except(KeyError):
            Color_edges[L[0][1]] = [(n,i)]
    return G, Color_vertices,Color_edges

def add_subgraph(G,i,Color_vertices, Color_edges):
    """
    Permite construir el subgrafo que parte de un nodo en la funcion lista_a_grafo
    """
    n = G.add_vertex()
    try:
        Color_vertices[i[0][0]].append(n)
    except(KeyError):
        Color_vertices[i[0][0]] = [n]
```

```
    if i[1]:
        for hijo in i[1]:
            m = add_subgraph(G,hijo,Color_vertices,Color_edges)
            G.add_edge(n,m)
            try:
                Color_edges[hijo[0][1]].append((n,m))
            except(KeyError):
                Color_edges[hijo[0][1]] = [(n,m)]
    return n



#Caso de elementos algebraicos
V1 = variable('b')

def cambio1(I,t,u):
    """
    Funcion que realiza una copia del ideal sustituyendo la primera variable pasada como
    argumento por 0 y la segunda por una nueva variable, y devuelve tanto la copia como el
    ideal con los cambios realizados.
    Ej: cambio1(ideal(x**2+a0**2,y+a1),x,y) devuelve (ideal(x,y-b0),ideal(a0**2,b0+a1))
    """
    R = I.ring()
    A = V1.devuelve(1)
    B = list(R.gens())
    Kp = PolynomialRing(QQ,B+A)
    m = ideal(Kp(t),Kp(u)-Kp(A[0]))
    I = [i.substitute({t:0, u:Kp(A[0])}) for i in I.gens()]*Kp
    return (m,I)

class punto_alg():
    """
    Clase que permite trabajar con puntos del plano proyectivo dados a traves de su ideal
    maximal en una carta afin en la que vivan y del ideal de relaciones algebraicas de sus
    coordenadas.
    Ej: El punto proyectivo (i:-i:1) se define como P = punto_alg(ideal(x-a0,y-b0),
    ideal(a0**2+1,a0+b0,z-1))
    """
    def __init__(self,P,Rel):
        self._rel = Rel
        if P.ring().ngens() > 3:
            self._ideal = P
        else:
            gb = Rel.groebner_basis()
            aux = [i.reduce(gb) for i in P.gens()]
            aux = [i//i.lc() for i in aux]
            self._ideal = ideal(aux)

    def __repr__(self):
        return 'Punto con ideal maximal '+str(tuple(self._ideal.gens()))+' y relaciones '+str
        (self._rel)

    def ideal(self):
        """
        Devuelve los ideales que definen al punto
        """
        return (self._ideal,self._rel)
```

```
    def grado_alg(self):
        """
        Devuelve el numero de conjugados del punto a partir de su ideal de relaciones
        """
        return (self._ideal+self._rel).vector_space_dimension()

class curva_alg():
    """
    Clase que permite definir curvas algebraicas proyectivas planas con coeficientes en
    una extension de QQ. Las relaciones que verifican los coeficientes son introducidas
    a traves del punto que se vaya a estudiar.
    """

    def __init__(self,f):
        self._ec = f

    def ec(self):
        """
        Devuelve la ecuacion de la curva.
        """
        return self._ec

    def contiene_alg(self,P):
        """
        Devuelve True si el punto P esta en la curva y False en caso contrario. P debe ser
        un elemento de la clase punto_alg.
        """
        return self._ec in (P.ideal()[0]+P.ideal()[1])

    def mult_alg(self,P):
        """
        Devuelve la multiplicidad del punto P sobre la curva. P debe ser un elemento de la
        clase punto_alg.
        """
        orden = 0
        m = P.ideal()[0]
        Rel = P.ideal()[1]
        I = m
        while self._ec in I+Rel:
            I = I*m
            orden = orden+1
        return orden

    def mult_int_alg(self,g,P):
        """
        Devuelve la multiplicidad de interseccion de la curva y g en el punto P. P y g
        deben ser elementos de la clase punto_alg y curva_alg, respectivamente.
        """
        I = ideal(self._ec,g.ec()) + P.ideal()[1]
        J = I.primary_decomposition()
        m = P.ideal()[0]+P.ideal()[1]
        for j in J:
            if m == j.radical():
                conj = P.grado_alg()
                mult = j.vector_space_dimension()
                return mult/conj
        return 0

    def div_exc(self,t,u,Rel,conjP):
```

```
        """
        Metodo que devuelve la informacion sobre los puntos de interseccion de la curva y el
        divisor excepcional t=0. Devuelve una lista de tuplas, cada una de ellas con la
        siguiente informacion de un punto de interseccion:(punto_alg,multiplicidad,numero de
        conjugados, tg multiple), donde tg multiple indica si el punto esta asociado a una
        direccion tg multiple de un punto no ordinario que ha sido explotado.
        """
        I = ideal(self._ec,t)+Rel
        J = I.primary_decomposition()
        L = []
        for j in J:
            Rad = j.radical()
            T = cambio1(Rad,t,u)
            P = punto_alg(T[0],T[1])
            conj = P.grado_alg()/conjP
            mult = self.mult_alg(P)
            mult_int = j.vector_space_dimension()/(conj*conjP)
            if mult_int==1:
                tangentemultiple = False
            else:
                tangentemultiple = True
            L = L+[(P,mult,conj,tangentemultiple)]
        return L

def no_tang(f,P,t,u,a,b):
    """
    Funcion que busca parametros k1,k2 tales que la recta k1(t-a)+k2(u-b) no es tangente a
    la curva f en el punto P. P y f son elementos de la clase punto_alg y curva_alg, resp.
    """
    r = f.mult_alg(P)
    g = curva_alg(t-a)
    mult = f.mult_int_alg(g,P)
    if r == mult:
        return 1,0
    cota = 2
    while True:
        v = random_vector(ZZ,2,cota)
        if v[0]>0:
            g = curva_alg(v[0]*(t-a)-v[1]*(u-b))
            mult = f.mult_int_alg(g,P)
            if r == mult:
                return v[0],v[1]
        cota = cota+1

def blow_up(f,P,Mult,ConjAcum):
    """
    Funcion que realiza la explosion (afin) de un punto_alg P en una curva_alg f,
    trasladandolo primero al origen de manera que la recta "x"=0 no sea tangente.
    Toma como input la curva_alg, el punto_alg, su multiplicidad y el numero total de
    conjugados, y devuelve una tupla formada por el transformado estricto, los puntos
    de corte con el divisor excepcional, el divisor excepcional y la recta no tangente
    que ha sido trasladada a "x"=0. Aqui "x" es una variable que depende del punto.
    """
    KK = P.ideal()[0].ring()
    Gens = P.ideal()[0].gens()
    t = KK(Gens[0]).variable(0)
    try:
        a = KK(Gens[0]).variable(1)
    except(IndexError):
```

```
    a = -(Gens[0]-t)
u = KK(Gens[1]).variable(0)
try:
    b = KK(Gens[1]).variable(1)
except(IndexError):
    b = -(Gens[1]-u)
k1,k2 = no_tang(f,P,t,u,a,b)
r = f.mult_alg(P)
Rel = P.ideal()[1]
g = (KK(f.ec()).substitute({t:t+a+k2*t*u, u:b+k1*t*u})).reduce(Rel.groebner_basis())//(t
**r)
g = KK(g)
f1 = curva_alg(g)
p = f1.div_exc(t,u,Rel,ConjAcum)
E = t
return f1,p,E,(k1,k2)
```

# Apéndice B

# Output de los ejemplos

**Ejemplo 1:** $x^2 - y^7$

Definimos la curva (proyectiva):

```
sage: f = curva((x**2-y**7).homogenize(z))
```

Singularidades y género:

```
sage: f.sing()
[(Ideal (y, x) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
Ideal (z - 1) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
2,
1,
False),
(Ideal (z, y) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
Ideal (x - 1) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
5,
1,
False)]
sage: f.genero()
0
```

Puntos de intersección con $y = x^2$:

```
sage: f.bezout(curva((y-x**2).homogenize(z)))
[(Ideal (y - z, x - z) of Multivariate Polynomial Ring in x, y,
    z over Rational Field,
z - 1,
1,
1),
(Ideal (y - z, x + z) of Multivariate Polynomial Ring in x, y, z
    over Rational Field,
z - 1,
1,
1),
(Ideal (y + z, x^2 + z^2) of Multivariate Polynomial Ring in x,
    y, z over Rational Field,
z - 1,
1,
2),
(Ideal (y^2 - y*z + z^2, x^2 - y*z) of Multivariate Polynomial
```

```
    Ring in x, y, z over Rational Field,
z - 1,
1,
4),
(Ideal (x + y + z, y^2 + y*z + z^2) of Multivariate Polynomial
    Ring in x, y, z over Rational Field,
z - 1,
1,
2),
(Ideal (x - y - z, y^2 + y*z + z^2) of Multivariate Polynomial
    Ring in x, y, z over Rational Field,
z - 1,
1,
2),
(Ideal (y, x) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
z - 1,
2,
1)]
```

**Ejemplo 2:** El trébol de cuatro hojas

Definimos la curva:

```
sage: f = curva(((x**2+y**2)**3-4*x**2*y**2).homogenize(z))
```

Singularidades y género:

```
sage: f.sing()
[(Ideal (x - a2, z - a3) of Multivariate Polynomial Ring in x, y
    , z, a2, a3 over Rational Field,
Ideal (a3, y^2 + a2^2, y - 1) of Multivariate Polynomial Ring in
     x, y, z, a2, a3 over Rational Field,
2,
2,
False),
(Ideal (y, x) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
Ideal (z - 1) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
4,
1,
False)]
sage: f.genero()
0
```

**Ejemplo 3:** Doble recubrimiento del trébol de cuatro hojas

Singularidades y género:

```
sage: f.sing()
[(Ideal (z, x) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
Ideal (y - 1) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
6,
1,
False),
(Ideal (y, x) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
Ideal (z - 1) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
6,
1,
```

```
11 False)]
12 sage: f.genero()
13 1
```

**Ejemplo 4:** Ejemplo de curva reducible

Definición de la curva y singularidades:

```
1  sage: f = curva((x**2+y**2-y*z)*(y**3+y*x**2-z*x**2)*(y**4-2*y
       **3*z+y**2*z**2-3*y*z*x**2+2*x**4))
2  sage: f.sing()
3  [(Ideal (2*y - z, 2*x - z) of Multivariate Polynomial Ring in x,
        y, z over Rational Field,
4  Ideal (z - 1) of Multivariate Polynomial Ring in x, y, z over
       Rational Field,
5  2,
6  1,
7  True),
8  (Ideal (2*y - z, 2*x + z) of Multivariate Polynomial Ring in x,
       y, z over Rational Field,
9  Ideal (z - 1) of Multivariate Polynomial Ring in x, y, z over
       Rational Field,
10 2,
11 1,
12 True),
13 (Ideal (x - a4, y - a5) of Multivariate Polynomial Ring in x, y,
        z, a4, a5 over Rational Field,
14 Ideal (z + a4, -z^3 + z^2*a5 + a5^3, z - 1) of Multivariate
       Polynomial Ring in x, y, z, a4, a5 over Rational Field,
15 2,
16 3,
17 True),
18 (Ideal (x - a6, y - a7) of Multivariate Polynomial Ring in x, y,
        z, a6, a7 over Rational Field,
19 Ideal (-z + a6, -z^3 + z^2*a7 + a7^3, z - 1) of Multivariate
       Polynomial Ring in x, y, z, a6, a7 over Rational Field,
20 2,
21 3,
22 True),
23 (Ideal (x - a8, y - a9) of Multivariate Polynomial Ring in x, y,
        z, a8, a9 over Rational Field,
24 Ideal (-z + 3*a9, -z^2 + 18*a8^2, z - 1) of Multivariate
       Polynomial Ring in x, y, z, a8, a9 over Rational Field,
25 2,
26 2,
27 True),
28 (Ideal (x - a10, z - a11) of Multivariate Polynomial Ring in x,
       y, z, a10, a11 over Rational Field,
29 Ideal (a11, y^2 + a10^2, y - 1) of Multivariate Polynomial Ring
       in x, y, z, a10, a11 over Rational Field,
30 2,
31 2,
32 True),
33 (Ideal (y - z, x) of Multivariate Polynomial Ring in x, y, z
       over Rational Field,
34 Ideal (z - 1) of Multivariate Polynomial Ring in x, y, z over
       Rational Field,
35 3,
36 1,
37 True),
38 (Ideal (y, x) of Multivariate Polynomial Ring in x, y, z over
```

```
    Rational Field,
Ideal (z - 1) of Multivariate Polynomial Ring in x, y, z over
    Rational Field,
5,
1,
False)]
```