Apuntes de Curvas Algebraicas

por Enrique Arrondo(*)

Versión de 23 de noviembre de 2021

El objetivo de estas notas es presentar una introducción a las curvas algebraicas planas, es decir, curvas en el plano afín o proyectivo definidas por los ceros de un polinomio. La filosofía general es que, en el plano proyectivo sobre un cuerpo algebraicamente cerrado, las curvas son completas en el sentido de que no les falta ningún punto. Por ejemplo, el Teorema de Bézout permite saber exactamente en cuántos puntos se cortan dos curvas. Se pueden contar otros invariantes (fórmulas de Plücker), como el número de puntos de inflexión o rectas tangentes a la curva desde un punto (generalizando a una curva arbitraria las nociones de recta polar o cónica dual, que se deben haber estudiado para cónicas en Geometría Proyectiva). Aparte de estos resultados globales (que incluyen el estudio de sistemas lineales), necesitaremos estudiar localmente las curvas, decidiendo cuántas veces una curva pasa por un mismo punto, y en qué forma lo hace. En una última sección esbozaremos brevemente cómo se generalizan todos los conceptos y resultados obtenidos cuando estudiamos geometría en dimensión superior, es decir, consideramos ceros de un número arbitrario de polinomios en un espacio de dimensión cualquiera.

(*) Departamento de Álgebra, Geometría y Topología, Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid, 28040 Madrid, arrondo@mat.ucm.es.

1. Ecuaciones implícitas

Empezaremos comparando las diferencias que hay entre el espacio afín y el proyectivo a la hora de definir subconjuntos mediante polinomios. Lo primero que haremos será estudiar si los polinomios definen funciones, y en ambos casos encontraremos ciertos problemas, algunos quizá insospechados.

Observación 1.1. En el caso afín, un polinomio $f \in k[X_1, \ldots, X_n]$ define automáticamente una función (llamada *función polinomial*) $\mathbb{A}_k^n \to k$ y tiene sentido hablar del valor del polinomio y de cuándo se hace o no cero. Podemos tener, sin embargo, el problema de que dos polinomios distintos definan la misma función. Por ejemplo, si p es un número primo, los polinomios $X^pY - 1, XY - 1 \in \mathbb{Z}_p[X, Y]$ definen la misma función en $\mathbb{A}^2_{\mathbb{Z}_p}$ ya que, por el Pequeño Teorema de Fermat, $a^p = a$ para cada $a \in \mathbb{Z}_p$.

Por otra parte, en el espacio proyectivo un polinomio cualquiera no define una función ni puede decirse siquiera cuándo se anula. Por ejemplo, el polinomio $F = X_0^3 - X_1X_2 \in k[X_0, X_1, X_2]$ no puede decirse si se anula o no en el punto $(1 : 1 : 1)$ ya que $(1 : 1 : 1) = (2 : 2 : 2)$ y, mientras que $F(1, 1, 1) = 0$, por otro lado también $F(2, 2, 2) = 4 \neq 0$.

El problema que se presenta en el caso afín se resuelve inmediatamente cuando estemos trabajando en cuerpos infinitos:

Lema 1.2. *Si k es un cuerpo infinito, entonces para todo $f \in k[X_1, \ldots X_n]$ no nulo existe algún $a \in \mathbb{A}_k^n$ tal que $f(a) \neq 0$. Como consecuencia, dos polinomios distintos definen siempre funciones distintas.*

Demostración: Lo demostraremos por inducción sobre n. El caso $n = 1$ es consecuencia de que un polinomio $f \in k[X]$ no nulo tiene siempre un número finito de raíces (como mucho tantas como el grado).

Supongamos pues que el resultado es cierto para polinomios en $n - 1$ variables. Tomamos entonces cualquier polinomio $f \in k[X_1, \ldots X_n]$ no nulo y veamos que existe algún punto en que no se anula. Escribiendo f como polinomio en la variable X_n, lo podemos escribir como

$$f = g_0(X_1, \ldots, X_{n-1}) + g_1(X_1, \ldots, X_{n-1})X_n + \ldots + g_d(X_1, \ldots, X_{n-1})X_n^d$$

con $g_d(X_1, \ldots, X_{n-1}) \neq 0$. Por hipótesis de inducción, existirá $(a_1, \ldots, a_{n-1})$ tal que $g_d(a_1, \ldots, a_{n-1}) \neq 0$. Eso quiere decir que el polinomio

$$f' = g_0(a_1, \ldots, a_{n-1}) + g_1(a_1, \ldots, a_{n-1})X_n + \ldots + g_d(a_1, \ldots, a_{n-1})X_n^d \in k[X_n]$$

es no nulo. Por tanto, ya sabemos que existirá algún $a_n \in k$ que no sea raíz de f'. Entonces, llamando $a = (a_1, \ldots, a_{n-1}, a_n)$ se tendrá $f(a) = f'(a_n) \neq 0$, como queríamos.

La parte final del enunciado es inmediata, ya que si $f, g \in k[X_1, \ldots, X_n]$ son polinomios distintos, entonces $f - g$ es no nulo, por lo que existirá $a \in \mathbb{A}_k^n$ tal que $f(a) - g(a) \neq 0$. Por tanto, las funciones polinomiales definidas por f y g toman distinto valor en el punto a, por lo que son distintas. □

A lo largo de estas notas **supondremos siempre que nuestro cuerpo k es infinito**.

Definición. Una *hipersuperficie algebraica en* $\mathbb{A}_k^n$ es un conjunto de puntos de la forma

$$V(f) := \{(a_1, \ldots, a_n) \in \mathbb{A}_k^n \mid f(a_1, \ldots, a_n) = 0\}$$

donde $f \in k[X_1, \ldots, X_n]$ es un polinomio no constante. Si $n = 2$ diremos que $V(f)$ es una *curva plana afín*, y normalmente indicaremos a las variables X, Y en lugar de X_1, X_2.

Para estudiar el caso proyectivo, necesitaremos la siguiente:

Definición. Se llama *polinomio homogéneo* a un polinomio $F \in k[X_0, \ldots, X_n]$ tal que todos sus monomios tienen el mismo grado.

Lema 1.3. *Sea $F \in k[X_0, \ldots, X_n]$ un polinomio no nulo. Entonces F es homogéneo de grado d si y sólo si $F(TX_0, \ldots, TX_n) = T^d F(X_0, \ldots, X_n)$ en $k[X_0, \ldots, X_n, T]$.*

Demostración: Es claro que, si F es homogéneo de grado d entonces $F(TX_0, \ldots, TX_n) = T^d F$. Recíprocamente, supongamos $F(TX_0, \ldots, TX_n) = T^d F$. Escribimos la descomposición $F = F_0 + F_1 + \ldots + F_r$ en suma de polinomios homogéneos con F_i homogéneo de grado i. Tendremos entonces una igualdad

$$F(TX_0, \ldots, TX_n) = F_0(TX_0, \ldots, TX_n) + F_1(TX_0, \ldots, TX_n) \ldots + F_r(TX_0, \ldots, TX_n)$$

y, usando nuestra hipótesis y el hecho de que ya hemos demostrado la otra implicación obtenemos una igualdad de polinomios $T^d F = F_0 + F_1 T + \ldots + F_r T^r$. Igualando los coeficientes de las potencias de T en cada miembro se obtiene que $F = F_d$ (y también $F_i = 0$ si $i \neq d$), es decir, que F es homogéneo de grado d. □

Recordemos que un polinomio se puede derivar respecto de sus variables, independientemente de que el cuerpo k sea o no $\mathbb{R}$ o $\mathbb{C}$. La expresión de la derivada, así como las propiedades que satisface (regla de Leibniz, regla de la cadena,...) es como en el caso clásico de derivadas de funciones reales o complejas.

Notación. Escribiremos $F_i = \frac{\partial F}{\partial X_i}$. Análogamente $F_{ij} = \frac{\partial^2 F}{\partial X_i \partial X_j}$.

Corolario 1.4 (Identidad de Euler)**.** *Si $F \in k[X_0, \ldots, X_n]$ es un polinomio homogéneo de grado d, entonces $F_0X_0 + \ldots + F_nX_n = dF$.*

Demostración: Derivamos respecto de T en la igualdad $F(TX_0, \ldots, TX_n) = T^dF$ en $k[X_0, \ldots, X_n, T]$ del Lema 1.3. Por la regla de la cadena, tendremos:

$$F_0(TX_0, \ldots, TX_n)X_0 + \ldots + F_n(TX_0, \ldots, TX_n)X_n = dT^{d-1}F$$

Haciendo $T = 1$ obtenemos el resultado. □

Observación 1.5. Obsérvese que, en el Lema 1.3, para que F sea homogéneo, no es suficiente pedir la condición $F(tX_0, \ldots, tX_n) = t^dF(X_0, \ldots, X_n)$ para todo $t \in k$. Por ejemplo, el polinomio $F := X^p + X \in \mathbb{Z}_p[X]$ cumple

$$F(tX) = t^pX^p + tX = tX^p + tX = tF(X)$$

pero no es homogéneo. Sin embargo, si k es infinito, entonces dicha condición ya es suficiente. En efecto, tal condición implica que $F(TX_0, \ldots, TX_n)$ y $T^dF(X_0, \ldots, X_n)$ son polinomios en $k[X_1, \ldots, X_n, T]$ que definen la misma función en $\mathbb{A}_k^{n+1}$, luego por el Lema 1.2 son iguales, y usando entonces el Lema 1.3 se sigue que F es homogéneo de grado d.

El Lema 1.3 nos indica que se puede decir cuándo un polinomio homogéneo en $k[X_0, \ldots, X_n]$ se anula o no en un punto del espacio proyectivo, ya que el anularse no depende del vector escogido para representar al punto. Sin embargo, un polinomio homogéneo sigue sin definir una función en $\mathbb{P}_k^n$. Por ejemplo, no puede indicarse el valor de $F = X_0X_2 - X_1^2$ para el punto $(0 : 1 : 0)$, ya que dicho punto es igual, por ejemplo, al punto $(0 : -3 : 0)$, y se tiene $F(0, 1, 0) = -1 \neq -9 = F(0, -3, 0)$.

Definición. Una *hipersuperficie algebraica en* $\mathbb{P}_k^n$ es un conjunto de puntos de la forma

$$V(F) := \{(a_0 : \ldots : a_n) \in \mathbb{P}_k^n \mid F(a_0, \ldots, a_n) = 0\}$$

donde $F \in k[X_0, \ldots, X_n]$ es un polinomio homogéneo no constante. Si $n = 2$, diremos que $V(F)$ es una *curva proyectiva plana.*

Ejercicio 1.6. Demostrar que los divisores de un polinomio homogéneo son necesariamente polinomios homogéneos.

Ejercicio 1.7. Demostrar que la aplicación $\mathbb{P}_k^1 \to \mathbb{P}_k^2$ definida por $(t_0 : t_1) \mapsto (t_0^2 : t_0t_1 : t_1^2)$ está bien definida y da una biyección entre $\mathbb{P}^1$ y $V(X_0X_2 - X_1^2)$.

Ejercicio 1.8. Demostrar que la aplicación $\mathbb{P}^1_k \to \mathbb{P}^2_k$ definida por $(t_0 : t_1) \mapsto (t_0^3 : t_0 t_1^2 : t_1^3)$ está bien definida y da una biyección entre $\mathbb{P}^1$ y $V(X_0X_2^2 - X_1^3)$.

Ejercicio 1.9. Demostrar que está bien definida la aplicación $\mathbb{P}^1_k \to \mathbb{P}^2_k$ definida por $(t_0 : t_1) \mapsto (t_0^3 : t_0t_1^2 - t_0^3 : t_1^3 - t_0^2t_1)$, que su imagen es $V(X_0X_1^2 - X_0X_2^2 + X_1^3)$ y que sólo un punto de la imagen tiene dos preimágenes distintas.

Recordamos la relación fundamental entre el espacio afín y el proyectivo, que se hace en dos sentidos:

Completación de un espacio afín a uno proyectivo. Dado un espacio afín, lo podemos ver dentro del proyectivo mediante la inclusión

$$\begin{array}{ccc} \mathbb{A}^n_k & \hookrightarrow & \mathbb{P}^n_k \\ (a_1, \ldots, a_n) & \mapsto & (1 : a_1 : \ldots : a_n). \end{array}$$

La imagen de esa inclusión es el complementario del hiperplano $V(X_0)$, llamado *hiperplano del infinito*, y un punto $(0 : a_1 : \ldots : a_n)$ del infinito se ve como la dirección del vector $(a_1, \ldots, a_n)$.

Estudio del espacio proyectivo mediante espacios afines. Es bien sabido que el complementario de un hiperplano en $\mathbb{P}^n_k$ es un espacio afín (por ejemplo, basta tomar coordenadas de forma que el hiperplano sea $V(X_0)$ y aplicar la construcción anterior). Como cada punto de $\mathbb{P}^n_k$ tiene alguna coordenada distinta de cero, nos bastará considerar sólo los hiperplanos de la forma $V(X_i)$; a los conjuntos $U_i := \mathbb{P}^n_k \setminus V(X_i)$ se les suele llamar *abiertos básicos*, y recubren todo $\mathbb{P}^n_k$. Cada U_i se identifica con $\mathbb{A}^n_k$ mediante la inclusión

$$\begin{array}{ccc} \mathbb{A}^n_k & \hookrightarrow & \mathbb{P}^n_k \\ (a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) & \mapsto & (a_0 : \ldots : a_{i-1} : 1 : a_{i+1} \ldots : a_n). \end{array}$$

Con esta identificación, la intersección de una hipersuperficie $V(F) \subset \mathbb{P}^n_k$ con U_i, vista en $\mathbb{A}^n_k$ será $V(f_i)$, donde $f_i(X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n) = F(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n)$. Esto justifica la siguiente:

Definición. Dado un polinomio homogéneo $F \in k[X_0, X_1, \ldots, X_n]$, se llama *deshomogeneizado de F respecto de la variable X_i* al polinomio $F(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n) \in k[X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$.

Podemos plantearnos ahora la situación opuesta, es decir, partimos de una hipersuperficie $V(f) \subset \mathbb{A}^n_k$ y nos preguntamos si existirá alguna $V(F) \subset \mathbb{P}^n_k$ cuya restricción a U_0 (que se identifica con el espacio afín de partida), sea $V(f)$. La respuesta la da el siguiente resultado (todos los resultados que siguen siguen siendo obviamente ciertos si cambiamos la indeterminada respecto de la cual deshomogeneizamos):

Lema 1.10. *Dado $f \in k[X_1, \ldots, X_n]$, de grado d, los polinomios homogéneos cuyo deshomogeneizado es f son de la forma $X_0^l F$, con $l \geq 0$, donde $F := X_0^d f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})$, que es un polinomio homogéneo de grado d no divisible por X_0.*

Demostración: Si el deshomogeneizado de un polinomio homogéneo G de grado d' es f, entonces

$$G(X_0, X_1, \ldots, X_n) = X_0^{d'} G(1, \frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}) = X_0^{d'} f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}).$$

Es claro que $X_0^{d'} f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})$ es un polinomio (y será homogéneo de grado d') si y sólo si $d' \geq d$, de donde se deduce el resultado. □

Definición. Se llama *homogeneizado del polinomio* $f \in k[X_1, \ldots, X_n]$ de grado d al polinomio $F := X_0^d f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})$, donde d es el grado total de f. A la hipersuperficie $V(F)$ se le llama *completado proyectivo de* $V(f)$.

Observación 1.11. El lector agudo habrá notado que, en principio, esta definición no es consistente: una misma hipersuperficie puede estar definida por distintos polinomios, y los correspondientes homogeneizados podrían definir completados proyectivos distintos. Por ejemplo, si tomamos $f = X^4Y + Y^3 \in \mathbb{R}[X, Y]$, su homogeneizado sería $F = X_1^4 X_2 + X_0^2 X_2^3$. Los puntos del infinito de $V(f)$ serían entonces los puntos de $V(F) \cap V(X_0)$, que son $(0 : 1 : 0)$ y $(0 : 0 : 1)$. Sin embargo, como $f = Y(X^4 + Y^2)$ y $X^4 + Y^2$ sólo se anula en $(0, 0)$ (por estar considerando $k = \mathbb{R}$), que es un punto de $V(Y)$, tendremos que $V(f)$ es simplemente la recta $V(Y)$, que sólo tiene un punto en el infinito (el punto $(0 : 1 : 0)$ correspondiente a la dirección horizontal). En realidad, este tipo de problemas no ocurre en cuerpos algebraicamente cerrados, en que la ecuación de una hipersuperficie es única salvo multiplicación por constante. Demostraremos esto, en el caso de curvas, en el Corolario 2.12.

Notación. En general, para saber si estamos en el caso homogéneo o no, escribiremos letras mayúsculas para los polinomios en $k[X_0, \ldots, X_n]$, y minúsculas para los polinomios en $k[X_1, \ldots, X_n]$.

Obsérvese que, como evidencia el Lema 1.10, muchos polinomios homogéneos (y como mucho uno irreducible) tienen el mismo deshomogeneizado. En particular, el que el deshomogeneizado de un polinomio homogéneo sea irreducible no implica que dicho polinomio homogéneo sea irreducible también. Esto sólo ocurrirá si el polinomio homogéneo es el "más pequeño" de entre los que tienen el mismo deshomogeneizado (es decir, si el polinomio es un polinomio homogeneizado). Dicho de forma más precisa, tenemos el siguiente resultado:

Lema 1.12. *Sea $f \in k[X_1, \ldots, X_n]$ y F su homogeneizado. Se tiene:*

(i) Si $f = f_1 f_2$, entonces $F = F_1 F_2$, donde cada F_i es el homogeneizado de f_i.

(ii) Si $F = F_1 F_2$, entonces $f = f_1 f_2$, y cada F_i es el homogeneizado de f_i.

(iii) f es irreducible si y sólo si F es irreducible.

(iv) $f = f_1^{m_1} \ldots f_s^{m_r}$ es la descomposición en factores irreducibles de f si y sólo si $F = F_1^{m_1} \ldots F_r^{m_r}$ es la descomposición en factores irreducibles de F, donde cada F_i es el homogeneizado de f_i.

(v) Si g es otro polinomio, y su homogeneizado es G, entonces f y g son primos entre sí si y sólo si F y G son primos entre sí.

Demostración: Veamos primero (i). Si $f = f_1 f_2$, entonces $\deg(f) = \deg(f_1) + \deg(f_2)$. Entonces tendremos

$$F = X_0^{\deg(f)} f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}) = X_0^{\deg(f_1)} f_1(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}) X_0^{\deg(f_2)} f_2(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}) = F_1 F_2.$$

Para demostrar (ii), si $F = F_1 F_2$ con F_1, F_2 de grados respectivos d_1 y d_2, entonces, deshomogeneizando,

$$f = F(1, X_1, \ldots, X_n) = F_1(1, X_1, \ldots, X_n) F_2(1, X_1, \ldots, X_n).$$

Como el grado de cada $F_i(1, X_1, \ldots, X_n)$ es como mucho d_i y la suma de los grados es $\deg(f) = \deg(F) = d_1 + d_2$ (por ser $F = F_1 F_2$), se sigue que cada $F_i(1, X_1, \ldots, X_n)$ tiene grado precisamente d_i, luego su homogeneizado es F_i.

Veamos ahora (iii). Supongamos que f sea irreducible de grado d. Entonces no puede ser $F = F_1 F_2$ con F_1, F_2 de grado estrictamente positivo, ya que (ii) implicaría que f sería reducible (ya que f_1, f_2 también tendrían grado positivo). De la misma forma, si F es irreducible, por (i) se tiene que f no puede ser reducible.

La primera implicación de la parte (iv) es consecuencia de (iii) y de aplicar (i) recursivamente. La otra implicacin es consecuencia de (iii) y de aplicar (ii) recursivamente.

Finalmente, la parte (v) es consecuencia de (iv), puesto que las descomposiciones en irreducibles de F y G vienen de las de f y g, es claro que F y G tendrán un factor común si y sólo si ya lo tenían f y g. □

Una primera aplicación del resultado anterior, tomando $n = 1$, es que los polinomios homogéneos en dos variables funcionan como los polinomios en una variable. Aunque ya desarrollaremos esto aún más en la sección 4, veamos a continuación, un primer ejemplo de este hecho.

Teorema 1.13. *Si $F \in k[X_0, X_1]$ es un polinomio homogéneo no nulo de grado d, entonces:*

(i) $(a_0 : a_1) \in V(F)$ *si y sólo si* $a_1X_0 - a_0X_1$ *divide a* F.

(ii) $V(F)$ *consiste en como mucho* d *puntos.*

(iii) Si k *es algebraicamente cerrado,* F *factoriza en factores lineales.*

Demostración: Escribimos $F = X_0^r F'$, donde F' no es divisible por X_0 (es decir, el coeficiente de X_1^{d-r} en F' es distinto de cero). Entonces, el resultado es evidente para $(a_0 : a_1) = (0 : 1)$, ya que $F(0, 1) = 0$ si y sólo si $r > 0$. Si suponemos ahora $a_0 \neq 0$, entonces $F(a_0, a_1) = 0$ si y sólo si $F'(a_0, a_1) = 0$, es decir, si y sólo si $F'(1, \frac{a_1}{a_0}) = 0$. Eso es equivalente a que $\frac{a_1}{a_0}$ sea una raíz del deshomogeneizado de F', y por la regla de Ruffini eso es equivalente a que $X_1 - \frac{a_1}{a_0}$ divida a tal deshomogeneizado. Usando el Lema 1.12(i), concluimos que es equivalente a que $X_1 - \frac{a_1}{a_0}X_0$ divida a F'. Como $X_1 - \frac{a_1}{a_0}X_0$ es primo con X_0, eso es equivalente a que $X_1 - \frac{a_1}{a_0}X_0$ (o equivalentemente $a_1X_0 - a_0X_1$) divida a F. Esto demuestra (i).

La parte (ii) es ahora una consecuencia inmediata de que F admite como mucho d factores lineales, y la parte (iii) se obtiene porque el deshomogeneizado de F' factoriza en factores lineales, y podemos aplicar el Lema 1.12(iv). □

Observación 1.14. Usemos el Teorema 1.13 para convencernos de que tiene que existir un Teorema de Bézout. Lo haremos en varios pasos:

1) En primer lugar, si tenemos una curva $C = V(F)$ definida por un polinomio homogéneo $F \in k[X_0, X_1, X_2]$ de grado d, veamos cuál es su intersección con una recta (esto que vamos a hacer serviría lo mismo para una hipersuperficie). Como una recta proyectiva se puede parametrizar, podemos escribir cualquier recta de la forma

$$L = \{\big((A_0(t_0, t_1) : A_1(t_0, t_1) : A_2(t_0, t_1)\big) \mid (t_0 : t_1) \in \mathbb{P}^1_k\}$$

donde $A_0, A_1, A_2 \in k[T_0, T_1]$ son polinomios homogéneos de grado uno. Los puntos de intersección de C y L vendrán dados entonces por los valores $(t_0 : t_1)$ tales que $F(A_0(t_0, t_1), A_1(t_0, t_1), A_2(t_0, t_1)) = 0$, es decir, los puntos de $V(P) \in \mathbb{P}^1_k$, donde $P := F(A_0(T_0, T_1), A_1(T_0, T_1), A_2(T_0, T_1)) \in k[T_0, T_1]$, que es un polinomio homogéneo de grado d (salvo que sea cero, en cuyo caso $L \subset C$). Por el Teorema 1.13, si k es algebraicamente cerrado, el conjunto $V(P)$ consistirá en d puntos, contados con multiplicidad.

2) Supongamos que tenemos ahora un conjunto

$$D = \{\big(A_0(t_0, t_1) : A_1(t_0, t_1) : A_2(t_0, t_1)\big) \mid (t_0 : t_1) \in \mathbb{P}^1_k\}$$

donde esta vez $A_0, A_1, A_2 \in k[T_0, T_1]$ son polinomios homogéneos de grado arbitrario e. Aunque en la sección 4 veremos que D es una curva, hay una forma de intuirlo a priori, que es cortando con una recta L. Como ahora es D lo que tenemos parametrizado, nos convendrá tener L en implícitas (en general, para calcular una intersección de dos objetos, conviene tener uno parametrizado y el otro en implícitas). Sea entonces $u_0X_0+u_1X_1+u_2X_2$ una ecuación de L. Entonces, la intersección de D y L se obtendrá ahora estudiando los puntos $(t_0 : t_1) \in \mathbb{P}^1_k$ tales que $u_0A_0(t_0, t_1) + u_1A_1(t_0, t_1) + u_2A_2(t_0, t_1) = 0$. Como el polinomio $u_0A_0(T_0, T_1) + u_1A_1(T_0, T_1) + u_2A_2(T_0, T_1)$ es homogéneo de grado e (salvo que sea cero, que ocurre cuando $D \subset L$), obtenemos, si k es algebraicamente cerrado, e soluciones contadas con multiplicidad. Esto hace sospechar que D sea una curva definida por un polinomio de grado e.

3) Finalmente, intersequemos los conjuntos C y D de 1) y 2). Los puntos de intersección vendrán dados por las soluciones $(t_0 : t_1) \in \mathbb{P}^1_k$ del polinomio homogéneo $F(A_0(T_0, T_1), A_1(T_0, T_1), A_2(T_0, T_1)) \in k[T_0, T_1]$, que ahora tiene grado *de* (salvo que sea cero, en cuyo caso $D \subset C$). Por tanto, en el caso en que k sea algebraicamente cerrado, obtendremos *de* puntos contados con multiplicidad. Hay dos problemas principales para poder concluir de aquí. El primero es que no toda curva se puede parametrizar como en 2) (de hecho, es muy raro que una curva se pueda parametrizar; ya lo discutiremos en la sección 9). El segundo es que, aunque así fuera, habría que demostrar que la multiplicidad de intersección no depende de la parametrización escogida. En la sección siguiente ya veremos un modo para calcular la intersección de dos curvas en implícitas, pero seguiremos teniendo el problema de ver que la multiplicidad con la que salen los puntos de intersección está bien definida.

Vamos a centrarnos de nuevo en el estudio de polinomios que sean ecuaciones implícitas de curvas. Empecemos notando que, en principio, una definición general de curva puede presentar aún anomalías.

Ejemplo 1.15. En la Observación 1.1 vimos que un polinomio, por ejemplo $X^pY - XY \in \mathbb{Z}_p[X, Y]$ puede anularse en todos los puntos, lo que haría que la curva que define es todo el plano afín (el Lema 1.2 excluye tal posibilidad si el cuerpo es infinito). Se puede dar sin embargo el caso opuesto, que una curva sea un conjunto muy pequeño, por ejemplo en $\mathbb{A}^2_{\mathbb{R}}$ la curva $V(X^2 + Y^2)$ es un solo punto y $V(X^2 + Y^2 + 1)$ es el conjunto vacío. Además, esto nos crea también el problema de que ecuaciones bien distintas dan lugar a la misma curva, ya que, por ejemplo, $V(X(X^2 + Y^2 + 1)) = V(X)$.

El lector habrá notado que para encontrar estos ejemplos hemos tenido que usar un cuerpo como $\mathbb{R}$ que no es algebraicamente cerrado. Veamos que, en efecto, ese problema no se da para cuerpos algebraicamente cerrados. Empezamos con un primer resultado que

necesitaremos y que nos indica en particular que (por el Lema 1.2) para estos cuerpos tampoco tenemos el problema de curvas o hipersuperficies que sean todo el espacio:

Lema 1.16. *Todo cuerpo algebraicamente cerrado es infinito.*

Demostración: En efecto, veamos que un cuerpo finito k no puede ser nunca algebraicamente cerrado. En efecto, si $a_1, \dots a_m$ son los elementos de k, entonces es claro que $f(X) = (X - a_1) \dots (X - a_m) + 1$ no puede tener ninguna raíz en k, por lo que k no es algebraicamente cerrado.

En realidad, si el lector sabe un mínimo de teoría de cuerpos finitos sabrá que, si k es un cuerpo finito, su cardinal es p^n, una potencia de un número primo, y que el polinomio de la demostración no es más que $f(X) = X^{p^n} - X + 1$. □

Proposición 1.17. *Si k es algebraicamente cerrado y $f \in k[X, Y]$ es un polinomio no constante, entonces $V(f)$ es un conjunto infinito (y propio) de puntos.*

Demostración: Que $V(f)$ sea un subconjunto propio de $\mathbb{A}^2_k$ es una consecuencia de los Lemas 1.2 y 1.16. Para ver la infinitud, observamos primero que, como f es no constante, dependerá de alguna de las variables, por ejemplo de Y. Entonces, podemos escribir

$$f = f_0(X) + f_1(X)Y + \dots + f_d(X)Y^d$$

donde $f_0, \dots, f_d \in k[X]$, $f_d \neq 0$ y $d > 0$. Como f_d tiene un número finito de raíces, al ser k infinito (por el Lema 1.16), existen infinitos valores $a \in k$ tales que $f_d(a) \neq 0$. Para cada uno de esos valores, el polinomio $f(a, Y) \in k[Y]$ tiene grado $d > 0$, luego tiene al menos una raíz $b \in k$, luego $(a, b) \in V(f)$. Al variar a, obtenemos infinitos puntos de $V(f)$. □

Corolario 1.18. *Si k es algebraicamente cerrado y $F \in k[X_0, X_1, X_2]$ es un polinomio no constante, entonces $V(F)$ es un conjunto infinito (y propio) de puntos.*

Demostración: Como F es no constante, su deshomogeneizado respecto de alguna variable es no constante, luego su intersección con algún plano afín es infinita, por la Proposición 1.17. Que $V(F)$ sea propio se obtiene del Lema 1.2, ya que si $V(F) = \mathbb{P}^2_k$, entonces F se anularía en todos los puntos de $\mathbb{A}^3_k$. □

2. Intersección de curvas. Lema de Study

Ahora que hemos fijado las condiciones para que una curva sea un conjunto propio con infinitos puntos, veamos que, en las mismas condiciones, la intersección de dos curvas, sin embargo, es en general un número finito de puntos. Lo idóneo (como muestra la Observación 1.14) sería tener una curva parametrizada. Como eso no es siempre posible, hay que ver cómo intersecar dos curvas dadas mediante sus ecuaciones implícitas. La técnica clave para esto es el uso de la resultante de dos polinomios, que recordamos brevemente aquí (quien no haya visto antes este concepto, puede entenderlo mirando el caso homogéneo en el Teorema 4.7):

Definición. Dado un dominio de factorización única A, se llama *resultante de los polinomios* $f = a_0 + a_1X + \ldots + a_nX^n$ (con $a_n \neq 0$) y $g = b_0 + b_1X + \ldots + b_mX^m$ (con $b_m \neq 0$) de $A[X]$ al elemento

$$\operatorname{res}(f,g) = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & 0 & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{n-1} & a_n & 0 & \ldots & 0 \\ & & \ddots & & & & & \\ 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_{n-1} & a_n \\ b_0 & b_1 & \ldots & b_{m-1} & b_m & 0 & \ldots & 0 \\ 0 & b_0 & \ldots & b_{m-2} & b_{m-1} & b_m & 0\ldots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_{m-1} & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ filas} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ filas} \end{matrix}$$

La utilidad de la resultante es el siguiente resultado que nos limitamos a recordar (una demostración en el caso homogéneo, que es idéntica a la que se hace en el caso clásico, se puede ver en el Teorema 4.7):

Teorema 2.1. *Sea A un dominio de factorización única y sean $f = a_0 + a_1X + \ldots + a_nX^n$, $g = b_0 + b_1X + \ldots + b_mX^m$ dos polinomios en $A[X]$ de grados respectivos n y m (es decir, $a_n, b_m \neq 0$). Entonces f y g tienen un factor común de grado positivo si y sólo si* $\operatorname{res}(f,g) = 0$.

La resultante tiene otras propiedades que necesitaremos, y que recordamos en forma de ejercicio:

Ejercicio 2.2. Sea A un D.F.U., sea $A' = A[X'_1, \ldots, X'_n, X''_1, \ldots, X''_m]$ y sean los polinomios $f = (X - X'_1)\ldots(X - X'_n)$ y $g = (X - X''_1)\ldots(X - X''_m)$ de $A'[X]$. Demostrar que

$$\operatorname{res}(f,g) = \prod_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} (X''_j - X'_i)$$

[Indicación, ver que $\mathrm{res}(f,g)$ es divisible por todos los polinomios $X_j'' - X_i'$ y comparar grados y coeficiente de mayor grado como polinomios en $X_1', \ldots, X_n']$. Concluir de lo anterior que, si A es un D.F.U. y $f, g \in A[X]$ tienen grados respectivos n y m, y además g es mónico y tiene raíces $\beta_1, \ldots, \beta_m$ (cada una repetida tantas veces como su multiplicidad), entonces $\mathrm{res}(f,g) = f(\beta_1) \ldots f(\beta_m)$.

Una primera aplicación inmediata de la resultante es para pasar de paramétricas a implícitas en curvas afines:

Proposición 2.3. *Sea k un cuerpo algebraicamente cerrado. Entonces, dados dos polinomios no constantes $p, q \in k[T]$, el conjunto de puntos $C = \{(p(t), q(t)) \in \mathbb{A}_k^2 \mid t \in k\}$ es una curva afín.*

Demostración: Un punto (a,b) está en C si y sólo si los polinomios $p(T) - a$ y $q(T) - b$ tienen alguna raíz común. Como k es algebraicamente cerrado, esto es equivalente a que tengan algún factor común de grado positivo. Por tanto, por el Teorema 2.1, esto es equivalente a que se anule $\mathrm{res}(p(T) - a, q(T) - b)$. Es inmediato observar (por ser p, q de grado positivo) que, si llamamos $f(X,Y) := \mathrm{res}_T(p(T) - X, q(T) - Y)$, entonces $f(a,b) = \mathrm{res}(p(T) - a, q(T) - b)$ para todo $(a,b) \in \mathbb{A}_k^2$. De todo lo anterior se deduce $C = V(f)$. □

Observación 2.4. Uno de los dos polinomios p, q podría ser constante, en cuyo caso también obtendríamos una recta (horizontal o vertical). Nótese que es fundamental que el cuerpo sea algebraicamente cerrado, ya que, por ejemplo, el conjunto $C = \{(t^2, t^2) \in \mathbb{A}_{\mathbb{R}}^2 \mid t \in \mathbb{R}\}$ es una semirrecta, que no es una curva afín. El hecho de que una semirrecta no sea una curva afín, aunque parece intuitivo, requiere una demostración sofisticada. Para demostrarlo, necesitaremos la Proposición 2.6, ya que si $C = V(f)$, está claro que f no puede ser un múltiplo de $g = X - Y$ (puesto que entonces C contendría a toda la recta). Como $V(f) \cap V(g)$ es infinito (es toda la semirrecta), entramos en contradicción con la Proposición 2.6.

Ejemplo 2.5. Cuando la parametrización no es polinomial sino racional (es decir, dada por cocientes de polinomios) aparecen algunos problemas. Por ejemplo, si consideramos el conjunto

$$C = \left\{ \left(\frac{t}{t+1}, \frac{t}{t-1} \right) \mid t \in k \setminus \{-1, 1\} \right\}$$

que un punto (a,b) esté en C es equivalente a que los polinomios $T - a(T+1)$ y $T - b(T-1)$ tengan una raíz común. Sin embargo, mientras que

$$f(X,Y) := \mathrm{res}_T(T - X(T+1), T - Y(T-1)) = \begin{vmatrix} -X & 1-X \\ Y & 1-Y \end{vmatrix} = -X - Y + 2XY,$$

no es cierto que, por ejemplo, $f(1,1)$ sea la resultante de $T-1(T+1)$ y $T-1(T-1)$, ya que en realidad ambos polinomios son constantes (incluso ya sólo $a=1$ o $b=1$ daría problemas). En realidad, lo que ocurre en este caso es que $C \subset V(f)$, pero el contenido es estricto, ya que el punto $(1,1) \in V(f)$ sólo se obtendría haciendo tender t a infinito. En realidad, veremos en la sección 4 que, completando con los puntos del infinito, las cosas ya funcionan bien.

Otra aplicación de la resultante, que de nuevo desarrollaremos más en el caso proyectivo porque allí funciona mejor, es el cálculo de los puntos de intersección de curvas:

Proposición 2.6. *Sean $f, g \in k[X,Y]$ dos polinomios. Entonces, si (a,b) es un punto de $V(f) \cap V(g)$, la coordenada a es una raíz de $res_Y(f,g)$ y la coordenada b es una raíz de $res_X(f,g)$. En particular, si f y g no tienen factores comunes, $V(f) \cap V(g)$ es un conjunto finito.*

Demostración: La última parte es obvia, porque la coprimalidad de f y g implica que $res_Y(f,g)$ y $res_X(f,g)$ son polinomios no nulos, y por tanto tienen un número finito de raíces. Las dos primeras partes son simétricas, así que bastará demostrar que a es una raíz de $res_Y(f,g)$.

Escribimos primero

$$f = f_0(X) + f_1(X)Y + \ldots + f_d(X)Y^d$$

$$g = g_0(X) + g_1(X)Y + \ldots + g_e(X)Y^e$$

con $f_i(X),\ g_j(X) \in k[X]$ para $i = 0,1,\ldots,d$, $j = 0,1,\ldots,e$ y $f_d(X) \neq 0$, $g_e(X) \neq 0$. Tenemos entonces que $r(X) := res_Y(f,g)$ tiene la forma

$$r(X) = \begin{vmatrix} f_0(X) & f_1(X) & \ldots & f_d(X) & 0 & 0 & \ldots & 0 \\ 0 & f_0(X) & \ldots & f_{d-1}(X) & f_d(X) & 0 & \ldots & 0 \\ & & \ddots & & & & & \\ 0 & \ldots & 0 & f_0(X) & f_1(X) & \ldots & f_{d-1}(X) & f_d(X) \\ g_0(X) & g_1(X) & \ldots & g_{e-1}(X) & g_e(X) & 0 & \ldots & 0 \\ 0 & g_0(X) & \ldots & g_{e-2} & g_{e-1}(X) & g_e(X) & 0\ldots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \ldots & 0 & g_0(X) & g_1(X) & \ldots & g_{e-1}(X) & g_e(X) \end{vmatrix}$$

Observamos que, si $(a,b) \in V(f) \cap V(g)$; entonces b es una raíz común de los polinomios $\tilde{f}(Y) := f(a,Y)$ y $\tilde{g}(Y) := g(a,Y)$, luego su resultante es cero. Si $f_d(a) \neq 0$ y $g_e(a) \neq 0$, los polinomios $\tilde{f}$ y $\tilde{g}$ tienen grados respectivos d y e, luego su resultante es $r(a)$, y por tanto a es una raíz de $res_Y(f,g)$.

Si en cambio $f(a,Y)$ tiene grado $d' < d$, i.e. $f_{d'+1}(a) = f_{d'+2}(a) = \ldots = f_d(a) = 0$ pero $g(a,Y)$ tiene grado e, i.e. $g_e(a) \neq 0$, entonces $r(a) = g_e(a)^{d-d'} res(\tilde{f}, \tilde{g}) = 0$. El mismo argumento se puede hacer si $f_d(a) \neq 0$ y $g_e(a) = 0$. Finalmente, si $f_d(a) = g_e(a) = 0$, no hay nada que probar, ya que directamente $r(a) = 0$. □

Observación 2.7. Como en el Ejemplo 2.5, se tiene el problema de que no es lo mismo calcular la resultante respecto de una indeterminada y luego sustituir la otras determinadas que hacer primero la sustitución y luego la resultante. En concreto, hemos visto que en la demostración de la proposición anterior que sólo tendremos problema a cuando ambos polinomios bajan de grado al sustituir. Por ejemplo, los polinomios $f = XY + 1$ y $g = XY - 1$ representan dos curvas planas afines sin puntos de intersección. Sin embargo,

$$\mathrm{res}_Y(f,g) = \begin{vmatrix} 1 & X \\ -1 & X \end{vmatrix} = 2X,$$

tiene como raíz $X = 0$. En realidad, aunque las dos curvas no tengan intersección en la recta afín $X = 0$, sí que se cortan en el punto del infinito de dicha recta. Esto indica de nuevo que la resultante funciona mejor en el caso proyectivo.

Pasemos por tanto al caso proyectivo, en que será además más fácil precisar mejor el número de puntos de interescción que esperamos. Recordemos que surgen problemas cuando tenemos un polinomio que, a pesar de tener cierto grado en una indeterminada, su grado baja al dar a las otras indeterminadas algún valor concreto. En el caso homogéneo, el modo de evitar esto es considerar polinomios cuyo coeficiente respecto de la variable que queremos, por ejemplo X_2, es distinto de cero. Esto es equivalente a decir que el punto $(0:0:1)$ no está en la curva definida por dicho polinomio. El resultado siguiente va a ser la clave en esta dirección.

Teorema 2.8. *Sean $F, G \in k[X_0, X_1, X_2]$ dos polinomios homogéneos primos entre sí y tales que $(0:0:1) \notin V(FG)$. Entonces, la resultante de F y G como polinomios en X_2 es un polinomio homogéneo en $k[X_0, X_1]$ de grado $\deg(F)\deg(G)$.*

Demostración: Podemos escribir

$$F = A_d(X_0, X_1) + A_{d-1}(X_0, X_1)X_2 + \ldots + A_1(X_0, X_1)X_2^{d-1} + A_0(X_0, X_1)X_2^d$$

$$G = B_e(X_0, X_1) + B_{e-1}(X_0, X_1)X_2 + \ldots + B_1(X_0, X_1)X_2^{e-1} + B_0(X_0, X_1)X_2^e$$

donde cada A_i, B_i es homogéneo de grado i. Nótese que la condición $(0:0:1) \notin V(FG)$ es equivalente a que $A_0(X_0, X_1), B_0(X_0, X_1)$ (que en realidad son constantes) son ambos no nulos. Por tanto, F y G tienen grados respectivos d y e como polinomios en la

indeterminada X_2, luego su resultante es

$$R(X_0,X_1)=\left|\begin{array}{cccccccc} A_d & A_{d-1} & \dots & A_0 & 0 & 0 & \dots & 0 \\ 0 & A_d & \dots & A_1 & A_0 & 0 & \dots & 0 \\ & & \ddots & & & & & \\ 0 & \dots & 0 & A_d & A_{d-1} & \dots & A_1 & A_0 \\ B_e & B_{e-1} & \dots & B_1 & B_0 & 0 & \dots & 0 \\ 0 & B_e & \dots & B_2 & B_1 & B_0 & 0\dots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \dots & 0 & B_e & B_{e-1} & \dots & B_1 & B_0 \end{array}\right| \begin{array}{l} \left.\begin{array}{l}\\\\\\\end{array}\right\} e \text{ filas} \\ \left.\begin{array}{l}\\\\\\\end{array}\right\} d \text{ filas} \end{array}$$

Para ver que es homogéneo de grado de aplicaremos el Lema 1.3 (nótese que R es no nulo puesto que F y G no tienen factores comunes). Observamos que se tiene

$$R(TX_0,TX_1)=\left|\begin{array}{cccccccc} T^dA_d & T^{d-1}A_{d-1} & \dots & A_0 & 0 & 0 & \dots & 0 \\ 0 & T^dA_d & \dots & TA_1 & A_0 & 0 & \dots & 0 \\ & & \ddots & & & & & \\ 0 & \dots & 0 & T^dA_d & T^{d-1}A_{d-1} & \dots & TA_1 & A_0 \\ T^eB_e & T^{e-1}B_{e-1} & \dots & TB_1 & B_0 & 0 & \dots & 0 \\ 0 & T^eB_e & \dots & T^2B_2 & TB_1 & B_0 & 0\dots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \dots & 0 & T^eB_e & T^{e-1}B_{e-1} & \dots & TB_1 & B_0 \end{array}\right| \begin{array}{l} \left.\begin{array}{l}\\\\\\\end{array}\right\} e \text{ filas} \\ \left.\begin{array}{l}\\\\\\\end{array}\right\} d \text{ filas} \end{array}$$

Efectuamos ahora la siguiente operación en la matriz del determinante anterior: dejamos la última fila igual, la penúltima la multiplicamos por T, la antepenúltima por T^2, y así sucesivamente hasta la fila $e+1$, que la multiplicamos por T^{d-1}; a continuación, repetimos el mismo proceso a partir de la fila e-ésima, que dejamos igual, la anterior la multiplicamos por T, la anterior por T^2, y así hasta la fila primera que la multiplicamos por T^{e-1}. Obtenemos entonces:

$$T^{1+2+\dots+(d-1)}T^{1+2+\dots+(e-1)}R(TX_0,TX_1)=$$

$$=\left|\begin{array}{cccccccc} T^{d+e-1}A_d & T^{d+e-2}A_{d-1} & \dots & T^{e-1}A_0 & 0 & 0 & \dots & 0 \\ 0 & T^{d+e-2}A_d & \dots & T^{e-1}A_1 & T^{e-2}A_0 & 0 & \dots & 0 \\ & & \ddots & & & & & \\ 0 & \dots & 0 & T^dA_d & T^{d-1}A_{d-1} & \dots & TA_1 & A_0 \\ T^{d+e-1}B_e & T^{d+e-2}B_{e-1} & \dots & T^dB_1 & T^{d-1}B_0 & 0 & \dots & 0 \\ 0 & T^{d+e-2}B_e & \dots & T^dB_2 & T^{d-1}B_1 & T^{d-2}B_0 & 0\dots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \dots & 0 & T^eB_e & T^{e-1}B_{e-1} & \dots & TB_1 & B_0 \end{array}\right| \begin{array}{l} \left.\begin{array}{l}\\\\\\\end{array}\right\} e \text{ filas} \\ \left.\begin{array}{l}\\\\\\\end{array}\right\} d \text{ filas} \end{array}$$

Tenemos entonces que de la última columna no podemos sacar nada, de la penúltima podemos sacar T, de la antepenúltima T^2, y así sucesivamente hasta la primera, que podemos

sacar T^{d+e-1}, y nos queda entonces el determinante que define $R(X_0, X_1)$. Tendremos por tanto

$$T^{1+2+\ldots+(d-1)}T^{1+2+\ldots+(e-1)}R(TX_0, TX_1) = T^{1+2+\ldots+(d+e-1)}R(X_0, X_1)$$

es decir

$$T^{\frac{d^2-d+e^2-e}{2}}R(TX_0, TX_1) = T^{\frac{d^2+2de+e^2-d-e}{2}}R(X_0, X_1)$$

de donde se deduce $R(TX_0, TX_1) = T^{de}R(X_0, X_1)$, y por el Lema 1.3 se sigue que R es homogéneo de grado de, como queríamos demostrar. □

Corolario 2.9 (Teorema débil de Bézout)**.** *Sean $F, G \in k[X_0, X_1, X_2]$ dos polinomios homogéneos primos entre sí de grados respectivos d y e. Entonces, si k es infinito, $V(F) \cap V(G)$ consiste como mucho en de puntos.*

Demostración: Veamos en primer lugar que $V(F) \cap V(G)$ es finito. Para ello, escogemos coordenadas de forma que el punto $(0 : 0 : 1)$ no esté en ninguna de las dos curvas (es algo que podemos hacer porque, al ser k infinito, $V(FG)$ no es todo $\mathbb{P}^2_k$, por el Corolario 1.18). Observamos que si $(a_0 : a_1 : a_2) \in V(F) \cap V(G)$ entonces los polinomios $f(X_2) := F(a_0, a_1, X_2)$ y $g(X_2) := G(a_0, a_1, X_2)$ tienen a_2 como raíz común, luego $\text{res}(f, g) = 0$. Como $(0 : 0 : 1)$ no está ni en $V(F)$ ni en $V(G)$, entonces F tiene un término en X_2^d y G tiene un término en X_2^e, luego $\deg(f) = d$ y $\deg(g) = e$. Esto quiere decir que la resultante de f y g es un determinante de orden $d + e$, precisamente el que se obtiene sustituyendo $X_0 = a_0$ y $X_1 = a_1$ en la resultante $R := \text{res}_{X_2}(F, G)$ de F y G como polinomios en X_2. En otras palabras, si $(a_0 : a_1 : a_2) \in V(F) \cap V(G)$, entonces $(a_0 : a_1)$ (que tiene sentido ya que $(0 : 0 : 1)$ no está en la intersección de las curvas) es una raíz de $R \in k[X_0, X_1]$, que es homogéneo por el Teorema 2.8. Por el Teorema 1.13, hay una cantidad finita de posibilidades para $(a_0 : a_1)$. Para cada una de dichas posibilidades, los posibles valores de a_2 están entre las raíces de $f(X_2) := F(a_0, a_1, X_2)$, que de nuevo es una cantidad finita por ser f no nulo. Esto concluye que el número de puntos de $V(F) \cap V(G)$ es finito.

Para acotar el número de puntos refinamos un poco más la demostración anterior, pero usando fuertemente que ya sabemos que $V(F)$ y $V(G)$ se cortan en un número finito de puntos, que llamaremos $p_1, \ldots, p_r$. Entonces, tenemos un número finito de pares de puntos p_i, p_j de la intersección, y denotaremos L_{ij} a una ecuación de la recta que pasa por p_i, p_j. Por tanto, podemos tomar coordenadas de forma que $(0 : 0 : 1)$ no esté ni en $V(F)$, ni en $V(G)$ ni en ninguna de las rectas $V(L_{ij})$, ya que $V(FG\prod_{i,j} L_{ij})$ no es todo $\mathbb{P}^2_k$ por el Corolario 1.18. Entonces, repitiendo la demostración anterior, nos volvemos a encontrar con una cantidad finita de posibilidades $(a_0 : a_1)$, de hecho como mucho de, aplicando el Teorema 1.13 y el hecho de que R tiene grado de por el Teorema 2.8. La diferencia ahora es que sabemos que, para cada uno de los $(a_0 : a_1)$, los posibles puntos

$(a_0 : a_1 : a_2) \in V(F) \cap V(G)$ están en la recta $V(a_1X_0 - a_0X_1)$, que pasa por $(0 : 0 : 1)$, luego contiene como mucho un punto de intersección. □

En realidad, en la demostración anterior hemos visto mucho más: que, si el cuerpo k es algebraicamente cerrado, se obtienen exactamente *de* puntos de intersección, aunque cada uno de ellos contado con cierta "multiplicidad". El problema es que, a priori, esta "multiplicidad" de cada punto de intersección podría depender de la elección de coordenadas que tomemos. Si no dependiera, obtendríamos lo que se conoce como el Teorema de Bézout. De hecho, las siguientes secciones irán encaminadas a definir con precisión la noción de multiplicidad de intersección, que coincidirá con la que aparece en la demostración anterior.

Los resultados anteriores tienen su aplicación a la hora de determinar una ecuación natural para una curva:

Teorema 2.10 (Lema de Study)**.** *Sea $f \in k[X, Y]$ un polinomio irreducible tal que $V(f)$ tiene infinitos puntos. Entonces, para todo $g \in k[X, Y]$ se tiene que $V(f) \subset V(g)$ si y sólo si f divide a g.*

Demostración: Es evidente que, si f divide a g, entonces $V(f) \subset V(g)$, así que basta demostrar la otra implicación. Si ocurre $V(f) \subset V(g)$, entonces se tiene que $V(f) \cap V(g)$ es un conjunto infinito de puntos. Por la Proposición 2.6, f y g tienen algún factor común. Como f es irreducible, se sigue que f divide a g. □

La misma demostración prueba:

Teorema 2.11 (Lema de Study proyectivo)**.** *Sea $F \in k[X_0, X_1, X_2]$ un polinomio homogéneo irreducible tal que $V(F)$ tiene infinitos puntos. Entonces, para todo polinomio homogéneo $G \in k[X_0, X_1, X_2]$ se tiene que $V(F) \subset V(G)$ si y sólo si F divide a G.* □

Corolario 2.12 (Teorema de los Ceros de Hilbert)**.** *Si k es algebraicamente cerrado, y $f \in k[X, Y]$ es un polinomio de grado positivo cuya factorización en factores irreducibles es $f = f_1^{m_1} \dots f_r^{m_r}$, entonces son equivalentes:*

(i) $V(f) \subset V(g)$

(ii) $f_1 \dots f_r$ *divide a* g

(iii) Existe $m \in \mathbb{N}$ *tal que* $f | g^m$.

En particular, $V(f) = V(g)$ si y sólo si f y g tienen los mismos factores irreducibles.

Demostración: Demostraremos cíclicamente las implicaciones:

$(i) \Rightarrow (ii)$: Como k es algebraicamente cerrado, entonces por la Proposición 1.17, cada $V(f_i)$ es infinito. Entonces, como $V(f) \subset V(g)$, se tiene también $V(f_i) \subset V(g)$, y por el

Lema de Study, cada f_i divide a g. Como los f_i son primos dos a dos, se sigue que $f_1 \dots f_r$ divide a g.

$(ii) \Rightarrow (iii)$: Basta tomar $m = \text{máx}\{m_1, \dots, m_r\}$.

$(iii) \Rightarrow (i)$: De $f|g^m$ obtenemos $V(f) \subset V(g^m)$, y el resultado sigue de la igualdad $V(g^m) = V(g)$.

Finalmente, si $V(f) = V(g)$ y la factorización en factores irreducibles de g es $g = g_1^{n_1} \dots g_s^{n_s}$, por (ii) tendremos que cada f_i divide a g, luego debe ser uno de los factores irreducibles g_j de g. Intercambiando el papel de f y g, cada g_j tiene que ser un f_i, lo que termina la demostración. □

De la misma forma se prueba:

Corolario 2.13 (Teorema de los Ceros proyectivo)**.** *Si k es algebraicamente cerrado, y $F \in k[X_0, X_1, X_2]$ es homogéneo de grado positivo y factoriza en factores irreducibles como $F = F_1^{m_1} \dots F_r^{m_r}$, entonces son equivalentes:*

(i) $V(F) \subset V(G)$

(ii) $F_1 \dots F_r$ *divide a* G

(iii) Existe $m \in \mathbb{N}$ *tal que* $F|G^m$.

En particular, $V(F) = V(G)$ *si y sólo si* F *y* G *tienen los mismos factores irreducibles.*

A partir de aquí supondremos siempre que, salvo que se diga lo contrario, **el cuerpo k es algebraicamente cerrado**.

Definición. Se llama *ecuación minimal (o reducida) de una curva* (afín o proyectiva) a un polinomio de grado mínimo que defina la curva.

Por los Corolarios 2.12 y 2.13, una ecuación es minimal si y sólo si no tiene factores múltiples, y tal ecuación es única salvo multiplicación por constante. Obviamente, dada cualquier ecuación de una curva, quitando sus factores múltiples se obtiene una ecuación minimal.

Definición. Se llama *grado de una curva* al grado de una ecuación minimal suya.

Definición. Se llama *curva irreducible* (afín o proyectiva) a una curva C tal que si $C = C_1 \cup C_2$ (con C_1, C_2 curvas, afines o proyectivas, según el caso), entonces $C = C_1$ o $C = C_2$.

Proposición 2.14. *Una curva es irreducible si y sólo si su ecuación minimal es irreducible.*

Demostración: Lo haremos en el caso afín, siendo igual el caso proyectivo. Si un polinomio $f \in k[X, Y]$ sin factores múltiples es reducible, entonces se puede escribir de forma no

trivial como $f = gh$, con g, h primos entre sí. Entonces $V(f) = V(g) \cup V(h)$, y además $V(f) \neq V(g)$ y $V(f) \neq V(h)$, por el Corolario 2.12.

Por otra parte, si fuera f irreducible y $V(f) = V(g) \cup V(h)$, entonces f es la ecuación minimal de $V(gh)$, lo que quiere decir que gh tiene a f como un único factor irreducible, luego necesariamente $V(g) = V(f) = V(h)$. □

Teorema 2.15. *Toda curva (afín o proyectiva) se escribe de forma única como unión finita de curvas irreducibles.*

Demostración: De nuevo, lo haremos sólo en el caso afín. Dada una curva, tomamos una ecuación minimal que factorizará en factores irreducibles $f = f_1 \dots f_r$. Por tanto, $V(f) = V(f_1) \cup \dots \cup V(f_r)$. Por la Proposición 2.14, cada $V(f_i)$ es irreducible, lo que demuestra la existencia de la descomposición. Por otra parte, si $V(f) = V(g_1) \cup \dots \cup V(g_s)$ es otra descomposición (en que tomamos cada g_i minimal, y por tanto irreducible), entonces cada $V(f_i)$ está contenido en $V(g_1) \cup \dots \cup V(g_s) = V(g_1 \dots g_s)$, y por el Lema de Study f_i divide a $g_1 \dots g_s$, luego al ser f_i irreducible divide a algún g_j, es decir coincide con él salvo multiplicación por constante. Análogamente, cada g_j debe coincidir con algún f_i, y por tanto las dos descomposiciones son iguales. □

Definición. Se llama *componente irreducible de una curva* a cada una de las curvas irreducibles que aparecen en la descomposición dada por el Teorema 2.15.

Terminamos la sección con un par de criterios de irreducibilidad que serán muy útiles. Empezamos recordando el conocido criterio de Eisenstein:

Teorema 2.16. *Sea A un DFU, y sea $f = a_0 + a_1 X + \dots + a_d X^d \in A[X]$ un polinomio primitivo (i.e. sus coeficientes no tienen un factor común) tal que existe un elemento irreducible $p \in A$ que satisface alguna de las dos condiciones siguientes:*

(i) p divide a $a_0, a_1, \dots, a_{d-1}$ pero no divide a a_d, y p^2 no divide a a_0.

(ii) p divide a $a_1, \dots, a_d$ pero no divide a a_0, y p^2 no divide a a_d.

Entonces f es irreducible.

Demostración: Posiblemente el lector conozca sólo una versión, y ésta sea que, si se satisface (i), entonces f es irreducible. En realidad, que (ii) implica que f es irreducible se demuestra de la misma forma, pero es también consecuencia de la primera versión. En efecto, si se satisface (ii), entonces de la primera versin del criterio lo que se deduce es que el polinomio $a_d + a_{d-1}X + \dots + a_1 X^{d-1} + a_0 X^d$ es irreducible. Pero por el Lema 1.12(iii) esto es equivalente a que su homogeneizado $F := a_d X_0^d + a_{d-1} X_0^{d-1} X_1 + \dots + a_1 X_0 X_1^{d-1} + a_0 X_1^d$ sea

irreducible. Y por el mismo lema, su deshomogeneizado respecto a X_1, que es precisamente f, es irreducible. □

Y terminamos con otro criterio muy práctico, llamado criterio de Gibson o de las formas:

Lema 2.17. *Sean $f, g \in k[X_1, \ldots, X_n]$ dos polinomios homogéneos primos entre sí y de grados consecutivos. Entonces $f + g$ es un polinomio irreducible.*

Demostración: Si fuera $f + g = h_1 h_2$, como $f + g$ tiene sólo monomios de dos grados consecutivos, necesariamente uno de los h_i tendría que ser homogéneo. Pero esto implicaría que h_i divide a cada componente homogénea de $f + g$, es decir, divide a f y a g. Como f y g son primos entre sí, esto es imposible salvo que h_i fuera una constante. □

3. Sistemas lineales de curvas

Veamos que ya con el Teorema Débil de Bézout se puede hacer mucha geometría. Por empezar con un ejemplo, veremos en esta sección que por cinco puntos del plano uno se espera que pase una única cónica, por lo que si por seis puntos pasa alguna cónica, deben estar en posición especial. El siguiente resultado caracteriza cuándo ocurre esto.

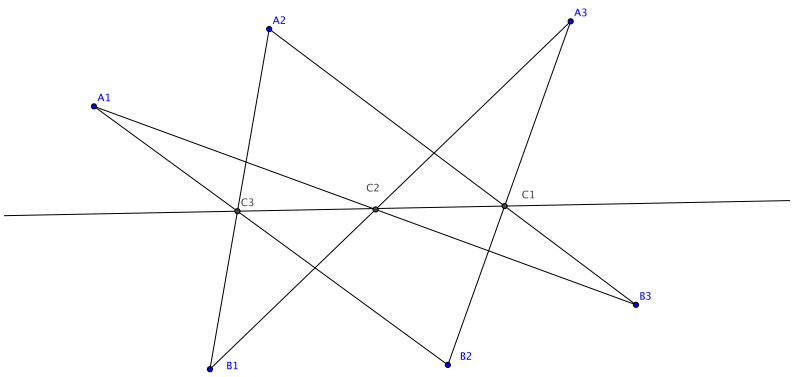
Teorema 3.1. *Sean $A_1, A_2, A_3, B_1, B_2, B_3 \in \mathbb{P}^2_k$ distintos tales que ningún B_j está alineado con dos de los A_i y ningún A_i está alineado con dos de los B_j. Consideramos los puntos*

$$C_1 = A_2B_3 \cap A_3B_2$$

$$C_2 = A_1B_3 \cap A_3B_1$$

$$C_3 = A_1B_2 \cap A_2B_1.$$

Entonces los puntos $A_1, A_2, A_3, B_1, B_2, B_3$ están en una misma cónica, si y sólo si los puntos C_1, C_2, C_3 están en una misma recta.



Demostración: Obsérvese en primer lugar que los puntos C_1, C_2, C_3 existen, ya que nuestras hipótesis prueban que las rectas A_iB_j y A_jB_i son distintas si $i \neq j$. Además, estos tres puntos son distintos dos a dos. Por ejemplo, si $C_1 = C_2$, entonces la recta C_1B_3 (no puede ser $C_1 = B_3$, porque entonces A_2, A_3, B_2, B_3 estarían alineados) contendría los puntos A_1, A_2, con lo que A_1, A_2, B_3 estarían alineados, contra nuestra hipótesis.

Si llamamos F_{ij} a la ecuación de la recta A_iB_j observamos entonces que $F := F_{12}F_{23}F_{31}$ y $G = F_{21}F_{32}F_{13}$ son dos polinomios homogéneos de grado tres que se anulan en $A_1, A_2, A_3, B_1, B_2, B_3, C_1, C_2, C_3$. Por tanto, para cualesquiera $\lambda, \mu \in k$ (no ambos nulos) la curva $V(\lambda F + \mu G)$ pasa por todos esos puntos. La idea central que vamos a usar en la demostración es bien simple: cada vez que fijemos un punto $P = (a_0 : a_1 : a_2) \in \mathbb{P}^2_k$, es

inmediato que existen $\lambda, \mu \in k$ no ambos nulos tales que $\lambda F(a_0, a_1, a_2) + \mu G(a_0, a_1, a_2) = 0$, y por tanto, una curva $V(\lambda F + \mu G)$ que pasa por P.

Supongamos en primer lugar que los puntos $A_1, A_2, A_3, B_1, B_2, B_3$ están en una misma cónica C. Fijando $P \in C \setminus \{A_1, A_2, A_3, B_1, B_2, B_3\}$, podremos encontrar λ, μ tales que la curva $D = V(\lambda F + \mu G)$ pase por P. Tendremos entonces que la cónica C y la cúbica D tienen en común siete puntos distintos, $A_1, A_2, A_3, B_1, B_2, B_3, P$. Entonces, el Teorema Débil de Bézout implica que C y D tienen alguna componente en común. Distinguimos dos casos.

–Si C es una cónica irreducible, entonces necesariamente $C \subset D$, luego $D = C \cup L$ para alguna recta L. Nótese que en este caso ningún C_i puede estar en C, ya que esto implicaría que C tiene rectas trisecantes, lo que contradiría de nuevo el Teorema Débil de Bézout. Por tanto, $C_1, C_2, C_3 \in L$.

–Si C es una cónica reducible, nuestras hipótesis implican que debe ser $C = A_1A_2A_3 \cup B_1B_2B_3$. Sin pérdida de generalidad podemos suponer $P \in A_1A_2A_3$. Esto implica que la recta $A_1A_2A_3$ corta a D en cuatro puntos, por lo que el Teorema débil de Bézout implica $D = A_1A_2A_3 \cup D'$ para alguna cónica D'. Como no puede ser $B_i \in A_1A_2A_3$, necesariamente $B_1, B_2, B_3 \in D'$. Por tanto, la cónica D' contiene tres puntos alineados, luego debe ser $D' = B_1B_2B_3 \cup L$ para alguna recta L. En resumidas cuentas

$$D = A_1A_2A_3 \cup B_1B_2B_3 \cup L.$$

Sin embargo, ningún C_i está en ninguna de las dos primeras rectas (queda como ejercicio para el lector), luego $C_1, C_2, C_3 \in L$.

Supongamos, recíprocamente, que existe una recta L que contiene a C_1, C_2, C_3. Fijamos ahora $P \in L \setminus \{C_1, C_2, C_3\}$. Como antes, existirá una curva $D = V(\lambda F + \mu G)$ que pase por P. Entonces la cúbica D y la recta L comparten los cuatro puntos C_1, C_2, C_3, P. El Teorema débil de Bézout implica que D y L tienen una componente común, es decir, $L \subset D$ y por tanto $D = L \cup C$, donde C es una cónica. El resultado se concluye si demostramos que ningún A_i o B_i está en la recta L. En efecto, si por ejemplo $A_1 \in L$, la recta L sería la recta A_1C_2 (que contiene a B_3) y también la recta A_1C_3 (que contiene a B_2); esto daría el absurdo de que A_1, B_2, B_3 están alineados, en contra de nuestra hipótesis. □

Una consecuencia inmediata del Teorema 3.1 son los siguiente resultados clásicos:

Corolario 3.2 (Teorema de Pascal)**.** *Dada una cónica irreducible $C \subset \mathbb{P}^2$ y seis puntos diferentes suyos $A_1, A_2, A_3, B_1, B_2, B_3$, entonces los puntos*

$$C_1 = A_2B_3 \cap A_3B_2$$

$$C_2 = A_1B_3 \cap A_3B_1$$

$$C_3 = A_1B_2 \cap A_2B_1.$$

están alineados. □

Corolario 3.3 (Teorema de Pappus)**.** *Dadas dos rectas distintas L_1, L_2 y puntos distintos $A_1, A_2, A_3 \in L_1$ y $B_1, B_2, B_3 \in L_2$ (ninguno de ellos el punto de intersección de L_1 y L_2), los puntos*

$$C_1 = A_2B_3 \cap A_3B_2$$

$$C_2 = A_1B_3 \cap A_3B_1$$

$$C_3 = A_1B_2 \cap A_2B_1.$$

están alineados. □

La clave de la demostración del Teorema 3.1 ha sido el hacer combinaciones lineales de dos ecuaciones, lo que al lector le habrá recordado los haces de rectas o de cónicas. En cambio, en este caso, al ser las ecuaciones de grado tres, se trata de un haz de cúbicas. Es a este tipo de conceptos al que vamos a dedicar la sección.

La primera observación es que tomar combinaciones lineales arbitrarias de curvas puede producir cosas en principio indeseadas. Por ejemplo, si tomamos las ecuaciones $F = X_0X_2 - X_1^2$ y $G = X_0X_2 + X_1^2$ de dos cónicas no degeneradas, en cambio $F - G = -2X_1^2$ ya no es la ecuación minimal de una cónica, sino lo que en Geometría Proyectiva se suele llamar recta doble. Por tanto, si queremos considerar todas las posibles combinaciones lineales de ecuaciones de curvas tendremos que aceptar la existencia de estas nuevas curvas. Formalicemos todo esto:

Notación. Denotaremos por V_d al espacio vectorial de polinomios homogéneos de grado d en $k[X_0, X_1, X_2]$ y sea $\mathbb{P}_d := \mathbb{P}(V_d)$ su proyectivizado (esta notación no es en absoluto estándar, pero es la que usaremos por simplicidad en estas notas). La clase de un $F \in V_d$ la denotaremos como $[F]$.

Como la ecuación minimal de una curva es única salvo multiplicación por constante, tenemos una aplicación

$$\{\text{Curvas de } \mathbb{P}^2_k \text{ de grado } d\} \to \mathbb{P}_d$$

que asocia a cada curva la clase $[F]$ de sus ecuaciones minimales. Esta aplicación es inyectiva, ya que, evidentemente, la curva se puede recuperar como $V(F)$. Como hemos notado, no todo elemento de $\mathbb{P}_d$ corresponde a una ecuación minimal de una curva, puesto que $\mathbb{P}_d$ contiene también clases de ecuaciones no minimales, es decir, polinomios en V_d con factores múltiples (por ejemplo, rectas dobles, como acabamos de ver).

Definición. Llamaremos *curva generalizada* a un elemento de $\mathbb{P}_d$, y *curva no reducida* a un elemento $[F] \in \mathbb{P}_d$ tal que F tenga algún factor múltiple.

De este modo, la palabra "curva" hará referencia en esta sección no sólo a los conjuntos $V(F)$ que habíamos definido (y que identificaremos con la clase de su correspondiente ecuación minimal) sino que hemos añadido también las curvas no reducidas.

Lema 3.4. *El espacio vectorial V_d de los polinomios homogéneos de grado d en las variables X_0, X_1, X_2 tiene dimensión $\binom{d+2}{2}$, y el espacio proyectivo $\mathbb{P}_d$ tiene dimensión $\frac{d(d+3)}{2}$.*

Demostración: Una base de V_d son los monomios de grado d en las variables X_0, X_1, X_2, así que todo el Lema es equivalente a demostrar que el número de tales monomios es $\binom{d+2}{2}$. Un monomio de grado d viene dado por un producto $X_{i_1} \dots X_{i_d}$, donde $i_1, \dots, i_d \in \{0, 1, 2\}$. Como el orden del producto no importa, hay tantos monomios como combinaciones con repetición de los tres elementos $0, 1, 2$ tomados de d en d, y ese número es bien sabido$^{(*)}$ que es $\binom{d+2}{d} = \binom{d+2}{2}$. Por tanto, $\dim(V_d) = \binom{d+2}{2}$, y $\dim(\mathbb{P}_d) = \binom{d+2}{2} - 1 = \frac{d(d+3)}{2}$. □

Observación 3.5. Con la notación anterior, tomando el sistema de referencia de $\mathbb{P}_d$ asociado a la base de V_d dada por los monomios de grado d, las coordenadas homogéneas de una curva de grado d, vista como un punto de $\mathbb{P}_d$, no son otra cosa que los coeficientes de la ecuación correspondiente de grado d.

Ejemplo 3.6. Si $d = 2$, entonces $\mathbb{P}_2$ tiene dimensión 5, y sus elementos son cónicas "de verdad" (es decir, o no degeneradas o pares de rectas) o bien rectas dobles. Si ponemos coordenadas, la ecuación de una cónica es de la forma $u_{00}X_0^2 + u_{01}X_0X_1 + u_{02}X_0X_2 + u_{11}X_1^2 + u_{12}X_1X_2 + u_{22}X_2^2$, luego el correspondiente punto de $\mathbb{P}_2$ será $(u_{00} : u_{01} : u_{02} : u_{11} : u_{12} : u_{22})$. Obsérvese que, dentro de $\mathbb{P}_2$, las rectas dobles (es decir, las cónicas nuevas que hemos tenido que admitir) corresponden a puntos $(u_{00} : u_{01} : u_{02} : u_{11} : u_{12} : u_{22})$ tales que la matriz

$$\begin{pmatrix} u_{00} & \frac{1}{2}u_{01} & \frac{1}{2}u_{02} \\ \frac{1}{2}u_{01} & u_{11} & \frac{1}{2}u_{12} \\ \frac{1}{2}u_{02} & \frac{1}{2}u_{12} & u_{22} \end{pmatrix}$$

tiene rango uno. Tal condición está caracterizada por la anulación de los menores de orden dos de la matriz, que son polinomios homogéneos de grado dos en las coordenadas de

$^{(*)}$ Una forma rápida de recordar que las combinaciones con repetición de m elementos tomados de d en d es $\binom{m+d-1}{d}$ es asociar a cada elección $1 \le i_1 \le i_2 \le \dots \le i_d \le m$ de d números entre $1, \dots, m$ la elección $1 \le i_1 < i_2 + 1 < \dots < i_d + d - 1 \le m + d - 1$ de d números distintos entre $1, \dots, m + d - 1$. Esto da una biyección entre las combinaciones con repetición de m elementos tomados de d en d y las combinaciones sin repetición de $m + d - 1$ elementos tomados de d en d, que son $\binom{m+d-1}{d}$.

$\mathbb{P}_2$. Aunque está fuera del alcance de estas notas, para d arbitrario se tiene un resultado análogo: el conjunto de puntos de $\mathbb{P}_d$ que corresponden a ecuaciones no minimales está caracterizado por la anulación de polinomios homogéneos en las coordenadas de $\mathbb{P}_d$ (un conjunto de un espacio proyectivo definido de esa forma, es decir, mediante la anulación de polinomios homogéneos, es lo que se llama un *conjunto proyectivo*, y generaliza la noción de curva algebraica; dedicaremos la sección 10 a esbozar una introducción a esta teoría). Lo mismo ocurre, por ejemplo, si queremos estudiar el conjunto de curvas reducibles (o curvas singulares, que estudiaremos más adelante), que en el caso $d = 2$ vienen caracterizadas porque la matriz anterior es degenerada; dicha condición se expresa mediante la anulación del determinante, que es ahora un polinomio homogéneo de grado tres. Sin embargo, los subconjuntos de $\mathbb{P}_d$ que vamos a considerar en esta sección son los más sencillos posibles: aquéllos definidos por ecuaciones homogéneas de grado uno, es decir, los subespacios lineales de $\mathbb{P}_d$.

Proposición 3.7. *El conjunto de curvas de grado d que pasan por un punto de $\mathbb{P}_k^2$ es un hiperplano de $\mathbb{P}_d$. Por tanto, el conjunto de curvas de grado d que pasan por r puntos distintos de $\mathbb{P}_k^2$ es un subespacio lineal de $\mathbb{P}_d$ de dimensión al menos $\frac{d(d+3)}{2} - r$. En particular, por $r \leq \frac{d(d+3)}{2}$ puntos de $\mathbb{P}_k^2$ pasa alguna curva de grado d.*

Demostración: Una curva de grado d viene dada por un polinomio de la forma

$$u_{d,0,0}X_0^d + u_{d-1,1,0}X_0^{d-1}X_1 + u_{d-1,0,1}X_0^{d-1}X_2 + \ldots + u_{00d}X_2^d$$

(por simplicidad, no usamos ahora la notación del Ejemplo 3.6, sino que ponemos sólo tres subíndices a los coeficientes u_{ijk}, indicando que es el coeficiente de $X_0^iX_1^jX_2^k$). Por la Observación 3.5, las coordenadas homogéneas de tal curva son$(u_{d,0,0} : u_{d-1,1,0} : u_{d-1,0,1} : \ldots : u_{00d}) \in \mathbb{P}_k^{\frac{d(d+3)}{2}}$. Entonces, fijado un punto $a = (a_0 : a_1 : a_2) \in \mathbb{P}_k^2$, el subconjunto de curvas de grado d que pasan por a son los puntos de $\mathbb{P}_k^{\frac{d(d+3)}{2}}$ que satisfacen la ecuación $a_0^dU_{d,0,0} + a_0^{d-1}a_1U_{d-1,1,0} + a_0^{d-1}a_2U_{d-1,0,1} + \ldots + a_2^dU_{00d} = 0$, que es un hiperplano. □

Definición. Se llama *sistema lineal de curvas* a un subespacio proyectivo de algún $\mathbb{P}_d$.

Observación 3.8. Si $d > 1$, no todos los sistemas lineales de curvas de grado d son conjuntos de curvas que pasan por unos puntos dados. Por ejemplo, el conjunto de cónicas de ecuación $t_0X_0^2 + t_1X_1^2 + t_2X_2^2$ no tiene ningún punto en común, luego no puede ser de esa forma.

Definición. Se llama *punto base* de un sistema lineal a un punto que está en todas las curvas del sistema. Se llama *lugar base* de un sistema lineal al conjunto de sus puntos base.

Observación 3.9. En general uno se espera que el lugar base de un sistema lineal "grande" sea vacío. Por ejemplo, dado un sistema lineal Λ, si consideramos dos curvas de Λ de ecuaciones respectivas F y G, los puntos base de Λ estarán en la intersección de $V(F)$ y $V(G)$, que ya sabemos que es un conjunto finito si F y G no tienen factores comunes. Por tanto, lo esperado sería que otra tercera curva de Λ no pasara ya por ninguno de esos puntos (es exactamente lo que ocurre en el ejemplo de la Observación 3.8, en que las curvas de ecuaciones X_0^2, X_1^2 y X_2^2 no tienen puntos en común). Cabe observar, sin embargo, que si tomamos esa tercera curva con ecuación de la forma $t_0F + t_1G$, entonces sí que pasa por los puntos de $V(F) \cap V(G)$. Obsérvese que las curvas de ecuación $t_0F + t_1G$ forman una recta en $\mathbb{P}_d$ (precisamente la recta generada por los puntos que corresponden a las curvas de ecuación F y G). Por tanto, en un sistema lineal de dimensión uno sí que hay puntos base, y lo esperado es que sean d^2 puntos (contados con multiplicidad). Es para sistemas lineales de dimensión mayor en que lo esperado es no tener puntos base (por ejemplo, el sistema de la Observación 3.8 tiene dimensión dos).

Definición. Se llama *haz de curvas* a un sistema lineal de dimensión uno.

Lema 3.10. *Sea Λ un sistema lineal de curvas que tiene dimensión al menos uno. Entonces son equivalentes*

(i) *Λ es un haz*

(ii) *Existe un punto $a \in \mathbb{P}_k^2$ tal que hay una única curva de Λ que pase por a.*

(iii) *Existen dos puntos $a, a' \in \mathbb{P}_k^2$ tales que no hay ninguna curva de Λ que pase al mismo tiempo por a y a'.*

Demostración: Veamos cíclicamente las implicaciones.

$(i) \Rightarrow (ii)$: Tomando un punto a que no esté en alguna curva de Λ, se tendrá que Λ no está en el hiperplano $H_a \subset \mathbb{P}_d$ de las curvas de grado d que pasan por a. Por tanto, la intersección en $\mathbb{P}_d$ de la recta Λ con el hiperplano H_a es un punto, es decir, existe una única curva de Λ que pasa por a.

$(ii) \Rightarrow (iii)$: Sea $a \in \mathbb{P}_k^2$ tal que hay una única curva C de Λ que pase por a. Tomando $a' \notin C$ no habrá ninguna curva de Λ que pase al mismo tiempo por a y a'.

$(iii) \Rightarrow (i)$: Si Λ no fuera un haz, entonces $\dim \Lambda \geq 2$, luego para todo $a, a' \in \mathbb{P}_k^2$ la intersección en $\mathbb{P}_d$ de Λ con los hiperplanos H_a y $H_{a'}$ tiene dimensión al menos cero, con lo que tal intersección es siempre no vacía, lo que contradice (iii). □

Obsérvese que, si $d = 2$, el número esperado de puntos del lugar base de un haz de cónicas es cuatro (véase Observación 3.9), y que por otro lado lo esperado es que las cónicas que pasan por cuatro puntos formen un haz (véase Proposición 3.7). Estudiemos con precisión cuándo cuatro puntos determinan un haz.

Teorema 3.11. *El sistema lineal de cónicas que pasan por cuatro puntos es un haz si y sólo si los cuatro puntos no están alineados.*

Demostración: Sean a_1, a_2, a_3, a_4 los cuatro puntos y llamemos Λ al sistema lineal de cónicas que pasan por a_1, a_2, a_3, a_4. Por la Proposición 3.7, el sistema lineal Λ tiene dimensión al menos uno, luego por el Lema 3.10 será un haz si y sólo si existe $a \in \mathbb{P}^2$ por el que pasa una única cónica de Λ. Demostraremos el resultado según la posición relativa de a_1, a_2, a_3, a_4:

–Si a_1, a_2, a_3, a_4 están alineados en una recta L, entonces una cónica de Λ consiste en la unión de L con otra recta. En particular, dados cualquier $a \in \mathbb{P}^2$, la unión de L y una recta que pase por a es una cónica de Λ. Como hay infinitas de ellas, Λ no es un haz.

–Si hay tres puntos, por ejemplo a_1, a_2, a_3, en una recta L, entonces cualquier cónica de Λ debe ser la unión de L y otra recta que pase por a_4. Por tanto, fijando $a \in \mathbb{P}^2_k$ que no esté en L ni sea a_4, existe una única cónica de Λ que pasa por a (concretamente la unión de L con la recta generada por a y a_4), luego Λ es un haz.

–Si en a_1, a_2, a_3, a_4 no hay tres puntos alineados, fijamos a alineado con a_1, a_2 (y distinto de ellos). Entonces, es evidente que sólo hay una cónica de Λ que pasa por a, que es la unión de las rectas a_1a_2 y a_3a_4, con lo que se concluye que Λ es un haz. □

Corolario 3.12. *Existe una única cónica que pasa por cinco puntos si y sólo si no hay ninguna recta que contenga cuatro de los puntos. Además, en tal caso, la cónica es irreducible si y sólo si no hay ninguna recta que contenga a tres de los puntos.*

Demostración: Basta ir estudiando las distintas posiciones relativas de los puntos:

–Si existe una recta L que pasa por cuatro de los puntos, la unión de L y cualquier recta que pase por el quinto punto es una cónica que pasa por los cinco puntos, y hay infinitas de ellas.

–Si hubiera tres puntos alineados pero no cuatro, claramente la recta que contiene los tres puntos tiene que formar parte de cualquier cónica que pase por los cinco puntos. Como los otros dos puntos no pueden estar en esa recta, la única cónica que pasa por los cinco puntos es la unión de la recta que pasa por tres de ellos y la recta que une los otros dos puntos restantes.

–Si no hay tres puntos alineados entre los cinco, ya sabemos por el Teorema 3.11 que el sistema lineal de cónicas que pasan por cuatro de los puntos es un haz Λ. Una de tales cónicas es un par de rectas, una que pase por dos de los cuatro puntos y otra por los otros dos. Por hipótesis, tal cónica no pasa por el quinto punto, luego Λ no está contenido en el hiperplano de $\mathbb{P}_2$ dado por las cónicas que pasan por el quinto punto. Por tanto, el conjunto de las cónicas que pasan por los cinco puntos, que es la intersección de

Λ con tal hiperplano, consiste en un solo punto, es decir, sólo hay una cónica que pase por los cinco puntos. Además, la cónica es irreducible, pues si fuera la unión de dos rectas necesariamente habría tres puntos alineados. $\square$

Observación 3.13. La demostración anterior nos da también un modo práctico para calcular la única cónica que pasa por cinco puntos. Obviamente, el único caso interesante es cuando no hay tres puntos alineados. Supongamos, por ejemplo, que tenemos los puntos $(1:0:0), (0:1:0), (0:0:1), (1:1:1), (1:2:3)$. Tomando dos pares de rectas podemos generar el haz de las cónicas que pasan por los cuatro primeros puntos. Por ejemplo, $X_2(X_0 - X_1)$ y $X_1(X_0 - X_2)$ son ecuaciones de dos cónicas que pasan por $(1:0:0), (0:1:0), (0:0:1), (1:1:1)$. Como las cónicas por esos cuatro puntos forman un haz, necesariamente son de ecuación

$$t_0 X_2(X_0 - X_1) + t_1 X_1(X_0 - X_2).$$

Para que pase por el quinto punto $(1:2:3)$ debe ser $-3t_0 - 4t_1 = 0$, luego $(t_0 : t_1) = (4 : -3)$, y la cónica buscada tiene ecuación $4X_2(X_0 - X_1) - 3X_1(X_0 - X_2)$, es decir, $-3X_0X_1 + 4X_0X_2 - X_1X_2$.

Para $d = 3$ (y en general para $d \geq 3$), los números no funcionan tan bien como para cónicas. En efecto, el número esperado de puntos base de un haz de cúbicas es nueve; por contra, el sistema lineal de cúbicas que pasan por nueve puntos tiene dimensión esperada cero (es decir, nos esperamos sólo una), mientras que para obtener un haz lo esperable sería considerar conjuntos de cúbicas que pasan por ocho puntos. Veamos en primer lugar cuándo tal conjunto es un haz.

Teorema 3.14. *El sistema lineal de cúbicas que pasan por ocho puntos es un haz si y sólo si no están todos en una cónica o cinco en una recta.*

Demostración: Llamando $a_1, \ldots, a_8$ a los puntos y Λ al sistema lineal de cúbicas que pasan por $a_1, \ldots, a_8$, por la Proposición 3.7 tal sistema tendrá dimensión al menos uno. Usando el Lema 3.10, el sistema Λ es un haz si y sólo si existe $a \in \mathbb{P}^2_k$ por el que pasa una única cúbica de Λ. Iremos distinguiendo casos:

–Si $a_1, \ldots, a_8$ están en una misma cónica C, entonces para cada $a \in \mathbb{P}^2_k$ la unión de C y cualquier recta que pase por a es una cúbica de Λ que pasa por a, luego Λ no es un haz.

–Si hay cinco puntos, por ejemplo $a_1, \ldots, a_5$, en una recta L, para cada punto $a \in \mathbb{P}^2_k$, por la Proposición 3.7 existe un sistema de dimensión al menos uno de cónicas que pasan por a_6, a_7, a_8, a, y la unión de cualquiera de esa cónicas y L es una cúbica de Λ que pasa por a, luego Λ no es un haz.

Podemos suponer entonces para los siguientes casos que no hay ninguna cónica que contenga a los puntos $a_1, \ldots, a_8$ ni ninguna recta que contenga cinco de ellos y hay que ver en todos los casos que existe $a \in \mathbb{P}^2_k$ por el que pasa una única cúbica de Λ.

–Si hay una recta L que pasa por cuatro de los puntos $a_1, \ldots, a_8$, por ejemplo por $a_1, \ldots, a_4$, entonces las cúbicas de Λ son exactamente las que son unión de L y una cónica que pase por $a_5, \ldots, a_8$. Como $a_5, \ldots, a_8$ no pueden estar en una recta (pues la unión de L y dicha recta sería una cónica que contiene a $a_1, \ldots, a_8$), entonces el Teorema 3.11 implica que las cónicas que pasan por $a_5, \ldots, a_8$ forman un haz. Tomando a fuera de L y de alguna de las cónicas del haz, existirá una única cónica C del haz que pase por a. Entonces, hay una única cúbica de Λ que pase por a, concretamente la unión de L y C, luego Λ es un haz en este caso.

–Si hay tres puntos entre $a_1, \ldots, a_8$ en una recta pero no hay cuatro alineados, sea L la recta que contiene esos tres puntos, que supondremos que son a_1, a_2, a_3. Como los otros cinco puntos $a_4, \ldots, a_8$ no contienen cuatro alineados, sólo hay una cónica C que pasa por ellos, por el Corolario 3.12. Por tanto, fijando un punto a de L distinto de a_1, a_2, a_3, las cúbicas de Λ que pasan por a contienen necesariamente a L, luego deben ser L más una cónica que pase por $a_4, \ldots, a_8$, que es necesariamente C. La unicidad de esta cúbica demuestra que Λ es un haz.

Podemos suponer entonces para los casos restantes que no hay tres puntos alineados entre los ocho puntos. Obsérvese que entonces cualquier cónica que contenga al menos cinco puntos de $a_1, \ldots, a_8$ es necesariamente irreducible. Seguimos distinguiendo casos:

–Si hay una cónica C que contiene siete de los ocho puntos, por ejemplo $a_1, \ldots, a_7$, entonces cualquier cúbica de Λ es la unión de C con una recta que pasa por a_8, tomando a fuera de C distinto de a_8, la única cúbica de Λ que pasa por a es la unión de C y la recta aa_8, de lo que se concluye que Λ es un haz.

–Si hay una cónica C que contiene seis de los ocho puntos, por ejemplo $a_1, \ldots, a_6$, tomamos un punto $a \in C$ distinto de $a_1, \ldots, a_6$. Entonces, una cúbica de Λ que pase por a es necesariamente la cónica C más la recta a_7a_8. Esto demuestra que Λ también es un haz en este caso.

–Finalmente, supongamos que no existe una cónica que pase por seis de los puntos. Tomamos entonces una cónica C que pase por $a_1, \ldots, a_5$, que no pasará por a_6, a_7, a_8. Para este caso usaremos la parte (iii) del Lema 3.10. Tomamos entonces $a, a' \in C$ distintos de $a_1, \ldots, a_5$, y si existiera una cúbica de Λ que pasara por a, a' sería necesariamente la unión de C y una recta. Pero tal recta debería contener a a_6, a_7, a_8, lo que es absurdo porque no podían estar alineados. Por tanto, no existe tal cúbica y Λ es un haz. □

El siguiente resultado nos explica que, para recuperar un haz de cúbicas a partir de

los nueve puntos base esperados, nos sobra uno de los nueve puntos.

Corolario 3.15. *Si C es una cúbica irreducible, entonces el sistema lineal de cúbicas por ocho puntos distintos de C es un haz. En particular, si otra cúbica D corta a C en nueve puntos distintos, entonces cualquier cúbica que pase por ocho de los nueve puntos pasa también por el noveno.*

Demostración: Basta demostrar que el sistema de cúbicas que pasan por ocho de los nueve puntos es un haz, porque entonces tales cúbicas tendrán como ecuación una combinación de las ecuaciones de C y D, luego se anularán en los nueve puntos de intersección de C y D. Pero eso es inmediato por el Teorema 3.14, ya que, al ser C irreducible, no puede cortar a una recta en más de tres puntos ni a una cónica en más de seis puntos. □

Observación 3.16. El resultado anterior nos muestra que no podemos aspirar a un resultado como el Corolario 3.12. En efecto, dados nueve puntos distintos $a_1, \ldots, a_9$, si queremos caracterizar cuándo determinan una única cúbica, podríamos proceder como en la demostración del corolario. En el caso en que no haya ni ocho puntos en una cónica ni cinco en una recta, el Teorema 3.14 nos permitiría decir que el conjunto Λ de cúbicas que pasan por $a_1, \ldots, a_8$ es un haz. Sin embargo, a diferencia de la demostración del Corolario 3.12, no podemos garantizar que haya una cúbica de Λ que no pase por a_9, ya que podríamos encontrarnos con la situación del Corolario 3.15. Por tanto, necesitaríamos imponer también la condición de que $a_1, \ldots, a_9$ no sean la intersección de dos cúbicas, pero eso es básicamente poner como hipótesis lo que queremos probar.

4. Curvas parametrizadas

Mientras que en Geometría Diferencial es más fácil trabajar con curvas parametrizadas, en Geometría Algebraica la situación es más complicada, ya que en general una curva definida por un polinomio no tiene por qué poder parametrizarse por polinomios, ni incluso por cocientes de polinomios. En caso de posible parametrización, veremos que el caso de curvas proyectivas es siempre mejor, ya que no hacen falta denominadores. Empezamos ilustrando este hecho con un ejemplo

Ejemplo 4.1. Retomemos el Ejemplo 2.5. Habíamos visto que el conjunto de puntos

$$C = \{(\frac{t}{t+1}, \frac{t}{t-1}) \mid t \in k \setminus \{-1, 1\}\}$$

era la curva $V(2XY - X - Y)$ menos el punto $(1, 1)$. Una primera cosa que podemos hacer es, como decíamos antes, quitar denominadores a base de ver la curva en el plano proyectivo. Efectivamente, como

$$(1 : \frac{t}{t+1} : \frac{t}{t-1}) = \big((t+1)(t-1) : t(t-1) : t(t+1)\big),$$

ya tenemos puntos incluso cuando $t = 1, -1$. En efecto, si $t = 1$ obtenemos el punto $(0 : 0 : 1)$, mientras que para $t = -1$ obtenemos el punto $(0 : 1 : 0)$, que son precisamente los puntos del infinito de $V(2X_1X_2 - X_0X_1 - X_0X_2)$, completado proyectivo de $V(2XY - X - Y)$. Seguimos teniendo el problema de que el punto $(1 : 1 : 1)$ del completado proyectivo no se obtiene para ningún valor de t. Dado que ese punto parecía corresponder al valor infinito del parámetro t, vamos a intentar formalizar esto. Para eso, vemos t como un punto de $\mathbb{A}^1_k$, y añadimos a la recta afín su punto del infinito viéndola dentro de $\mathbb{P}^1_k$. Esto quiere decir que un punto $(t_0 : t_1) \in \mathbb{P}^1_k$ se ve como el parámetro $t = \frac{t_1}{t_0}$. Por tanto, la parametrización queda, quitando denominadores, como

$$\big((\frac{t_1}{t_0} + 1)(\frac{t_1}{t_0} - 1) : \frac{t_1}{t_0}(\frac{t_1}{t_0} - 1) : \frac{t_1}{t_0}(\frac{t_1}{t_0} + 1)\big) = (t_1^2 - t_0^2 : t_1^2 - t_0t_1 : t_1^2 + t_0t_1),$$

y ahora para el punto del infinito $(t_0 : t_1) = (0 : 1)$ se obtiene efectivamente el punto $(1 : 1 : 1)$.

Veamos ahora qué tipo de parametrización como la anterior tiene sentido. Si queremos que sea polinomial, parece razonable que los polinomios sean homogéneos. Si tomamos $A_0, A_1, A_2 \in k[T_0, T_1]$ homogéneos de grados respectivos d_0, d_1, d_2, y queremos definir

$$\begin{array}{ccccc} \varphi_{A_0,A_1,A_2} & \mathbb{P}^1_k & \longrightarrow & \mathbb{P}^2_k \\ & (t_0 : t_1) & \mapsto & (A_0(t_0, t_1) : A_1(t_0, t_1) : A_2(t_0, t_1)) \end{array}$$

en principio no está bien definida, porque si cambiamos el representante, entonces la imagen de $(\lambda t_0 : \lambda t_1)$ sería $(\lambda^{d_0} A_0(t_0,t_1) : \lambda^{d_1} A_1(t_0,t_1) : \lambda^{d_2} A_2(t_0,t_1))$, que en principio será distinto de $(A_0(t_0,t_1) : A_1(t_0,t_1) : A_2(t_0,t_1))$, a no ser que $d_0 = d_1 = d_2$. Por tanto, a partir de ahora consideraremos polinomios homogéneos A_0, A_1, A_2 del mismo grado d. Además, para que la imagen de un punto $(t_0 : t_1)$ tenga sentido necesitaremos que los tres polinomios no se anulen nunca a la vez en ningún $(t_0 : t_1)$, es decir, que $t_1T_0 - t_0T_1$ no divida simultáneamente a A_0, A_1, A_2. Para ello, supondremos siempre que A_0, A_1, A_2 no tienen factores comunes. Estudiemos los casos de grado pequeño.

Ejemplo 4.2. Si A_0, A_1, A_2 tienen grado uno, entonces no pueden ser todos proporcionales entre sí, pues en tal caso todos se anularían en el mismo punto. Por tanto, si escribimos $A_0 = a_0T_0 + b_0T_1$, $A_1 = a_1T_0 + b_1T_1$, $A_2 = a_2T_0 + b_2T_1$, entonces se tiene que $\begin{pmatrix} a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix}$ tiene rango dos, luego la imagen de φ_{A_0,A_1,A_2} es precisamente la recta generada por los puntos $(a_0 : a_1 : a_2)$ y $(b_0 : b_1 : b_2)$. Recuperamos entonces la parametrización habitual de una recta proyectiva. Nótese que se podía haber razonado también del siguiente modo: dentro del espacio vectorial de dimensión dos de los polinomios de grado uno en $k[T_0, T_1]$, los elementos A_0, A_1, A_2 son un sistema de generadores y satisfacen una relación de dependencia lineal no trivial de la forma $\lambda_0A_0 + \lambda_1A_1 + \lambda_2A_2 = 0$, luego la imagen de φ_{A_0,A_1,A_2} está contenida en la recta $V(\lambda_0X_0 + \lambda_1X_1 + \lambda_2X_2)$, y no es difícil comprobar que en realidad se tiene la igualdad.

Ejemplo 4.3. Supongamos ahora que A_0, A_1, A_2 son homogéneos de grado dos. Retomando el último argumento del ejemplo anterior, distinguimos dos casos:

–Si A_0, A_1, A_2 generan todo el espacio vectorial (de dimensión tres) de los polinomios homogéneos de grado dos en $k[T_0, T_1]$, entonces la imagen de φ_{A_0,A_1,A_2} son los puntos de la forma

$$\begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix} = P \begin{pmatrix} t_0^2 \\ t_0t_1 \\ t_1^2 \end{pmatrix}$$

donde las filas de P son los coeficientes de A_0, A_1, A_2, y por hipótesis $\det(P) \neq 0$. Por tanto, haciendo el cambio

$$\begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix} = P \begin{pmatrix} X_0' \\ X_1' \\ X_2' \end{pmatrix}$$

la parametrización en las nuevas coordenadas queda $(X_0' : X_1' : X_2') = (t_0^2 : t_0t_1 : t_1^2)$, y el Ejercicio 1.7 muestra que tales puntos son la cónica $V(X_0'X_2' - {X_1'}^2)$ o lo que es lo mismo (si estamos en característica distinta de dos), de ecuación matricial.

$$\begin{pmatrix} X_0' & X_1' & X_2' \end{pmatrix} \begin{pmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} X_0' \\ X_1' \\ X_2' \end{pmatrix} = 0.$$

Por tanto, en las coordenadas iniciales, la imagen de φ_{A_0,A_1,A_2} será la cónica de ecuación matricial

$$(\,X_0 \quad X_1 \quad X_2\,)\,(P^{-1})^t \begin{pmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{pmatrix} P^{-1} \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix} = 0.$$

Además, como toda cónica irreducible es proyectivamente equivalente a $V(X_0'X_2' - X_1'^2)$, se concluye que las imágenes de todas las φ_{A_0,A_1,A_2} son exactamente todas las cónicas irreducibles de $\mathbb{P}^2_k$.

–Si A_0, A_1, A_2 generan un subespacio de dimensión dos de polinomios, entonces satisfacen una relación de dependencia lineal, que por simplicidad supondremos que es de la forma $A_2 = \lambda_0 A_0 + \lambda_1 A_1$. Por tanto, en este caso la imagen de φ_{A_0,A_1,A_2} está contentida en la recta $V(X_2 - \lambda_0 X_0 - \lambda_1 X_1)$. En realidad, podemos descomponer φ_{A_0,A_1,A_2} de la siguiente forma:

$$\begin{array}{ccccc} \mathbb{P}^1_k & \longrightarrow & \mathbb{P}^1_k & \longrightarrow & \mathbb{P}^2_k \\ (t_0 : t_1) & \mapsto & (A_0(t_0,t_1) : A_1(t_0,t_1)) & & \\ & & (t_0 : t_1) & \mapsto & (t_0 : t_1 : \lambda_0 t_0 + \lambda_1 t_1) \end{array}$$

Mientras la segunda aplicación es una parametrización "razonable" de la recta $V(X_2 - \lambda_0 X_0 - \lambda_1 X_1)$, la primera aplicación no es inyectiva, ya que en general cada punto $(s_0 : s_1) \in \mathbb{P}^1_k$ tiene dos preimágenes $(t_0 : t_1)$. En efecto, decir que la imagen de $(t_0 : t_1)$ es $(s_0 : s_1)$ quiere decir que los vectores $(A_0(t_0,t_1), A_1(t_0,t_1))$ y (s_0, s_1) son proporcionales, es decir, $\begin{vmatrix} A_0(t_0,t_1) & A_1(t_0,t_1) \\ s_0 & s_1 \end{vmatrix} = 0$, que es una ecuación de grado dos en t_0, t_1, que en general se anula en dos puntos $(t_0 : t_1) \in \mathbb{P}^1_k$. Por tanto, nuestra parametrización φ_{A_0,A_1,A_2} original consiste en "recorrer la recta dos veces".

En grado superior las cosas son más complicadas. Por ejemplo, los Ejercicios 1.8 y 1.9 nos dan dos comportamientos distintos de parametrizaciones de grado tres. Para entender mejor la situación general comenzaremos estudiando un poco más en detalle los polinomios homogéneos en dos variables. La filosofía general es que se comportan como los polinomios en una variable (ya vimos un primer indicio en el Teorema 1.13), aunque en general funcionan mejor en muchos aspectos. Empezamos con una definición inspirada en el Teorema 1.13.

Definición. Llamaremos *raíz de un polinomio homogéneo* $F \in k[T_0, T_1]$ a cualquier punto de $V(F)$. Se llama *multiplicidad de una raíz* $(t_0 : t_1)$ de F a la mayor potencia de $t_1T_0 - t_0T_1$ que divide a F. Cuando la multiplicidad es uno, diremos que se trata de una *raíz simple*, y en caso contrario diremos que es una *raíz múltiple*.

Teorema 4.4. *Si k es un cuerpo cuya característica no es un divisor de d, un polinomio*

$F \in k[T_0, T_1]$ tiene una raíz múltiple $(t_0 : t_1) \in \mathbb{P}^1_k$ si y sólo si $(t_0 : t_1)$ es una raíz de F_0 y F_1[(*)].

Demostración: Evidentemente, una raíz múltiple $(t_0 : t_1)$ de F es una raíz tanto de F_0 como de F_1. Recíprocamente, si $(t_0 : t_1)$ es una raíz de F_0 y F_1, por la identidad de Euler tendremos que $dF(t_0, t_1) = 0$, luego nuestra hipótesis sobre la característica implica que $(t_0 : t_1)$ es una raíz de F. Por el Teorema 1.13(i) podremos escribir $F = (t_1T_0 - t_0T_1)G$ para cierto polinomio $G \in k[T_0, T_1]$, y basta ver que $(t_0 : t_1)$ es una raíz de G. Eso es evidente derivando en la anterior igualdad respecto de T_0, T_1 y evaluando en (t_0, t_1), ya que obtenemos $F_0(t_0, t_1) = t_1G(t_0, t_1)$ y $F_1(t_0, t_1) = -t_0G(t_0, t_1)$. Como $(t_0 : t_1)$ es una raíz de F_0 y F_1 y no se anulan a la vez t_0 y t_1, se sigue el resultado. □

Ejemplo 4.5. Si tenemos un polinomio cuadrático $F := aT_1^2 + bT_0T_1 + cT_0^2$ (lo escribimos de este modo para que sea el homogeneizado de $aT^2 + bT + c$), entonces tendrá una raíz múltiple si y sólo si $F_0 = bT_1 + 2cT_0$ y $F_1 = 2aT_1 + bT_0$ tienen una raíz común. Como son de grado uno, la única forma de compartir raíz es ser proporcionales, lo que es equivalente a la anulación de $\begin{vmatrix} b & 2c \\ 2a & b \end{vmatrix} = b^2 - 4ac$, que, como no podía ser de otra forma, es el discriminante de $aT^2 + bT + c$. En general, el discriminante de un polinomio de una variable se suele definir como la resultante de un polinomio y su derivada. Sin embargo, la resultante de $f(T) = aT^2 + bT + c$ y $f'(T) = 2aT + b$ es $-a(b^2 - 4ac)$, que no es exactamente el discriminante. Esto en realidad es un indicio de que los polinomios homogéneos funcionan mejor. De hecho, para ellos existe también la noción de resultante, que estudiamos a continuación, y que veremos que también funciona mejor.

El ejemplo anterior tiene ya el gusto de resultante, ya que la existencia de raíces (o factores) comunes de dos polinomios se decide mediante la anulación de un determinante cuyas entradas son precisamente los coeficientes de los polinomios. Antes de definir la resultante para polinmnios homogéneos, demostraremos un lema técnico que aliviará la demostración de por qué funciona la nueva noción de resultante.

Lema 4.6. *Sean $F, G \in A[T_0, T_1]$ polinomios homogéneos de grados respectivos d y e con coeficientes en un DFU A. Entonces son equivalentes:*

(i) F y G comparten algún factor de grado positivo.

(ii) Existe un entero $c \geq 1$ y polinomios homogéneos $F', G' \in A[T_0, T_1]$ no nulos de grados respectivos $d - c, e - c$ tales que $FG' = GF'$.

(*) Como se verá en la demostración, la hipótesis sobre la característica no es necesaria si en el enunciado suponemos que $(t_0 : t_1)$ es una raíz de F.

(iii) Existen polinomios homogéneos $F', G' \in A[T_0, T_1]$ no nulos de grados respectivos $d-1, e-1$ tales que $FG' = GF'$.

Demostración: Demostraremos las implicaciones cíclicamente.

$(i) \Rightarrow (ii)$: Sea H un factor común de F y G de grado $c \geq 1$. Entonces podemos escribir $F = F'H$ y $G = G'H$, donde $F', G' \in A[T_0, T_1]$ son no nulos de grados respectivos $d-c, e-c$. Tendremos entonces

$$FG' = F'HG' = F'G$$

como queríamos demostrar.

$(ii) \Rightarrow (iii)$: Basta sustituir F' por $F'T_0^{c-1}$ y G' por $G'T_0^{c-1}$.

$(iii) \Rightarrow (i)$: De la igualdad $FG' = GF'$ se sigue que cada factor irreducible de F es un factor irreducible de G o de F'. Como F' tiene grado menor que F, no puede contener todos los factores irreducibles de F de grado positivo, luego algún factor irreducible de F de grado positivo es también un factor de G. □

Teorema 4.7. *Sea A un dominio de factorización única. Entonces, dos polinomios $F = a_0T_0^d + a_1T_0^{d-1}T_1 + \ldots + a_dT_1^d$ y $G = b_0T_0^e + b_1T_0^{e-1}T_1 + \ldots + b_eT_1^e$ de $A[T_0, T_1]$ tienen un factor común de grado positivo si y sólo si* $\mathrm{Res}(F, G) = 0$, *donde*

$$\mathrm{Res}(F,G) = \left|\begin{array}{cccccccc} a_0 & a_1 & \ldots & a_d & 0 & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{d-1} & a_d & 0 & \ldots & 0 \\ & & \ddots & & & & & \\ 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_{d-1} & a_d \\ b_0 & b_1 & \ldots & b_{e-1} & b_e & 0 & \ldots & 0 \\ 0 & b_0 & \ldots & b_{e-2} & b_{e-1} & b_e & 0\ldots & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_{e-1} & b_e \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} e \text{ filas} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} d \text{ filas} \end{array}$$

Demostración: Como el resultado es evidente si alguno de los polinomios es nulo (puesto que en tal caso cualquier polinomio se puede considerar factor suyo, y se tiene por otra parte que $\mathrm{Res}(F, G) = 0$), supondremos que F y G son ambos no nulos. Por el Lema 4.6, F y G tienen un factor común de grado positivo si y sólo si existen polinomios F', G' no nulos de grados respectivos $d-1$ y $e-1$ tales que $FG' = GF'$. Entonces la existencia de F' y G' es equivalente a la existencia de elementos $c_0, c_1, \ldots, c_{d-1}, d_0, d_1, \ldots, d_{e-1} \in A$, no todos nulos, tales que

$$F \cdot (d_0T_0^{e-1} + d_1T_0^{e-2}T_1 + \ldots + d_{e-1}T_1^{e-1}) = G \cdot (c_0T_0^{d-1} + c_1T_0^{d-2}T_1 + \ldots + c_{d-1}T_1^{d-1}).$$

En otras palabras, el sistema homogéneo en las variables $c_0, c_1, \ldots, c_{d-1}, d_0, d_1, \ldots, d_{e-1}$ (supondremos $d \geq e$)

$$
\begin{array}{cccccccccc}
a_0d_0 & & & & & -b_0c_0 & & & & = 0 \\
a_1d_0 & +a_0d_1 & & & & -b_1c_0 & -b_0c_1 & & & = 0 \\
\vdots & & & & & & & & & \\
a_{e-1}d_0 & +a_{e-2}d_1 & \ldots & +a_0d_{e-1} & & -b_{e-1}c_0 & -b_{e-2}c_1 & \ldots & & = 0 \\
a_ed_0 & +a_{e-1}d_1 & \ldots & +a_1d_{e-1} & & -b_ec_0 & -b_{e-1}c_1 & \ldots & & = 0 \\
a_{e+1}d_0 & +a_ed_1 & \ldots & +a_2d_{e-1} & & & -b_ec_1 & \ldots & & = 0 \\
\vdots & & & & & & & & & \\
a_{d-1}d_0 & +a_{d-2}d_1 & \ldots & +a_{d-e}d_{e-1} & & & & \ldots & -b_0c_{d-1} & = 0 \\
a_dd_0 & +a_{d-1}d_1 & \ldots & +a_{d-e+1}d_{e-1} & & & & \ldots & -b_1c_{d-1} & = 0 \\
 & +a_dd_1 & \ldots & +a_{d-e+2}d_{e-1} & & & & \ldots & -b_2c_{d-1} & = 0 \\
\vdots & & & & & & & & & \\
 & & & a_dd_{e-1} & & & & & -b_ec_{d-1} & = 0
\end{array}
$$

tiene solución no trivial. Obsérvese que, quitando denominadores, el que el sistema anterior tenga solución no trivial en elementos A es equivalente a que tenga solución no trivial en elementos del cuerpo de fracciones de A. Podemos usar entonces al Álgebra Lineal para concluir que el sistema tiene solución no trivial si y sólo si el determinante de la matriz de coeficientes es cero. Pero, cambiando de signo las d últimas columnas de la matriz de coeficientes y trasponiendo, obtenemos exactamente la matriz que define $\mathrm{Res}(F, G)$, lo que demuestra el resultado. □

Definición. Se llama *resultante homogénea de dos polinomios homogéneos en dos variables* F, G a la expresión $\mathrm{Res}(F, G)$ del teorema anterior. Para distinguirla de la resultante como polinomios en alguna de las variables, seguiremos nuestra notación ya habitual de usar mayúsculas para el caso homogéneo. Se llama *discriminante de un polinomio homogéneo* F *en dos variables* a $\mathrm{Disc}(F) = \mathrm{Res}(F_0, F_1)$.

Ejercicio 4.8. Demostrar, usando la definición como determinante del Teorema 4.7, las siguientes propiedades de la resultante homogénea(*):

(*) Los resultados que se piden aquí son más generales, y se basan en realidad en que, como ocurre en el caso de resultantes clásicas, la resultante de F y G se puede calcular, salvo constante, como el producto $G(a_1, b_1) \ldots G(a_d, b_d)$, donde $(a_1 : b_1), \ldots, (a_d : b_d)$ son las raíces de F. De la misma forma, el discriminante de F es, salvo constante, el producto de todos los posibles $\begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix}$

(i) Si F, G son homogéneos del mismo grado d, entonces

$$\mathrm{Res}(F(\lambda T_0, \mu T_1), G(\lambda T_0, \mu T_1)) = \lambda^{d^2}\mu^{d^2}\,\mathrm{Res}(F, G)$$

[Indicación: Usar el mismo truco que en la demostración del Teorema 2.8].

(ii) Si F, G son homogéneos del mismo grado, entonces

$$\mathrm{Res}\left(F(T_0 + \lambda T_1, T_1), G(T_0 + \lambda T_1, T_1)\right) = \mathrm{Res}(F, G)$$

$$\mathrm{Res}\left(F(T_0, T_1 + \lambda T_0), G(T_0, T_1 + \lambda T_0)\right) = \mathrm{Res}(F, G)$$

[Indicación: Escribir la expresón determinantal de la resultante y manipular las columnas].

(iii) Usando los apartados anteriores, demostrar que, si F es un polinomio homogéneo de grado d, entonces

$$\mathrm{Disc}\big(F(aT_0 + bT_1, cT_1)\big) = (ac)^{d(d-1)}\mathrm{Disc(F)}$$

$$\mathrm{Disc}\big(F(aT_0, bT_0 + cT_1)\big) = (ac)^{d(d-1)}\mathrm{Disc(F)}.$$

(iv) Deducir que, si F es un polinomio homogéneo de grado d, entonces

$$\mathrm{Disc}(F(a_{00}T_0 + a_{01}T_1, a_{10}T_0 + a_{11}T_1) = \begin{vmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{vmatrix}^{d(d-1)} \mathrm{Disc(F)}$$

[Indicación: Descompóngase el cambio de variable usando una igualdad matricial como $\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} = \begin{pmatrix} \frac{a_{00}a_{11} - a_{01}a_{10}}{a_{11}} & a_{01} \\ 0 & a_{11} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{a_{10}}{a_{11}} & 1 \end{pmatrix}$].

Teorema 4.9. *Sean $A_0, A_1, A_2 \in k[T_0, T_1]$ tres polinomios homogéneos de grado d sin factores comunes. Entonces existe un polinomio no nulo $F \in k[X_0, X_1, X_2]$ homogéneo de grado d tal que:*

(i) $\mathrm{Res}(X_0A_1 - X_1A_0, X_0A_2 - X_2A_0) = X_0^d F$

$\mathrm{Res}(X_0A_1 - X_1A_0, X_1A_2 - X_2A_1) = X_1^d F$

$\mathrm{Res}(X_0A_2 - X_2A_0, X_1A_2 - X_2A_1) = X_2^d F$

(donde las resultantes son resultantes homogéneas como polinomios en T_0, T_1).

(ii) $\left\{(A_0(t_0, t_1) : A_1(t_0, t_1) : A_2(t_0, t_1)) \in \mathbb{P}_k^2 \mid (t_0 : t_1) \in \mathbb{P}_k^1\right\} = V(F)$

Demostración: Obsérvese que existe una relación

$$X_1(X_0A_2 - X_2A_0) = X_2(X_0A_1 - X_1A_0) + X_0(X_1A_2 - X_2A_1) \qquad (*)$$

Por tanto

$$X_1^d \operatorname{Res}(X_0A_1 - X_1A_0, X_0A_2 - X_2A_0) = \operatorname{Res}(X_0A_1 - X_1A_0, X_1(X_0A_2 - X_2A_0)) =$$

$$= \operatorname{Res}(X_0A_1 - X_1A_0, X_2(X_0A_1 - X_1A_0) + X_0(X_1A_2 - X_2A_1)) =$$

$$= \operatorname{Res}(X_0A_1 - X_1A_0, X_0(X_1A_2 - X_2A_1)) = X_0^d \operatorname{Res}(X_0A_1 - X_1A_0, X_1A_2 - X_2A_1)$$

lo que implica la existencia de F (que en principio podría ser cero) tal que

$$\operatorname{Res}(X_0A_1 - X_1A_0, X_0A_2 - X_2A_0) = X_0^d F$$

$$\operatorname{Res}(X_0A_1 - X_1A_0, X_1A_2 - X_2A_1) = X_1^d F$$

Análogamente,

$$X_1^d \operatorname{Res}(X_0A_2 - X_2A_0, X_1A_2 - X_2A_1) = \operatorname{Res}(X_1(X_0A_2 - X_2A_0), X_1A_2 - X_2A_1) =$$

$$= \operatorname{Res}(X_2(X_0A_1 - X_1A_0) + X_0(X_1A_2 - X_2A_1), X_1A_2 - X_2A_1) =$$

$$= \operatorname{Res}(X_2(X_0A_1 - X_1A_0), X_1A_2 - X_2A_1) =$$

$$= X_2^d \operatorname{Res}(X_0A_1 - X_1A_0, X_1A_2 - X_2A_1) = X_2^d X_1^d F$$

lo que implica

$$\operatorname{Res}(X_0A_2 - X_2A_0, X_1A_2 - X_2A_1) = X_2^d F$$

y demuestra (i), excepto que F sea no nulo. Esto último lo dejamos hasta demostrar (ii).

Veamos ahora (ii), es decir, que el conjunto

$$C = \{(A_0(t_0, t_1) : A_1(t_0, t_1) : A_2(t_0, t_1)) \in \mathbb{P}_k^2 \mid (t_0 : t_1) \in \mathbb{P}_k^1\}$$

es la curva $V(F)$. En primer lugar, si $(x_0 : x_1 : x_2)$ está en C, eso quiere decir que existe algún $(t_0 : t_1) \in \mathbb{P}_k^1$ tal que $(x_0 : x_1 : x_2) = (A_0(t_0, t_1) : A_1(t_0, t_1) : A_2(t_0, t_1))$, es decir, la matriz

$$M := \begin{pmatrix} x_0 & x_1 & x_2 \\ A_0(t_0, t_1) & A_1(t_0, t_1) & A_2(t_0, t_1) \end{pmatrix}$$

tiene rango uno. Esto quiere decir que existe una raíz común $(t_0 : t_1) \in \mathbb{P}_k^1$ de los polinomios

$$x_0A_2 - x_2A_0, \quad x_0A_1 - x_1A_0, \quad x_1A_2 - x_2A_1$$

de $k[T_0, T_1]$. Por tanto, sus resultante homogéneas dos a dos son cero, y dichas resultantes consisten en sustituir X_0, X_1, X_2 por x_0, x_1, x_2 en las resultantes de (i) (aunque alguno de los tres polinomios fuera cero). Por tanto, se anulan todos los $x_i^d F(x_0, x_1, x_2)$. Como

algún x_i debe ser distinto de cero, entonces necesariamente $F(x_0, x_1, x_2) = 0$, luego está en la curva $V(F)$.

Recíprocamente, sea $(x_0 : x_1 : x_2) \in V(F)$, y veamos que está en C. Supongamos, por ejemplo, $x_0 \neq 0$ (siendo los otros casos simétricos). De (i) sabemos que entonces que, al sustituir X_0, X_1, X_2 por x_0, x_1, x_2 en $\mathrm{Res}(X_0A_1 - X_1A_0, X_0A_2 - X_2A_0)$, se obtiene el valor cero. Esto implica que los polinomios $x_0A_1 - x_1A_0, x_0A_2 - x_2A_0$ tienen algún factor común (o bien porque alguno de ellos es cero o bien porque la resultante de ambos polinomios es cero), y por tanto alguna raíz común, ya que k es algebraicamente cerrado. Si llamamos $(t_0 : t_1) \in \mathbb{P}^1_k$ a esa raíz común, de (*) y de $x_0 \neq 0$ se sigue también que $(t_0 : t_1)$ es también raíz de $x_1A_2 - x_2A_1$, por lo que la matriz M anterior tiene rango uno y por tanto $(x_0 : x_1 : x_2) = (A_0(t_0, t_1) : A_1(t_0, t_1) : A_2(t_0, t_1))$ (como A_0, A_1, A_2 no tienen un factor común, no se anulan los tres a la vez en $(t_0 : t_1)$).

Veamos finalmente que F no es nulo, es decir, que C no es todo $\mathbb{P}^2_k$. En efecto, algún $A_i \neq 0$, lo que quiere decir que sólo hay una cantidad finita de valores $(t_0 : t_1)$ tales que $A_i(t_0, t_1) = 0$. Por tanto, la intersección de C con la recta $V(X_i)$ es un conjunto finito de puntos, por lo que C no puede ser todo $\mathbb{P}^2_k$. □

Definición. Una *curva parametrizable* es una curva como en el Teorema 4.9.

Teorema 4.10. *Toda curva parametrizable es irreducible.*

Demostración: Supongamos que podemos escribir

$$\left\{(A_0(t_0, t_1) : A_1(t_0, t_1) : A_2(t_0, t_1)) \in \mathbb{P}^2_k \mid (t_0 : t_1) \in \mathbb{P}^1_k\right\} = V(F) \cup V(G)$$

Por tanto $F(A_0(t_0, t_1), A_1(t_0, t_1), A_2(t_0, t_1)) \cdot G(A_0(t_0, t_1), A_1(t_0, t_1), A_2(t_0, t_1)) = 0$ para todo $(t_0 : t_1) \in \mathbb{P}^1_k$, luego

$$F(A_0(T_0, T_1), A_1(T_0, T_1), A_2(T_0, T_1)) \cdot G(A_0(T_0, T_1), A_1(T_0, T_1), A_2(T_0, T_1)) = 0$$

como polinomios en $k[T_0, T_1]$ (por ser k infinito). Por tanto, alguno de los dos factores es cero. Si, por ejemplo $F(A_0(T_0, T_1), A_1(T_0, T_1), A_2(T_0, T_1)) = 0$, entonces necesariamente

$$\left\{(A_0(t_0, t_1) : A_1(t_0, t_1) : A_2(t_0, t_1)) \in \mathbb{P}^2_k \mid (t_0 : t_1) \in \mathbb{P}^1_k\right\} \subset V(F)$$

luego se da necesariamente la igualdad. Esto demuestra que la curva es o bien $V(F)$ o bien $V(G)$, con lo que es irreducible □

El resultado anterior implica que, en el Teorema 4.9, el polinomio F que aparece es necesariamente la potencia de un polinomio irreducible. No siempre ocurre que el exponente es uno:

Ejemplo 4.11. Veamos cómo funciona el Teorema 4.9 en los casos del Ejemplo 4.3. Si empezamos con la parametrización del Ejercicio 1.7, es decir, $A_0 = T_0^2$, $A_1 = T_0T_1$, $A_2 = T_1^2$, entonces, por ejemplo, $\mathrm{Res}(X_0A_1 - X_1A_0, X_0A_2 - X_2A_0) = X_0^2(X_0X_2 - X_1^2)$, con lo que obtenemos de nuevo la cónica $V(X_0X_2 - X_1^2)$. Si en cambio tomamos tres polinomios linealmente dependientes, como $A_0 = T_0^2$, $A_1 = T_1^2$, $A_2 = T_0^2 + T_1^2$, entonces $\mathrm{Res}(X_0A_1 - X_1A_0, X_0A_2 - X_2A_0) = X_0^2(X_0 + X_1 - X_2)^2$, con lo que obtenemos la recta $V(X_0 + X_1 - X_2)$. El exponente dos con que aparece la ecuación indica que la recta está recorrida dos veces.

Las parametrizaciones homogéneas explican un poco mejor las parametrizaciones afines, y por qué en este caso se suelen necesitar denominadores:

Ejemplo 4.12. Retomemos la curva $V(2XY - X - Y)$ del Ejemplo 4.1. Ya hemos visto que su completado proyectivo $V(2X_1X_2 - X_0X_1 - X_0X_2)$ se podía parametrizar mediante $(t_1^2 - t_0^2 : t_1^2 - t_0t_1 : t_1^2 + t_0t_1)$. Al deshomogeneizar respecto de X_0 es cuando obtenemos denominadores, que se anulan precisamente para los valores $(t_0 : t_1) = (1 : 1), (1 : -1)$, que dan los puntos del infinito de la curva, mientras que al deshomogeneizar el parámetro respecto de T_0 es cuando perdemos el punto $(1, 1)$, que corresponde al valor infinito del parámetro. Parece claro entonces que se puede mejorar la parametrización, haciendo corresponder al valor infinito del parámetro un punto del infinito del parámetro. Por ejemplo, podemos componer con nuestra parametrización cualquier proyectividad de $\mathbb{P}^1_k$ que mande $(0 : 1)$ (el punto del infinito de la recta) a $(1 : 1)$ (el valor del parámetro que corresponde al punto del infinito $(0 : 0 : 1)$). Esto puede conseguirse, por ejemplo, con $(t_0' : t_1') \mapsto (t_0 : t_1) = (t_0' + t_1' : t_1')$. Se obtiene así una nueva parametrización

$$(t_0' : t_1') \mapsto \left(t_1'^{\,2} - (t_0' + t_1')^2 : t_1'^{\,2} - (t_0' + t_1')t_1' : t_1'^{\,2} + (t_0' + t_1')t_1'\right) =$$
$$= (-t_0'^{\,2} - 2t_0't_1' : -t_0't_1' : t_0't_1' + 2t_1'^{\,2})$$

que, deshomogeneizando tanto respecto de t_0' como de X_0, produce una nueva parametrización de $V(2XY - X - Y)$ de la forma

$$t' \mapsto \left(\frac{t'}{1 + 2t'}, -t'\right).$$

Obsérvese que siempre quedará una parametrización con denominadores, ya que el valor infinito del parámetro sólo puede ir a uno de los dos puntos del infinito. En realidad, sólo se pueden parametrizar sin denominadores las curvas con un sólo punto del infinito y de forma que por ese punto "se pase sólo una vez" (el dar sentido a esta expresión será uno de los objetivos fundamentales de este curso).

Definición. Sea $\varphi : \mathbb{P}^1_k \to \mathbb{P}^2$ una parametrización de una curva. Se llama *reparametrización de la curva*, o bien *parametrización equivalente* a toda parametrización de la forma $\varphi \circ \psi$, donde ψ es una proyectividad de $\mathbb{P}^1_k$.

Observación 4.13. Para las curvas parametrizables es fácil dar otra "demostración" del Teorema de Bézout. En efecto, si tenemos una parametrización φ_{A_0,A_1,A_2} de grado d que "sólo da una vuelta" (es decir, que el polinomio F del Teorema 4.9 es irreducible), entonces, para cualquier $G \in k[X_0.X_1X_2]$ homogéneo de grado e, el polinomio $P(T_0,T_1) := G(A_0,A_1,A_2) \in k[T_0,T_1]$ es homogéneo de grado de (salvo que sea cero, lo que es equivalente a decir que G es divisible por F). Por tanto, P tiene de soluciones contadas con su multiplicidad. Como cada raíz de P da un punto de la curva $V(F)$, la multiplicidad de intersección de $V(F)$ y $V(G)$ en cada punto puede definirse como la suma de las multiplicidades de las raíces que corresponden al punto (recuérdese que la curva puede pasar varias veces por el mismo punto, es decir, que un mismo punto puede corresponder a varios valores del parámetro). Además, si reparametrizamos la curva, el nuevo polinomio P' consistirá en aplicar a P el cambio de variable, por lo que los factores y sus multiplicidades serán los correpondientes transformados de P. Por tanto, esta noción de multiplicidad de intersección es invariante por reparametrizaciones.

Además, es invariante por cambio de coordenadas. En efecto, si hacemos el cambio $(X_0\ X_1\ X_2) = (X_0'\ X_1'\ X_2')M$, donde M es una matriz invertible de orden 3, la nueva parametrización será $(A_0'\ A_1'\ A_2') := (A_0\ A_1\ A_2)M^{-1}$ y la nueva ecuación de $V(G)$ será $G'(X_0',X_1',X_2') := G((X_0'\ X_1'\ X_2')M)$. Por tanto, para calcular las multiplicidades de intersección hay que calcular

$$P'(T_0,T_1) := G'(A_0',A_1',A_2') = G\big((A_0',A_1',A_2')M\big) = G(A_0,A_1,A_2) = P(T_0,T_1)$$

con lo que se obtiene el mismo polinomio.

Evidentemente, dos parametrizaciones de grado uno de una recta son siempre equivalentes (ya que cada parametrización es una proyectividad de $\mathbb{P}^1_k$ en la recta). Del mismo modo, de un clásico teorema de Chasles se deduce que dos parametrizaciones de grado dos de una cónica irreducible son siempre equivalentes. En realidad, lo mismo es cierto para parametrizaciones de grado d de curvas irreducibles de grado d. Este último resultado permitiría dar una definición mucho más general de la que damos a continuación (que es sólo para $d = 1$).

Definición. Se llama *multiplicidad de intersección de una recta L con una curva C en un punto $p \in L \cap V(F)$* a la multiplicidad de la raíz $(t_0 : t_1)$ de $F(A_0,A_1,A_2) \in k[T_0,T_1]$, donde F es una ecuación minimal de C, φ_{A_0,A_1,A_2} es una parametrización de grado uno de L y $\varphi_{A_0,A_1,A_2}(t_0 : t_1) = p$. Denotaremos a tal multiplicidad $\mathrm{mult}_p(L,C)$.

Aparte de no depender de cambios de coordenadas en el parámetro o en el plano, tal multiplicidad se puede calcular con parametrizaciones afines, lo que nos será muy útil en la sección siguiente.

5. Estudio local de puntos. Tangentes

En esta sección vamos a empezar a estudiar los distintos tipos de puntos que puede tener una curva. Lo primero que vamos a hacer es estudiar cómo pueden ser las distintas rectas que pasan por el punto.

Lema 5.1. *Sea p un punto de una curva C. Entonces, existe $r \in \mathbb{N}$ tal que $\mathrm{mult}_p(C, L) \geq r$ para toda las recta L que pasa por p, y la igualdad estricta se da sólo para un número finito de rectas (que es como mucho r).*

Demostración: En primer lugar, podemos suponer que C es afín y que el punto p es $(0,0)$. Sea f una ecuación minimal de C. Una recta que pase por $(0,0)$ tiene de ecuación implícita $\lambda X + \mu Y = 0$, y por tanto se puede parametrizar como $(\mu t, -\lambda t)$. Por tanto, la multiplicidad de intersección de la recta y la curva en $(0,0)$ será el número de veces que $f(\mu T, -\lambda T)$ pueda dividirse por T (ya que es el valor $t = 0$ el que da el origen en la parametrización de la recta). Si escribimos la descomposición en componentes homogéneas de f (llamaremos r al menor natural tal que f tiene monomios de grado r):

$$f = f_r + \ldots + f_d$$

tendremos entonces

$$f(\mu t, -\lambda t) = f_r(\mu, -\lambda)t^r + \ldots + f_d(\mu, -\lambda)t^d$$

lo que indica que la multiplicidad de intersección es al menos r, y que es mayor si y sólo si $f_r(\mu, -\lambda) = 0$, lo que ocurre si y sólo si (ver Teorema 1.13(i)) f_r es divisible por la ecuación $\lambda X + \mu Y$ de la recta. □

Definición. Se llama *multiplicidad de una curva C en un punto p* al mínimo de las multiplicidades de intersección en p de C con las rectas que pasan por p. Denotaremos por $\mathrm{mult}_p C$ a tal multiplicidad. Se llama *recta tangente a C en un punto $p \in C$* a cualquier recta L tal que $\mathrm{mult}_p(L, C) > \mathrm{mult}_p C$. Llamaremos *cono tangente a la curva C en el punto $p \in C$* a la unión de las rectas tangentes. Un *punto singular de una curva C* es un punto $p \in C$ tal que $\mathrm{mult}_p C > 1$, mientras que un *punto regular* o *no singular* o *liso* es un punto $p \in C$ tal que $\mathrm{mult}_p C = 1$. En este último caso existe una única recta tangente a C en p, que denotaremos por $\mathbb{T}_p C$.

Observación 5.2. Nótese que la descomposición $f = f_r + \ldots + f_d$ de la demostración del Lema 5.1 es en realidad el desarrollo en serie de Taylor del polinomio f en $p = (0,0)$ (para eso hace falta que la característica del cuerpo sea mayor que el grado de f). Entonces la

multiplicidad de C en p no es sino el mínimo r tal que alguna derivada de orden r de f no se anula en p. Además, la ecuación del cono tangente es f_r, y en particular, si el punto p es regular, la ecuación de la recta tangente es $f_1 = \frac{\partial f}{\partial X}(p)X + \frac{\partial f}{\partial Y}(p)Y$. Si C es ahora una curva afín de ecuación minimal f y el punto que estudiamos no es el origen, sino un punto arbitrario $p = (a, b)$, entonces basta hacer una traslación de vector (a, b) para obtener:

Proposición 5.3. *Sea C una curva afín de ecuación minimal f. Entonces:*

(i) Un punto $p \in C$ es un punto liso de C si y sólo si el par $(\frac{\partial f}{\partial X}(p), \frac{\partial f}{\partial Y}(p))$ no es idénticamente nulo. En tal caso, la ecuación de $\mathbb{T}_p C$ es $\frac{\partial f}{\partial X}(p)(X-a)+\frac{\partial f}{\partial Y}(p)(Y-b) = 0$.

(ii) Si la característica del cuerpo es cero o mayor que r, la multiplicidad de C en un punto $p = (a, b)$ es r si y sólo si r es el orden mínimo tal que alguna derivada de orden r de f en p no se anula.

Demostración: Basta hacer una traslación al origen y aplicar lo que hemos visto en la Observación 5.2. La condición sobre la característica es porque, para calcular el término i-ésimo del desarrollo en serie de Taylor hay que dividir entre $i!$, que no tiene sentido si el cuerpo es de característica positiva y menor o igual que i. Para la parte (i) no hay ningún problema con la característica, ya que depende sólo de la parte de grado uno del desarrollo en serie de Taylor. □

Observación 5.4. En el caso de característica pequeña, el criterio para estudiar la multiplicidad debe ser el de el grado de las componentes homogéneas. Por ejemplo, si consideramos el polinomio $f = X^2 + Y^3$ con coeficientes en un cuerpo de característica dos, entonces $\frac{\partial f}{\partial X} = 0$ y $\frac{\partial f}{\partial Y} = 3Y^2 = Y^2$. Por tanto, la curva $V(f)$ (que es irreducible por el Lema 2.17) tiene como único punto singular el punto $(0, 0)$ y, como hemos visto, su multiplicidad es dos, ya que f tiene parte homogénea de grado dos. Sin embargo, todas las parciales de orden dos (y por tanto, las sucesivas) son idénticamente nulas.

Lo mismo ocurrirá para la curva de ecuación $f = X^2 + Y^3 + Y^2 + Y$. En este caso, $\frac{\partial f}{\partial X} = 0$ y $\frac{\partial f}{\partial Y} = 3Y^2 + 1 = Y^2 + 1 = (Y + 1)^2 = (Y - 1)^2$, que tiene como único punto singular el $(1, 1)$ y todas las parciales de orden al menos dos son nulas. Observemos que, haciendo el cambio $X = X' + 1$, $Y = Y' + 1$, obtenemos la ecuación anterior $X'^2 + Y'^3$ luego el punto singular, que en estas nuevas coordenadas es el origen, tiene multiplicidad dos. De hecho, deshaciendo el de coordenadas, podemos escribir $f = (X - 1)^2 + (Y - 1)^3$, que sería el desarrollo en serie de Taylor en el punto singular, pero que hay que calcularlo sin derivadas (ya que no podemos dividir entre 2! ni 3!, puesto que son cero).

Estudiamos a continuación cómo estudiar la regularidad en un punto de una curva proyectiva.

Proposición 5.5. *Sea $C \subset \mathbb{P}^2_k$ una curva de ecuación minimal F y a un punto de la curva. Entonces:*

(i) El punto a es liso en C si y sólo si $(F_0(a), F_1(a), F_2(a) \neq (0,0,0)$. En tal caso, la ecuación de la recta tangente a C en a es $F_0(a)X_0 + F_1(a)X_1 + F_2(a)X_2 = 0$.

(ii) Si la característica de k es cero o mayor que r, el punto p tiene multiplicidad r en C si y sólo si todas las derivadas parciales de orden menor que r de F se anulan en p, pero alguna derivada parcial de orden r no se anula.

Demostración: Supondremos, por simplicidad, que la coordenada a_0 de a es distinta de cero, siendo simétricos los casos restantes. Entonces, la ecuación minimal de $C \cap \{X_0 \neq 0\}$ es $f(X,Y) = F(1,X,Y)$. Por tanto, decir que a es un punto no singular es equivalente a que $\frac{\partial f}{\partial X}(\frac{a_1}{a_0}, \frac{a_2}{a_0})$ y $\frac{\partial f}{\partial Y}(\frac{a_1}{a_0}, \frac{a_2}{a_0})$ no sean ambos nulos, es decir $F_1(1, \frac{a_1}{a_0}, \frac{a_2}{a_0})$ y $F_2(1, \frac{a_1}{a_0}, \frac{a_2}{a_0})$ no son ambos nulos, que es lo mismo que decir que $F_1(a)$ y $F_2(a)$ no son ambos nulos. Esto demuestra una implicación de (i). Para demostrar la otra, bastará ver que no puede ocurrir que $F_1(a)$ y $F_2(a)$ se anulen pero que no se anule $F_0(a)$. En efecto, sustituyendo las variables por las coordenadas de a en la identidad de Euler $dF = F_0X_0 + F_1X_1 + F_2X_2$, tendremos (ya que $F(a) = 0$ por ser a un punto de C) que $a_0F_0(a) = -a_1F_1(a) - a_2F_2(a)$, luego la anulación de $F_1(a)$ y $F_2(a)$ implica también la anulación de $F_0(a)$ cuando $a_0 \neq 0$.

Para calcular la recta tangente en este caso, observamos que la ecuación de la recta tangente en el plano afín $\{X_0 \neq 0\}$ es

$$\frac{\partial f}{\partial X}(a)(X - \frac{a_1}{a_0}) + \frac{\partial f}{\partial Y}(a)(Y - \frac{a_2}{a_0}) = 0$$

La ecuación homogénea de la recta será, por tanto,

$$F_1(a)(X_1 - \frac{a_1}{a_0}X_0) + F_2(a)(X_2 - \frac{a_2}{a_0}X_0) = 0$$

El coeficiente de X_0 será, por tanto $\frac{a_1F_1(a)+a_2F_2(a)}{-a_0}$ que, como ya hemos observado antes, es igual a $F_0(a)$, lo que demuestra (ii).

Finalmente, para demostrar (ii) basta demostrar que es equivalente el anularse en a de todas las derivadas de orden menor o igual que s de $F(1,X,Y)$ al anularse de todas las derivadas de orden s de F en a. Lo haremos por inducción sobre s, siendo trivial el caso $s = 0$ (y en realidad el caso $s = 1$ lo hemos hecho separadamente en (i)). Supongamos por tanto que sabemos que el resultado es cierto para $s - 1$.

Por una parte, si se anulan en a todas las derivadas parciales de orden s de F, aplicando la identidad de Euler a cada derivada parcial de orden $s-1$ tenemos

$$(d - s + 1)\frac{\partial^{s-1}F}{\partial X_0^i \partial X_1^j \partial X_2^{s-1-i-j}} =$$

$$= \frac{\partial^s F}{\partial X_0^{i+1}\partial X_1^j \partial X_2^{s-1-i-j}} X_0 + \frac{\partial^s F}{\partial X_0^{i}\partial X_1^{j+1} \partial X_2^{s-1-i-j}} X_1 + \frac{\partial^s F}{\partial X_0^{i}\partial X_1^{j} \partial X_2^{s-i-j}} X_2$$

y usando la hipótesis sobre la característica, se sigue que se anula en a cada derivada $\frac{\partial^{s-1} F}{\partial X_0^i \partial X_1^j \partial X_2^{s-1-i-j}}$ de orden $s-1$ de F. Por tanto, por hipótesis de inducción, se anulan en a todas las derivadas parciales de orden menor o igual que $s-1$ de $F(1, X, Y)$. Por tanto, se anulan en a todas las derivadas de orden menor o igual que s de $F(1, X, Y)$ (las de orden s se obtienen inmediatamente de la anulación de las correspondientes de F).

Recíprocamente, si se anulan todas las derivadas de orden menor o igual que s de $F(1, X, Y)$, entonces en particular se anulan las de orden menor o igual que $s-1$, y por hipótesis de inducción se anulan las derivadas parciales de orden $s-1$ de F. Veamos ahora por inducción sobre i que se anulan en a todas las derivadas $\frac{\partial^s F}{\partial X_0^i \partial X_1^j \partial X_2^{s-i-j}}$ de orden s. Si $i = 0$, es inmediato, por el hecho de que se anulan en a las derivadas parciales de orden s de $F(1, X, Y)$. Supongamos entonces $i > 0$ y que el resultado es cierto para $i-1$ y veámoslo para i. Aplicamos ahora la identidad de Euler a $\frac{\partial^{s-1} F}{\partial X_0^{i-1} \partial X_1^j \partial X_2^{s-i-j}}$ y tendremos

$$(d-s-1)\frac{\partial^{s-1} F}{\partial X_0^{i-1}\partial X_1^j \partial X_2^{s-i-j}} =$$

$$\frac{\partial^s F}{\partial X_0^{i}\partial X_1^j \partial X_2^{s-i-j}} X_0 + \frac{\partial^s F}{\partial X_0^{i-1}\partial X_1^{j+1} \partial X_2^{s-i-j}} X_1 + \frac{\partial^s F}{\partial X_0^{i-1}\partial X_1^{j} \partial X_2^{s+1-i-j}} X_2.$$

Como $\frac{\partial^{s-1} F}{\partial X_0^{i-1} \partial X_1^j \partial X_2^{s-i-j}}$ es una derivada de orden $s-1$, se anula en a, y también se anulan en a, por hipótesis de inducción, $\frac{\partial^s F}{\partial X_0^{i-1}\partial X_1^{j+1} \partial X_2^{s-i-j}}$ y $\frac{\partial^s F}{\partial X_0^{i-1}\partial X_1^{j} \partial X_2^{s+1-i-j}}$, ya que se deriva $i-1$ veces sobre X_0. Por tanto, también $\frac{\partial^s F}{\partial X_0^{i}\partial X_1^j \partial X_2^{s-i-j}}$ se anula en a, como queríamos demostrar. □

Observación 5.6. Nótese que, si queremos calcular los puntos singulares de una curva afín (por ejemplo la de ecuación $f = X^2 + Y^2 - 1$), no basta con estudiar los puntos que se anulan para $\frac{\partial f}{\partial X}$ y $\frac{\partial f}{\partial Y}$ (en nuestro ejemplo $\frac{\partial f}{\partial X} = 2X$ y $\frac{\partial f}{\partial Y} = 2Y$ se anulan en el punto $(0,0)$) ya que podrían no estar en la curva (como, en efecto, ocurre con el punto $(0,0)$, que no está en la curva de ecuación $f = X^2 + Y^2 - 1$). Sin embargo, en el caso proyectivo, gracias a la identidad de Euler $F_0X_0 + F_1X_1 + F_2X_2 = dF$, un punto que se anule para F_0, F_1, F_2 se anula automáticamente (salvo que el grado d sea un múltiplo de la característica del cuerpo) para F.

Veamos que la noción de tangente que hemos definido coincide con la ya conocida de Geometría Proyectiva para rectas y cónicas:

Ejemplo 5.7. Si C es una recta, entonces su ecuación minimal es de la forma $F = u_0X_0 + u_1X_1 + u_2X_2$, luego $F_0 = u_0$, $F_1 = u_1$ y $F_2 = u_2$. Esto indica que la recta tangente a C en cualquier punto es la propia recta C.

Ejemplo 5.8. Si C es una cónica, podemos escribir su ecuación minimal de la forma

$$F = (\, X_0 \quad X_1 \quad X_2 \,) M \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix}$$

donde M es una matriz simétrica (para esto necesitamos que la característica no sea dos)

$$M = \begin{pmatrix} u_{00} & u_{01} & u_{02} \\ u_{01} & u_{11} & u_{12} \\ u_{02} & u_{12} & u_{22} \end{pmatrix}$$

y por tanto

$$F = u_{00}X_0^2 + 2u_{01}X_0X_1 + 2u_{02}X_0X_2 + u_{11}X_1^2 + 2u_{12}X_1X_2 + u_{22}X_2^2$$

de donde obtenemos:

$$F_0 = 2u_{00}X_0 + 2u_{01}X_1 + 2u_{02}X_2$$

$$F_1 = 2u_{01}X_0 + 2u_{11}X_1 + 2u_{12}X_2$$

$$F_2 = 2u_{02}X_0 + 2u_{12}X_1 + 2u_{22}X_2$$

es decir

$$(\, F_0(a) \quad F_1(a) \quad F_2(a) \,) = 2\,(\, a_0 \quad a_1 \quad a_2 \,)\, M.$$

Por tanto, a es singular en C (en nuestro sentido) si y sólo si $(\, a_0 \quad a_1 \quad a_2 \,) M = 0$ (porque la característica del cuerpo no es dos), es decir, a es singular en el sentido de Geometría Proyectiva. Además, cuando a es un punto regular, la recta tangente (en nuestro sentido) tiene ecuación

$$(\, F_0(a) \quad F_1(a) \quad F_2(a) \,) \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix}$$

es decir,

$$(\, a_0 \quad a_1 \quad a_2 \,) M \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix}$$

que es la ecuación de la recta polar de a respecto de C, y por tanto la recta tangente en el sentido de Geometría Proyectiva (ver Ejemplo 8.5).

Observación 5.9. Obsérvese que, en el ejemplo anterior surgen problemas si trabajamos sobre un cuerpo de característica dos, ya que todas las derivadas parciales se anularían. En realidad, el problema en característica dos es que no se puede hablar de la matriz de una cónica (ya que las entradas de la matriz de fuera de la diagonal son coeficientes de la

ecuación de la cónica divididos por 2, que en este caso es cero). Si nos cogemos la ecuación más sencilla de una cónica, $F = X_0X_2 - X_1^2$, tendremos

$$F_0 = X_2$$

$$F_1 = 0$$

$$F_2 = X_0.$$

Como el punto $(0 : 1 : 0)$ no está en la cónica, la cónica es lisa. El hecho de que F_1 sea idénticamente cero quiere decir que el coeficiente de X_1 de cualquier recta tangente es siempre cero. En otras palabras, todas las rectas tangentes pasan por el punto $(0 : 1 : 0)$. Las curvas que satisfacen esta propiedad de que todas sus tangentes pasen por un mismo punto se llaman *curvas extrañas*, y puede demostrarse que, salvo cambio de coordenadas, esta cónica en característica dos es la única curva extraña. Una de las extrañezas principales de esta cónica es que su cónica dual es un haz de rectas, es decir, una recta en $\mathbb{P}_k^{2^*}$, por lo que ya no es cierto que la dual de la dual sea la propia cónica(*). En general, cuando uno tiene que derivar, se encuentra con problemas de este tipo cuando la característica del cuerpo es baja. Aunque basta suponer que la característica sea mayor que el grado de la curva en la que trabajemos, **a partir de ahora supondremos que nuestro cuerpo base tiene característica cero**, para evitar estos problemas extraños.

Ejercicio 5.10. Demostrar que el conjunto de rectas tangentes de la curva $V(X_0X_2^2 - X_1^3)$ forma una curva en $\mathbb{P}^{2^*}$ dando una ecuación en u_0, u_1, u_2 que caracterice cuándo la recta de ecuación $u_0X_0 + u_1X_1 + u_2X_2$ es tangente a la curva [Indicación: Parametrizar la curva y, para cada punto de ella, calcular la recta tangente en función de los parámetros; comprobar entonces que el conjunto de rectas tangentes se puede parametrizar también].

Observación 5.11. Si tenemos una curva reducible $C = V(FG)$ (con F, G primos entre sí) y tenemos un punto $a = (a_0 : a_1 : a_2)$ que esté en $V(F)$ pero no en $V(G)$, entonces es inmediato ver que a es liso en C si y sólo sí es liso en $V(F)$, y en tal caso $\mathbb{T}_aC = \mathbb{T}_aV(F)$. Más en general, C y $V(F)$ tienen en a la misma multiplicidad y el mismo cono tangente.

Veamos un modo alternativo de demostrar para curvas proyectivas lo visto hasta ahora, sin necesidad de pasar al caso afín. La clave será el siguiente:

(*) En realidad, usando la parametrización del Ejercicio 1.7, se demuestra que la tangente en el punto $(t_0^2 : t_0t_1 : t_1^2)$ es $V(t_1^2X_0 + t_0^2X_2)$, luego la curva dual se puede parametrizar como $(u_0 : u_1 : u_2) = (t_1^2 : 0 : t_0^2)$ y, como en la segunda parte del Ejemplo 4.11, obtendremos como ecuación implícita la recta doble de ecuación u_1^2, es decir el haz doble de las rectas que pasan por $(0 : 1 : 0)$.

Lema 5.12. *Sean $a, b \in k^3$ representantes de dos puntos distintos de $\mathbb{P}^2_k$ y sea $F \in k[X_0, X_1, X_2]$ un polinomio homogéneo. Si escribimos $f(T) = F(a + bT)$, entonces su expresión como polinomio en $k[T]$ empieza por*

$$f(T) = F(a + Tb) = F(a) + (F_0(a)b_0 + F_1(a)b_1 + F_2(a)b_2)T + \\ + \frac{1}{2}(b_0\ b_1\ b_2)\begin{pmatrix} F_{00}(a) & F_{01}(a) & F_{02}(a) \\ F_{10}(a) & F_{11}(a) & F_{12}(a) \\ F_{20}(a) & F_{21}(a) & F_{22}(a) \end{pmatrix}\begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} T^2 + \dots$$

Demostración: Nótese que en realidad la expresión que buscamos es el desarrollo en serie de Taylor de f en $T = 0$, que será finita por ser f un polinomio. Basta entonces observar que, aplicando la regla de la cadena para derivar $f(T) = F(a_0 + b_0T, a_1 + b_1T, a_2 + b_2T)$, se obtiene

$$f'(T) = b_0F_0(a_0 + b_0T, a_1 + b_1T, a_2 + b_2T) + \\ + b_1F_1(a_0 + b_0T, a_1 + b_1T, a_2 + b_2T) + b_2F_2(a_0 + b_0T, a_1 + b_1T, a_2 + b_2T)$$

$$f''(T) = b_0\big(b_0F_{00}(a + bT) + b_1F_{01}(a + bT) + b_2F_{02}(a + bT)\big) + \\ b_1\big(b_0F_{10}(a + bT) + b_1F_{11}(a + bT) + b_2F_{12}(a + bT)\big) + \\ b_2\big(b_0F_{20}(a + bT) + b_1F_{21}(a + bT) + b_2F_{22}(a + bT)\big)$$

Haciendo $T = 0$ se obtiene entonces

$$f(0) = F(a)$$

$$f'(0) = F_0(a)b_0 + F_1(a)b_1 + F_2(a)b_2$$

$$f''(0) = (b_0\ b_1\ b_2)\begin{pmatrix} F_{00}(a) & F_{01}(a) & F_{02}(a) \\ F_{10}(a) & F_{11}(a) & F_{12}(a) \\ F_{20}(a) & F_{21}(a) & F_{22}(a) \end{pmatrix}\begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix}$$

□

Observación 5.13. Del Lema 5.12 se sigue que, si tomamos $a \in V(F)$ (por abuso de notación escribiremos de la misma forma al punto a que al representante escogido en el lema), la recta que pasa por a y b corta a $V(F)$ con multiplicidad al menos dos si y sólo si $F_0(a)b_0 + F_1(a)b_1 + F_2(a)b_2 = 0$, con lo que volvemos a obtener que los puntos b de la recta tangente a C en a son los que satisfacen dicha ecuación.

Definición. La matriz $M_F = \begin{pmatrix} F_{00} & F_{01} & F_{02} \\ F_{10} & F_{11} & F_{12} \\ F_{20} & F_{21} & F_{22} \end{pmatrix}$ se llama *matriz hessiana del polinomio* F, y su determinante H_F se llama *hessiano del polinomio* F (nótese que, si F es homogéneo de grado d, entonces H_F es homogéneo de grado $3(d-2)$). Denotaremos por $M_F(a)$ y $H_F(a)$ a los valores de M_F y H_F en un punto a.

El hecho de que la matriz Hessiana aparezca en un desarrollo en serie de Taylor relativo a F sugiere que, lo mismo que la parte de grado uno representa la recta más cercana a $V(F)$ en a, la matriz hessiana representará a una cónica muy parecida a $V(F)$ y a su recta tangente en a. El siguiente resultado nos confirma esto.

Lema 5.14. *Sea $C \subset \mathbb{P}^2_k$ una curva de ecuación minimal F de grado d y sea $a \in K^3$ un representante del punto $[a] \in \mathbb{P}^2_k$. Entonces:*

(i) $(a_0 \quad a_1 \quad a_2)\, M_F(a) = (d-1)\,(F_0(a) \quad F_1(a) \quad F_2(a))$.

(ii) $(a_0 \quad a_1 \quad a_2)\, M_F(a) \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} = d(d-1)F(a)$.

(iii) El punto $[a]$ está en C si y sólo si está en la cónica de matriz $M_F(a)$.

(iv) El punto $[a]$ es un punto liso de C si y sólo si es un punto liso de la cónica de matriz $M_F(a)$. Además, en tal caso, la recta tangente a dicha cónica en $[a]$ es $\mathbb{T}_a C$.

Demostración: La parte (i) se obtiene por la identidad de Euler aplicada a F_0, F_1, F_2. La parte (ii) es ahora consecuencia de (i) aplicando la identidad de Euler a F. La parte (iii) es consecuencia de (ii)$^{(*)}$.

Para la parte (iv), como a es liso para la cónica si y sólo si $aM_F(a)$ no es cero, se sigue de (i) que esto es equivalente a que $[a]$ es un punto liso de C. Además, en este caso, la ecuación de la tangente a la cónica en $[a]$ es $(a_0 \quad a_1 \quad a_2)\, M_F(a) \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix}$, que, por (i), es $(d-1)(F_0(a)X_0 + F_1(a)X_1 + F_2(a)X_2)$, y ésta es (salvo la multiplicación por $d-1$), la ecuación de $\mathbb{T}_{[a]}C$. □

Observación 5.15. En el caso en que a sea un punto doble entonces el lema está diciendo que la cónica de matriz $M_F(a)$ es un par de rectas (que pueden ser iguales si el rango de la matriz es uno) que pasan por a. Además, los puntos b de dicha cónica son los que satisfacen, por el Lema 5.12, que la multiplicidad de intersección de la curva con la recta ab en el punto a es al menos tres. Por tanto, el cono tangente a la curva en el punto a es

(*) Aquí es importante que la característica no divida a $d(d-1)$

precisamente la cónica. En general, con un poco más de trabajo se puede demostrar que el coeficiente de T^r en el desarrollo del Lema 5.12 es $F^{(r)}(b)$, donde

$$F^{(r)}(X_0, X_1, X_2) := \sum_{i_0+i_1+i_2=r} \frac{i_0!i_1!i_2!}{r!} \frac{\partial^r F}{\partial X_0^{i_0} \partial X_1^{i_1} \partial X_2^{i_2}}(a) X_0^{i_0} X_1^{i_1} X_2^{i_2}.$$

De aquí se reobtiene que la multiplicidad de una curva en un punto es el mínimo orden tal que alguna derivada de su ecuación minimal no se anula. Más aún, el cono tangente de un punto a de multiplicidad r es precisamente $V(F^{(r)})$.

Otra aplicación del Lema 5.12 es calcular la multiplicidad de intersección de una curva con su recta tangente en un punto. Lo esperado es que tal multiplicidad sea dos, pero en casos especiales será mayor.

Definición. Un punto regular de una curva se dice que es un *punto de inflexión* si la multiplicidad de intersección en el punto de la curva y de su recta tangente es al menos tres. Si la multiplicidad de intersección es tres se dice que es un *punto de inflexión ordinario.*

Teorema 5.16. *Si $C \subset \mathbb{P}_k^2$ es una curva de ecuación minimal F, entonces $C \cap V(H_F) = \mathrm{Sing}(C) \cup \mathrm{Flex}(C)$, donde Flex$(C)$ es el conjunto de puntos de inflexión de C.*

Demostración: En primer lugar, del Lema 5.14 se sigue que los puntos singulares de C están en $V(H_F)$. Por tanto, basta ver que un punto liso $a \in C$ es de inflexión si y sólo si está en $V(H_F)$. Del Lema 5.12 se sigue que el punto a es un punto de inflexión si y sólo si cada punto $b = (b_0 : b_1 : b_2)$ de la recta tangente satisface

$$(b_0\ b_1\ b_2) \begin{pmatrix} F_{00}(a) & F_{01}(a) & F_{02}(a) \\ F_{10}(a) & F_{11}(a) & F_{12}(a) \\ F_{20}(a) & F_{21}(a) & F_{22}(a) \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} = 0,$$

es decir, que la cónica definida por la matriz Hessiana contiene a la recta tangente a C en a, luego en particular es una cónica degenerada y la matriz Hessiana tiene determinante nulo, es decir $a \in V(H_F)$.

Recíprocamente, si $H_F(a) = 0$ implica que la cónica de matriz $M_F(a)$ es un par de rectas, y por el Lema 5.14 (y la Observación 5.11), una de las rectas debe ser $\mathbb{T}_a C$. □

Ejemplo 5.17. Sea $F = X_0X_2^2 - X_1^3$. Entonces es fácil ver que

$$M_F = \begin{pmatrix} 0 & 0 & 2X_2 \\ 0 & -6X_1 & 0 \\ 2X_2 & 0 & 2X_0 \end{pmatrix}$$

por lo que $H_F = 24X_1X_2^2$. Entonces $V(F) \cap V(H_F)$ consiste sólo en el punto singular $(1:0:0)$ y el punto $(0:0:1)$, que es no singular, luego es un punto de inflexión. Puede verse también que en esta intersección el punto de inflexión aparece sólo al intersecar con la parte $V(X_1)$ de $V(H_F)$, y que la multiplicidad de intersección es 1. Por tanto, el punto singular $(1:0:0)$ aparece con multiplicidad de intersección 8 al cortar $V(F)$ y $V(H_F)$, a pesar de tener sólo multiplicidad 2 como punto de la curva.

Obsérvese también que, si queremos calcular los puntos de inflexión de una curva afín, el modo más eficiente es calcular los puntos de inflexión de su proyectado proyectivo. Por ejemplo, la curva $V(Y^2-X^3)$ no tiene puntos de inflexión, ya que su completado proyectivo $V(X_0X_2^2-X_1^3)$ acabamos de ver que sólo tiene al punto $(0:0:1)$ como punto de inflexión, y es un punto de la recta del infinito.

En realidad, muchas veces para estudiar una curva afín conviene estudiar su comportamiento en sus puntos del infinito. Recordamos los siguientes dos ejemplos de Geometría Proyectiva.

Ejemplo 5.18. Consideremos la hipérbola $V(XY-1)$. Su completado proyectivo es la cónica $X_1X_2 - X_0^2$, que tiene como puntos del infinito $(0:1:0)$ y $(0:0:1)$. Las rectas tangentes en ellos son, respectivamente, $V(X_2)$ y $V(X_1)$, y sus restricciones al afín son $V(Y)$ y $V(X)$, que son precisamente las asíntotas de la hipérbola.

Ejemplo 5.19. Si consideramos ahora la parábola $V(Y-X^2)$, su completado proyectivo es $V(X_0X_2 - X_1^2)$, que tiene un único punto en el infinito, el $(0:0:1)$. La recta tangente en dicho punto es ahora $V(X_0)$, la recta del infinito, luego no produce ninguna recta en el afín. De hecho, el modo de aproximarse la parábola al punto del infinito (que representa la dirección vertical) no es, en este caso, asintótico.

Los ejemplos anteriores justifican las siguiente definiciones:

Definición. Se llama *asíntota de una curva afín* a toda recta afín cuyo completado proyectivo sea una recta tangente al completado proyectivo de la curva en algún punto del infinito. Se dice que una curva afín tiene una *rama parabólica* en una dirección dada si el completado proyectivo de la curva pasa por el punto del infinito correspondiente a dicha dirección, y la recta del infinito es tangente al completado proyectivo en ese punto.

Observación 5.20. En las definiciones anteriores las tangentes pueden serlo en puntos singulares. Incluso un mismo punto del infinito puede dar lugar a la vez a una asíntota y una rama parabólica. Por ejemplo, consideremos la curva de ecuación minimal $f = 1+XY+X^3$. Su completado proyectivo es la curva de ecuación mimimal $X_0^3 + X_0X_1X_2 + X_1^3$, así que su único punto en el infinito es el $(0:0:1)$. Deshomogeneizando respecto de X_2, se comprueba que el cono tangente en dicho punto es el par de rectas $V(X_0X_1)$. La primera

de las rectas prueba que la curva tiene una rama parabólica vertical, mientras la segunda da lugar a la asíntota $V(X)$.

6. Estudio local de puntos. Ramas

En la sección anterior hemos visto que la multiplicidad de intersección de una curva con una recta en un punto se puede calcular bien gracias a que la recta se puede parametrizar. De hecho, el tener una curva parametrizada, nos permite saber también "cuántas veces" pasa la curva por cada punto, ya que el mismo punto puede venir de varios valores distintos del parámetro. En esta sección, definiremos de modo más formal el número de veces que una curva pasa por un punto (ésa será la noción de rama: cada forma distinta de pasar una curva por un punto).

Lo primero que veremos es que, de un modo "formal", toda curva se puede parametrizar cerca de cualquier punto. De hecho, para puntos lisos, eso es lo que diría el teorema de la función implícita en el caso en que el cuerpo base sea $\mathbb{C}$. Además, en este caso, nos esperamos que haya una sola rama. Antes de iniciar la teoría específica, veamos en un ejemplo cómo se haría eso:

Ejemplo 6.1. Sea la curva de ecuación minimal $f = X^2 - Y^3 + 2Y^2 - Y$. Como $\frac{\partial f}{\partial y}(0,0) = -1 \neq 0$, el teorema de la función implícita dice que existirá una función $g(X)$ (definida en un entorno de $X = 0$) tal que $g(0) = 0$ y $f(X, g(X)) = 0$. De esta función g se puede obtener mucha información, por ejemplo sus derivadas en el origen, a base de ir derivando. En efecto, derivando en la igualdad $X^2 - g(X)^3 + 2g(X)^2 - g(X) = 0$, se obtendrá

$$2X - 3g'(X)g(X)^2 + 4g'(X)g(X) - g'(X) = 0$$

luego, haciendo $X = 0$ y sabiendo que $g(0) = 0$ se obtiene $g'(0) = 0$. Obviamente se puede reiterar el proceso y calcular $g''(0) = 2$ y en general, por recurrencia, cada derivada. De este modo, podemos determinar todo el desarrollo en serie de Taylor de g en $X = 0$. Si estamos en el caso de funciones analíticas sobre los complejos, el desarrollo en serie de Taylor determina completamente la función. De hecho, en pocos cuerpos más tiene sentido hablar de desarrollo en serie de Taylor que converja a una función, pero aún así podemos seguir escribiendo en modo meramente formal, sin pensar en convergencia, una serie infinita $g(X) = a_0 + a_1X + a_2X^2 + \ldots$. No tendrá sentido evaluar en ningún punto salvo en $X = 0$, y será $g(0) = a_0$, luego la condición $g(0) = 0$ se traduce en $a_0 = 0$. El resto de coeficientes, en lugar de con el teorema de la función implícita, se pueden intentar calcular usando la igualdad

$$X^2 - (a_0 + a_1X + a_2X^2 + \ldots)^3 + 2(a_0 + a_1X + a_2X^2 + \ldots)^2 - (a_0 + a_1X + a_2X^2 + \ldots) = 0$$

en que, igualando a cero cada coeficiente (empezando por el término independiente), obtenemos

$$-a_0^3 + 2a_0^2 - a_0 = 0$$

$$-3a_0^2a_1 + 4a_0a_1 - a_1 = 0$$
$$1 - 3a_0^2a_2 - 3a_0a_1^2 + 4a_0a_2 + 2a_1^2 - a_2 = 0$$
$$\vdots$$

La primera ecuación en realidad no dice nada nuevo, porque ya sabemos que $a_0 = 0$. A partir de aquí, la segunda ecuación implica $a_1 = 0$ (que corresponde a $g'(0) = 0$, que ya vimos). De nuevo, usando ahora la tercera ecuación, se tiene $a_2 = 1$ (que corresponde ahora a $g''(0) = 2$). No es difícil ver que cada ecuación nos dará el valor de cada a_i en función de $a_0, a_1, \ldots, a_{i-1}$, con lo que se pueden calcular por recurrencia todos los coeficientes de la serie $g(X)$.

Nótese también que en realidad la primera ecuación da otra posibilidad para a_0, que es $a_0 = 1$. Esto es porque la curva pasa también por el punto $(0, 1)$, que resulta ser un punto singular. Precisamente por ello, el teorema de la función implícita no garantiza la existencia de una función $g(X)$ tal que $g(0) = 1$ y $f(X, g(X)) = 0$. Sin embargo, si ahora hacemos $a_0 = 1$, y empezamos la iteración anterior, la segunda ecuación no da ninguna restricción ya que se anula idénticamente. Pasando a la tercera ecuación, obtenemos $1 - a_1^2 = 0$, lo que ahora da dos posibilidades para a_1 (y por tanto, dos series distintas). Aunque ahora no sea tan inmediato, para cada solución $a_1 = 1$ y $a_1 = -1$ se obtiene por recurrencia ya una única serie $g(X)$ con $f(X, g(X)) = 0$. La justificación geométrica es fácil: resulta que la curva pasa dos veces por el punto $(0, 1)$ (y sus rectas tangentes son $V(X - Y + 1)$ y $V(X + Y - 1)$), y cada una de las veces que pasa corresponde a la "parametrización" $(T, g(T))$ (nótese que $(1, g'(0))$ da precisamente el vector director de cada recta tangente).

En esta sección, demostraremos que el método anterior (con alguna pequeña variación) funciona siempre, y daremos un algoritmo explícito para calcular más fácilmente los posibles desarrollos en series en cada punto, ya sea singular o no.

Definición. Se llama *serie formal de potencias* en la indeterminada T con coeficientes en un anillo A a una expresión de la forma $p(T) = a_0 + a_1T + a_2T^2 + \ldots$, con $a_0, a_1, a_2, \ldots \in A$. Con las operaciones naturales de suma y producto, las series formales forman un anillo que denotaremos por $A[[T]]$. Por analogía con los desarrollos en serie de Taylor, escribiremos $p(0) := a_0$ y $p'(0) := a_1$.

El siguiente resultado (o más bien la demostración) muestra que, para trabajar con series de potencias, basta trabajar formalmente.

Lema 6.2. *Sea $f = a_0 + a_1T + \ldots \in k[[T]]$ una serie formal. Entonces:*

(i) Existe una única serie $g \in k[[T]]$ tal que $fg = 1$ si y sólo si $a_0 \neq 0$.

(ii) Si $a_0 \neq 0$, para cada $n \in \mathbb{N}$ no divisible por la característica de k y cada b_0 tal que $b_0^n = a_0$, existe una única serie $g \in k[[T]]$ tal que $g^n = f$ y $g(0) = b_0$.

Demostración: Para (i), si $f = a_0 + a_1T + a_2T^2 + \ldots$, buscamos $g = b_0 + b_1T + b_2T^2 + \ldots$ tal que

$$a_0b_0 = 1$$

$$a_0b_1 + a_1b_0 = 0$$

$$a_0b_2 + a_1b_1 + a_2b_0 = 0$$

$$\vdots$$

De la primera ecuación ya se deduce que $a_0 \neq 0$ es una condición necesaria, así que veamos que es también suficiente.

Como $a_0 \neq 0$, entonces de la primera ecuación sacamos una única posibilidad para b_0, que es $b_0 = \frac{1}{a_0}$. A partir de este valor de b_0, la segunda ecuación nos dice que hay una única posibilidad para b_1. En general, conocidos los valores de $b_0, b_1, \ldots, b_{i-1}$ a partir de las i primeras ecuaciones, la ecuación $a_0b_i + a_1b_{i-1} + \ldots + a_ib_0 = 0$ da una única posibilidad para b_i (usando de nuevo que a_0 no se anula). Por tanto, por recurrencia, obtenemos una única serie g

Para (ii), se usa también recurrencia, aunque sea un poco más lioso de escribir. De nuevo buscamos una serie $g = b_0 + b_1T + b_2T^2 + \ldots$ que esta vez debe cumplir

$$b_0^n = a_0$$

$$\binom{n}{1} b_0^{n-1} b_1 = a_1$$

$$\binom{n}{2} b_0^{n-2} b_1^2 + \binom{n}{1} b_0^{n-1} b_2 = a_2$$

$$\binom{n}{3} b_0^{n-3} b_1^3 + \frac{n!}{(n-2)!1!1!} b_0^{n-2} b_1 b_2 + \binom{n}{1} b_0^{n-1} b_3 = a_3$$

$$\vdots$$

Aunque no sea fácil escribir la ecuación general, lo importante ahora son dos cosas. La primera, que de la primera ecuación obtenemos tantas posibilidades para b_0 como raíces n-ésimas tenga a_0 (que siempre existen al ser k un cuerpo algebraicamente cerrado, y serán exactamente n ya que la característica de k no es un divisor de n). La segunda es que, una vez fijado un valor de b_0, podemos como antes calcular cada b_i de forma única en función de $b_0, b_1, \ldots, b_{i-1}$ y a_i. En efecto, cada expresión para a_i es la suma de todos los posibles $\frac{n!}{n_0!\ldots n_i!} {b_0}^{n_0} {b_1}^{n_1} \ldots {b_i}^{n_i}$ con $0 \cdot n_0 + 1 \cdot n_1 + \ldots i \cdot n_i = i$. En particular, la incógnita b_i sólo aparece en el sumando $\binom{n}{1} b_0^{n-1} b_i$, luego se puede despejar en función de $b_0, b_1, \ldots, b_{i-1}$ y a_i (porque $b_0 \neq 0$, y también $n \neq 0$ como elemento de k, por la hipótesis

sobre la característica). Como en el caso (i), se construyen así por recurrencia tantas series como posibles valores de b_0. □

La parte (i) del resultado anterior está diciendo que las unidades del anillo $k[[T]]$ son las series que tienen término independiente no nulo. Por tanto, cada serie distinta de cero se podrá escribir de forma única como $T^r p$ donde p es una unidad. Esto demuestra que el producto de dos series no nulas es no nula (luego $k[[T]]$ es un dominio de integridad) y además el cociente de dos series siempre se puede escribir de la forma $\frac{p(T)}{T^r}$, es decir, una serie infinita en que una cantidad finita de términos pueden tener exponente negativo (en otras palabra, una serie de Laurent).

Definición. Denotaremos con $k((T))$ al cuerpo de fracciones de $k[[T]]$. Cada elemento no nulo $p \in k((T))$ se puede escribir de forma única como $p = T^r q(T)$, con $r \in \mathbb{Z}$ y $q(T) \in k[[T]]$ con $q(0) \neq 0$ (es decir, r es el menor exponente de T que tiene coeficiente no nulo en p). Diremos que r es el *orden* de p, y lo escribiremos como $O(p)$. Por convenio, $O(0) = \infty$

Ejercicio 6.3. Demostrar que el orden de $k((T))^*$ satisface las siguientes propiedades:

(i) $O(fg) = O(f) + O(g)$

(ii) $O(f + g) \geq \min\{O(f), O(g)\}$, dándose la igualdad cuando $O(f) \neq O(g)$.

(iii) $O(f) \geq 0$ si y sólo si $f \in k[[T]]$.

(iv) $O(f) > 0$ si y sólo si $f \in k[[T]]$ y f no es una unidad.

Generalizamos ahora el Ejemplo 6.1. Consideraremos no sólo polinomios en X, Y, sino que permitiremos que sean series formales en X (en realidad, el resultado es cierto cuando trabajamos con series formales en X, Y, pero es un concepto que no necesitaremos usar).

Teorema 6.4 (de la función implícita formal)**.** *Sea $f(X, Y) \in k[[X]][Y]$ tal que $f(0, 0) = 0$ y $\frac{\partial f}{\partial Y}(0, 0) \neq 0$. Entonces existe una única serie formal $p \in k[[X]]$ tal que $p(0) = 0$ y $f(X, p(X)) = 0$.*

Demostración: Escribimos

$$f = p_0(X) + p_1(X)Y + \ldots + p_d(X)Y^d$$

donde $p_0, p_1, \ldots, p_d \in k[[X]]$. Más concretamente escribiremos

$$p_0(X) = a_{00} + a_{01}X + a_{02}X^2 + \ldots$$

$$p_1(X) = a_{10} + a_{11}X + a_{12}X^2 + \ldots$$

$$\vdots$$

$$p_d(X) = a_{d0} + a_{d1}X + a_{d2}X^2 + \dots$$

Las hipótesis del enunciado equivalen a decir que $a_{00} = 0$ y $a_{10} \neq 0$. Tenemos que ver que existe una única expresión

$$p(X) = b_1X + b_2X^2 + \dots$$

tal que

$$p_0(X) + p_1(X)(b_1X + b_2X^2 + \dots) + \dots + p_d(X)(b_1X + b_2X^2 + \dots)^d = 0$$

Si en la identidad anterior igualamos a cero cada coeficiente de X^i (obsérvese que no hay término independiente por ser $a_{00} = 0$), obtendremos, para el coeficiente de X,

$$a_{01} + a_{10}b_1 = 0$$

lo que da como único posible valor $b_1 = -\frac{a_{01}}{a_{10}}$. Para el coeficiente de X^2 tendremos

$$a_{02} + a_{11}b_1 + a_{10}b_2 + a_{20}b_1^2$$

que de nuevo permite calcular ahora de forma única b_2 en función de $a_{02}, a_{11}, b_1, a_{10}, a_{20}$. Como b_1 lo tenemos determinado de antes, podemos determinar el único posible valor de b_2. En general, el coeficiente de X^i para i general será más complicado de escribir, pero tendrá el aspecto

$$(\text{expresión en algunos } a_{jk} \text{ y en } b_1, b_2, \dots, b_{i-1}) + a_{10}b_i = 0$$

lo que de nuevo permite determinar de forma única el valor de b_i. □

El resultado anterior permite dar una parametrización de una curva $V(f)$ cerca del punto $(0,0)$, suponiendo que sea un punto liso de la curva. En efecto, $X = t, Y = p(t)$ sería una parametrización de la curva, aunque en realidad p no tome valores. Obsérvese que, al querer despejar la Y en función de la X como serie formal sólo tiene sentido tomar el valor $X = 0$. Podríamos generalizarlo todo tomando series formales de la forma $p(T - a)$, pero preferimos a partir de ahora estudiar puntos de la forma $(0, b)$ (cosa que siempre podremos conseguir con una simple traslación). Muchas veces supondremos también $b = 0$.

Definición. Se llama *parametrización formal en* (a, b) *de una curva afín* de ecuación minimal f a un par $(p(T), q(T))$ de series formales $p, q \in k[[T]]$ tales que $f(p, q) = 0$, $p(0) = a$ y $q(0) = b$.

Como hemos dicho, por comodidad, trabajaremos muchas veces con parametrizaciones formales en $(0,0)$, algo que siempre se puede conseguir con una traslación. Análogamente, se puede dar la definición para curvas proyectivas

Definición. Se llama *parametrización formal en* $(a_0 : a_1 : a_2)$ *de una curva proyectiva* de ecuación minimal F a una terna $(p_0(T), p_1(T), p_2(T))$ de series formales no todas de orden estrictamente positivo tales que $F(p_0, p_1, p_2) = 0$ y $(p_0(0) : p_1(0) : p_2(0)) = (a_0 : a_1 : a_2)$.

Observación 6.5. Obsérvese que, en el caso proyectivo, multiplicar las series formales de una parametrización por una unidad en $k[[T]]$ (es decir, una serie con término independiente no nulo), produce una nueva parametrización, que puede considerarse equivalente. En realidad, una parametrización formal de una curva proyectiva podría verse como un punto de $\mathbb{P}^2_{k((T))}$. En efecto, dados tres elementos $p_0, p_1, p_2 \in k((T))$ no todos nulos, dividiendo todos ellos por T^r, donde r es el máximo de los órdenes de p_0, p_1, p_2 obtendremos tres series formales, y no todas de orden estrictamente positivo. Nótese que si, por ejemplo, $a_0 \neq 0$, entonces una parametrización formal $(p_0(T), p_1(T), p_2(T))$ en $(a_0 : a_1 : a_2)$ es equivalente a $(1, \frac{p_1(T)}{p_0(T)}, \frac{p_2(T)}{p_0(T)})$. Como, por el Lema 6.2(i), p_0 es una unidad en $k[[T]]$, se obtiene una parametrización formal de la curva afín $V(F) \cap \{X_0 \neq 0\}$.

Ejemplo 6.6. Volvamos a la curva $V(2XY - X - Y)$ del Ejemplo 4.1. La teníamos parametrizada mediante $(\frac{T}{T+1}, \frac{T}{T-1})$. Ahora bien, por el Lema 6.2(ii), si vemos $T + 1$ y $T - 1$ como series formales, tienen inversa para el producto, y se ve enseguida

$$\frac{1}{1+T} = 1 - T + T^2 - T^3 + \dots$$

$$\frac{1}{-1+T} = -1 - T - T^2 - T^3 - \dots$$

luego podemos parametrizar la curva mediante

$$(X, Y) = (T - T^2 + T^3 - T^4 + \dots, -T - T^2 - T^3 - T^4 - \dots)$$

(ya vimos en el Ejemplo 4.12 que era imposible parametrizarla por polinomios). A partir de aquí es fácil sacar también una parametrización como la del Teorema de la Función Implícita. En efecto, bastaría despejar de la igualdad $X = T - T^2 + T^3 - T^4 + \dots$ la T en función de la X y sustituir luego en la expresión de Y. El modo de hacer esto es, de nuevo, suponer que podemos escribir $T = a_1X + a_2X^2 + a_3X^3 + \dots$ (nótese que para $X = 0$ debemos obtener el valor $T = 0$, por lo que la serie formal no tiene término independiente), y entonces debería ser

$$(a_1X + a_2X^2 + a_3X^3 + \dots) - (a_1X + a_2X^2 + a_3X^3 + \dots)^2 +$$

$$+(a_1X + a_2X^2 + a_3X^3 + \ldots)^3 - (a_1X + a_2X^2 + a_3X^3 + \ldots)^4 + \ldots = X$$

luego, igualando coeficientes, debe ser

$$a_1 = 1$$

$$a_2 - a_1^2 = 0$$

$$a_3 - 2a_1a_2 + a_1^3 = 0$$

$$\vdots$$

lo que va dando por recurrencia $a_1 = 1$, $a_2 = 1$, $a_3 = 1, \ldots$ (en realidad, se puede obtener directamente de $X = \frac{T}{T+1}$ que $T = \frac{X}{1-X} = X + X^2 + X^3 + \ldots$, pero queríamos hacer énfasis en el método general, con vistas al próximo Teorema 6.7). Con esta expresión, ya podemos calcular el valor de Y en función de X, concretamente:

$$Y = -T - T^2 - T^3 - T^4 - \ldots = -(X + X^2 + X^3 + \ldots) - (X + X^2 + X^3 + \ldots)^2 -$$

$$-(X + X^2 + X^3 + \ldots)^3 - (X + X^2 + X^3 + \ldots)^4 - \ldots = -X - 2X^2 - 4X^3 - \ldots$$

(como antes, esta última expresión se podía haber obtenido directamente del hecho de que la igualdad $2XY - X - Y = 0$ implica $Y = \frac{X}{2X-1}$, que desarrollado nos da la serie formal que hemos encontrado).

Este ejemplo nos muestra que, aparte de la estructura de anillo, las series formales tienen otra operación. En efecto, una serie formal debe interpretarse como un desarrollo en serie de Taylor, aunque sin preocuparse por la convergencia (aunque si $k = \mathbb{C}$, puede demostrarse que las series que salen de forma natural en esta sección son convergentes). En otras palabras, pueden considerarse como funciones de una variable en un entorno de $t = 0$. Por tanto, pueden componerse, aunque para que tenga sentido, la primera serie que operemos deberá mandar el cero al cero.

Definición. Se llama *composición de las series formales* $f, g \in k[[T]]$, donde $g(0) = 0$, a la serie $f \circ g = c_0 + c_1T + c_2T^2 + \ldots$ dada por

$$c_0 = a_0$$

$$c_1 = a_1b_1$$

$$c_2 = a_1b_2 + a_2b_1^2$$

$$\vdots$$

siendo

$$f(T) = a_0 + a_1T + a_2T^2 + \ldots, \qquad g(T) = b_1T + b_2T^2 + \ldots$$

Obviamente, la definición anterior (que dejamos sólo indicada) es el modo natural de agrupar la expresión

$$a_0 + a_1(b_1T + b_2T^2 + \ldots) + a_2(b_1T + b_2T^2 + \ldots)^2 + \ldots$$

Nótese que, si g tuviera término independiente b_0 sería imposible determinar el valor de c_0, que tendría que ser $c_0 = a_0 + a_1b_0 + a_2b_0^2 + \ldots$

Teorema 6.7 (función inversa formal)**.** *Sea $f \in k[[T]]$ tal que $f(0) = 0$. Entonces existe una serie $g \in k[[T]]$ tal que $g(0) = 0$ y $f(g(T)) = T$ si y sólo si $O(f) = 1$ (es decir, $f(0) = 0$ y $f'(0) \neq 0$). Además, en este caso, la serie g es única y se tiene también $g(f(T)) = T$ y $g'(0) = \frac{1}{f'(0)}$.*

Demostración: Escribiendo de nuevo $f = a_1T + a_2T^2 + a_3T^3 + \ldots$, buscamos ahora $g = b_1T + b_2T^2 + b_3T^3 + \ldots$ tal que

$$T = a_1(b_1T + b_2T^2 + b_3T^3 + \ldots) + a_2(b_1T + b_2T^2 + b_3T^3 + \ldots)^2 + a_3(b_1T + b_2T^2 + b_3T^3 + \ldots)^3 + \ldots$$

o equivalentemente

$$a_1b_1 = 1$$

$$a_1b_2 + a_2b_1^2 = 0$$

$$a_1b_3 + 2a_2b_1b_2 + a_3b_1^3 = 0$$

y, en general, igualando a cero el coeficiente de T^i obtenemos que

$$a_1b_i + (\text{expresión que depende de } a_1, \ldots, a_i \text{ y de } b_1, \ldots, b_{i-1}) = 0.$$

Por tanto, es necesario que $a_1 \neq 0$ (usando la primera ecuación), y en tal caso cada b_i se obtiene de forma única a partir de los b_j con $j < i$ y de los a_k, luego g existe. Además, $g'(0) = b_1 = \frac{1}{a_1} = \frac{1}{f'(0)}$.

Si ahora consideramos la única h tal que $g(h(T)) = T$, se tendrá, sustituyendo T por $h(T)$ en la igualdad $f(g(T)) = T$,

$$h(T) = f(g(h(T))) = f(T)$$

lo que demuestra también $g(f(T)) = T$. □

Definición. Llamaremos *serie invertible* a una serie formal de orden uno. Su inversa la denotaremos por f^{-1} (OJO: no confundir esta inversa para la composición con la inversa $\frac{1}{f}$ para el producto).

Ejercicio 6.8. Demostrar que $O(f \circ g) = O(f)O(g)$ para cualesquiera series formales $f, g \in k[[T]]$. En particular, el orden de una serie coincide con el de su composición con cualquier serie invertible.

Lema 6.9. *Sea $f \in k[[T]]$ una serie y sea $r \geq 1$. Entonces son equivalentes:*

(i) $O(f) = r$

(ii) Existe una serie invertible g tal que $f = g^r$.

(iii) Existe una serie invertible g tal que $f \circ g = T^r$.

Demostración: Demostremos las equivalencias cíclicamente.

$(i) \Rightarrow (ii)$: Por definición de orden, podremos escribir $f(T) = T^r g(T)$, con $g(0) \neq 0$. Por el Lema 6.2(ii) existirá alguna serie formal $h(T)$ tal que $g(T) = h(T)^r$ (y obviamente será $h(0) \neq 0$). Por tanto, $f(T) = \big(Th(T)\big)^r$, y evidentemente $Th(T)$ es una serie invertible, ya que su orden es 1.

$(ii) \Rightarrow (iii)$: Si g es la serie invertible tal que $f = g^r$, entonces $(f \circ g^{-1})(T) = f(g^{-1}(T)) = g(g^{-1}(T))^r = T^r$

$(iii) \Rightarrow (i)$: Si $f \circ g = T^r$, del Ejercicio 6.8 se sigue que $O(T^r) = O(f)O(g)$, es decir, $r = O(f)$ (ya que g tiene orden 1 por ser invertible). □

Obviamente, si (p, q) es una parametrización de una curva, también lo es $(p \circ g, q \circ g)$ para cualquier serie tal que $g(0) = 0$. Sin embargo, si g no es invertible, no podemos volver atrás.

Definición. Se llama *reparametrización* de una parametrización (p, q) a una nueva parametrización de la forma $(p \circ g, q \circ g)$. Dos *parametrizaciones equivalentes* son dos parametrizaciones obtenidas una a partir de la otra mediante una reparametrización en la que g es invertible.

Es un simple ejercicio comprobar que la relación *ser parametrización equivalente* es, en efecto, una relación de equivalencia.

Teorema 6.10. *Toda parametrización formal (p, q) en (a, b) de una curva afín es equivalente a una parametrización de la forma $(a + T^r, \bar{q}(T))$, con $\bar{q} \in k[[T]]$. Además, necesariamente $r = O(p - a)$ y cualquier otra parametrización de esa forma se escribe como $(a + T^r, \bar{q}(\omega T))$, donde ω es una raíz r-ésima de la unidad.*

Demostración: Sea $r = O(p - a)$ (que es necesariamente positivo). Por el Lema 6.9, podemos encontrar una serie invertible g tal que $(p - a) \circ g = T^r$, es decir, $p \circ g = a + T^r$. Por tanto, (p, q) es equivalente a $(p \circ g, q \circ g) = (a + T^r, \bar{q})$, donde $\bar{q} = q \circ g$.

Además, si $(a + T^s, \tilde{q}(T))$ es equivalente a (p, q) (y por tanto equivalente a la $(a + T^r, \bar{q}(T))$ que acabamos de encontrar), deberá existir alguna g invertible tal que $(a + T^s, \tilde{q}(T)) = (a + g(T)^r, \bar{q}(g(T)))$. De la igualdad $g(T)^r = T^s$ se sigue fácilmente que $s = r$ y $g(T) = \omega T$, donde ω es una raíz r-ésima de la unidad. Por tanto, $\tilde{q}(T) = \bar{q}(\omega T)$, como queríamos. □

Lema 6.11. *Dada una parametrización formal, y un entero $m > 1$, son equivalentes:*

(i) La parametrización es de la forma $(p \circ g, q \circ g)$, con $O(g) = m$.

(ii) La parametrización es equivalente a una parametrización de la forma $(p(T^m), q(T^m))$.

(iii) Las parametrizaciones equivalentes del Teorema 6.10 son de la forma $(a+T^{mr}, \bar{q}(T^m))$.

Demostración: Probaremos las implicaciones cíclicamente.

$(i) \Rightarrow (ii)$: Por el Lema 6.9, existe h invertible tal que $g \circ h = T^m$. Entonces $(p \circ g, q \circ g)$ es equivalente a $(p \circ g \circ h, q \circ g \circ h) = (p(T^m), q(T^m))$.

$(ii) \Rightarrow (iii)$: Sea $r = O(p - a)$. Por el Lema 6.9, existe g invertible tal que $p - a = g^r$. Podremos escribir entonces

$$\big(p(T^m), q(T^m)\big) = \big(a + g(T^m)^r, q(g^{-1}(g(T^m)))\big)$$

Como $g(T^m)$ tiene orden m, usando de nuevo el Lema 6.9, existirá h invertible tal que $g(T^m) \circ h = T^m$, es decir, $g(h(T)^m) = T^m$. Entonces nuestra parametrización será equivalente a $\big(a + g(h(T)^m)^r, q(g^{-1}(g(T^m)) \circ h)\big) = (a + T^{mr}, q(g^{-1}(T^m)))$.

$(iii) \Rightarrow (i)$: Por hipótesis, la parametrización se podrá escribir como $(a+h(T)^{mr}, \bar{q}(h(T)^m))$ para alguna serie invertible h. Llamando $g(T) := h(T)^m$, $p(T) = a + T^r$ y $q = \bar{q}$, se sigue el resultado. □

Definición. Se llama *parametrización reducida* a una parametrización que no es como en el Lema 6.11.

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

Obviamente, la misma noción sirve para curvas proyectivas, basta deshomogeneizar respecto de alguna de las variables.

Dedicaremos el resto de la sección a estudiar cómo encontrar las ramas de una curva en un punto. La clave será la siguiente:

Observación 6.12. Volvamos ahora al Teorema 6.10 y supongamos $a = 0$. Entonces, una rama se puede representar mediante una parametrización formal reducida, que podemos hacer equivalente a una parametrización de la forma $(p, q(T)) = (T^r, a_0 + a_1T + a_2T^2 + \ldots)$. Obviamente, se trata de una parametrización en $(0, a_0)$ de una curva afín, y escribiremos $f \in k[X, Y]$ para su ecuación minimal. Esto quiere decir que tenemos una identidad $f(T^r, q(T)) = 0$. Si (de la misma forma que se construye el símbolo i para un elemento

cuyo cuadrado es -1), escribimos el símbolo $X^{\frac{1}{r}}$ para representar una raíz r-ésima de X, tendremos la identidad $f(X, q(X^{\frac{1}{r}})) = 0$, es decir, que

$$p(X) := q(X^{\frac{1}{r}}) = a_0 + a_1 X^{\frac{1}{r}} + a_2 X^{\frac{2}{r}} + \dots$$

es una raíz de f considerado como polinomio en la variable Y y coeficientes en $k[X]$. Obsérvese lo siguiente:

(i) El hecho de tomar la parametrización reducida es equivalente a que en los exponentes de p no se pueda encontrar un denominador común más pequeño que r. Recíprocamente, si encontramos una raíz $p(X)$ de la forma anterior en que el denominador r no se puede reducir, entonces encontramos una parametrización formal reducida $((T^r, q(T)))$ como al principio.

(ii) De la misma forma que ocurre con el símbolo i, en que también $-i$ es una raíz cuadrada de -1, para cada raíz r-ésima ω de la unidad, $\omega X^{\frac{1}{r}}$ es también una raíz r-ésima de X. Por tanto, también serán raíces de f las expresiones

$$p_\omega(X) := a_0 + a_1 \omega X^{\frac{1}{r}} + a_2 \omega^2 X^{\frac{2}{r}} + \dots$$

De hecho, estas nuevas raíces son las conjugadas (en el sentido de la teoría de Galois) de la raíz $p(X)$. Estas raíces corresponden (ver Teorema 6.10) a las parametrizaciones equivalentes a $(T^r, q(T))$, que son de la forma

$$(T^r, q(\omega T)) = (T^r, a_0 + a_1 \omega T + a_2 \omega^2 T^2 + \dots)$$

Por tanto, cada rama de $V(f)$ en un punto $(0, a_0)$ corresponde a un conjunto de raíces conjugadas de f.

Esto nos lleva a la siguiente definición:

Definición. Se llama *serie de Puiseux* a un elemento de $k\{\{X\}\} := \bigcup_{r=1}^{\infty} k[[X^{\frac{1}{r}}]]$ (para ser precisos, hay que aclarar que identificamos los símbolos $X^{\frac{a}{r}}$ y $X^{\frac{b}{s}}$ si $\frac{a}{r} = \frac{b}{s}$).

Observación 6.13. Nótese que, aunque permitamos exponentes racionales, los exponentes de las series de Puiseux deben tener siempre un común denominador. Por ejemplo, $1 + X^{\frac{1}{2}} + X^{\frac{2}{3}} + X^{\frac{3}{4}} + \dots$ no es una serie de Puiseux, ya que los denominadores se hacen arbitrariamente grandes. Sin embargo, $p(X) = 1 + X^{\frac{1}{3}} + X^{\frac{1}{2}}$ sí es una serie de Puiseux, ya que podemos escribir $p(X) = 1 + X^{\frac{2}{6}} + X^{\frac{3}{6}}$, luego $p(X) = q(X^{\frac{1}{6}})$, donde $q(T) = 1 + T^2 + T^3$. Además, 6 es el mínimo denominador que podemos tomar en este caso.

Definición. Se llama *orden de una serie de Puiseux* p al mínimo exponente $m \in \mathbb{Q}$ tal que el coeficiente de X^m en p es no nulo. En otras palabras, si $p(X) = q(X^{\frac{1}{r}})$ para alguna

serie formal $q \in k[[T]]$, entonces $O(p) = \frac{O(q)}{r}$. Obviamente, el orden $O(p)$ de una serie de Puiseux puede ser un número racional no entero.

Las series de Puiseux se comportan en muchos aspectos como las series formales:

Ejercicio 6.14. Demostrar que $k\{\{X\}\}$ es un anillo, que tiene un único ideal maximal y que tal ideal no admite un número finito de generadores. Demostrar también que un elemento $p \in k\{\{X\}\}$ es una unidad si y sólo $p(0) \neq 0$, y concluir que el cuerpo de fracciones de $k\{\{X\}\}$ es $\bigcup_{r=1}^{\infty} k((X^{\frac{1}{r}}))$, es decir, el conjunto de series que pueden tener un número finito de exponentes negativos. Finalmente, demostrar que sobre los elementos no nulos del cuerpo de fracciones se puede definir un orden (que tomará valores en $\mathbb{Q}$) que satisface las propiedades del Ejercicio 6.3$^{(*)}$.

Llegamos pues al problema de encontrar las raíces de un polinomio $f \in k[X, Y]$ visto como polinomio en la variable Y, sospechando que puedan ser series de Puiseux. Podemos intentar hacer como en el Ejemplo 6.1 para encontrar series de Puiseux que sean raíces de polinomios $f \in k[X, Y]$. Obsérvese que no es una tarea fácil, ya que en principio no sabemos cuál es el común denominador r que necesitaremos. Una primera respuesta nos viene de la siguiente generalización del Teorema de la Función Implícita a las series de Puiseux:

Lema 6.15. *Sea $f = p_0(X) + p_1(X)Y + \ldots + p_d(X)Y^d$, donde $p_0, p_1, \ldots, p_d$ son series de Puiseux, $p_0(0) = 0$ y $p_1(0) \neq 0$. Entonces existe una única serie de Puiseux p tal que $p(0) = 0$ y $f(X, p(X)) = 0$. Además, si los coeficientes de f están en $k[[X^{\frac{1}{r}}]]$, entonces también la raíz p está en $k[[X^{\frac{1}{r}}]]$.*

Demostración: Sea $r \in \mathbb{N}$ cualquiera tal que $p_0, p_1, \ldots, p_d \in k[[X^{\frac{1}{r}}]]$. Entonces, $g(X', Y) = f(X'^r, Y)$ satisface las hipótesis del Teorema de la Función Implícita Formal. Por tanto, existe una serie formal $q(X') \in k[[X']]$ tal que $q(0) = 0$ y $g(X', q(X')) = 0$, es decir, $f(X'^r, q(X')) = 0$. Entonces, si tomamos $p(X) = q(X^{\frac{1}{r}})$, se tendrá $p(0) = 0$ y $f(X, p(X)) = 0$.

Para ver la unicidad, si $p, \bar{p}$ fueran dos raíces de f, entonces tomamos r tal que $p_0, p_1, \ldots, p_d, p, \bar{p} \in k[[X^{\frac{1}{r}}]]$ y se tendría que $p(X'^r)$ y $\bar{p}(X'^r)$ serían dos funciones implícitas para g, luego $p(X'^r) = \bar{p}(X'^r)$, es decir, $p(X) = \bar{p}(X)$ como series de Puiseux. □

En general, si queremos calcular las raíces de un polinomio f en Y con coeficientes polinomios (o más en general, series de Puiseux) en X, más que intentar averiguar a priori

$^{(*)}$ Para quien sepa Álgebra Conmutativa, tal conjunto de propiedades quiere decir que $k[[X]]$ es un anillo de valoración discreta (ya que el orden toma valores enteros), mientras que $k\{\{X\}\}$ es un anillo de valoración, pero no anillo de valoración discreta.

el común denominador r de las raíces, intentaremos averiguar cuál es el primer coeficiente distinto de cero. En concreto, si queremos que una sustitución en f del tipo $Y = cX^q + \ldots$ (con $c \neq 0$) cancele el término de menor grado necesitamos dos cosas:

(i) Que si el exponente de menor grado en $f(X, cX^q + \ldots)$ es d, entonces cada vez que X^iY^j tiene coeficiente distinto de cero en f, tiene que ser $i + qj \geq d$.

(ii) Que se cancelen entre sí todos los coeficientes no nulos (por tanto al menos dos) de los X^iY^j tales que $i + qj = d$.

Obsérvese que no está claro ni quién debe ser este d. Todo esto se puede visualizar de forma gráfica. Para ello, pintamos en el plano todos los puntos (i, j) tales que el coeficiente de X^iY^j de f (el conjunto de tales puntos lo llamaremos *soporte de* f). En ese plano buscamos posibles rectas de la forma $i + qj = d$ que dejen arriba a la derecha a todo el soporte de f (condición (i)) y que pasen por al menos dos puntos del soporte (condición (ii)).

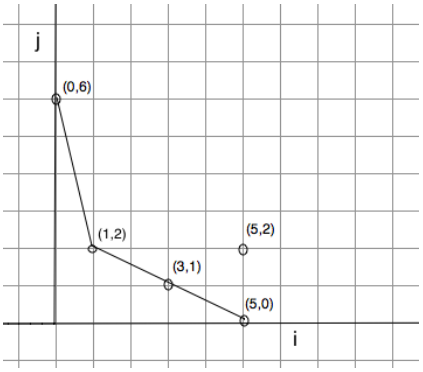
Definición. Dado un polinomio $f \in k\{\{X\}\}[Y]$, se llama *soporte* de f al conjunto de pares (i, j) tales que f tiene un coeficiente no nulo en X^iY^j. Se llama *polígono de Newton-Puiseux* a la unión, en el primer cuadrante de los semiplanos de la forma $i + qj \geq d$, con $q \geq 0$, que contienen al soporte de f, donde $i + qj = d$ es una recta que pasa por al menos dos puntos del soporte de f.

Observación 6.16. En este lenguaje, la hipótesis $p_1(0) \neq 0$ del Lema 6.15 nos está diciendo que, si $(0, 1)$ está en el soporte de f (es decir, el polígono de Newton de f tiene un solo lado), entonces existe una única raíz, q con $q(0) = 0$.

Ejemplo 6.17. Consideremos la curva de ecuación minimal

$$f = Y^6 - XY^2 + 2X^3Y - X^5 + X^5Y^2$$

y estudiemos sus posibles parametrizaciones formales en $(0, 0)$. Obsérvese primero que el cono tangente en $(0, 0)$ es $V(XY^2)$, con lo que nos esperamos que la curva pase una vez en la dirección de $V(X)$ y dos veces o una sola vez con multiplicidad dos en la dirección de $V(Y)$. El polígono de Newton de tal polinomio viene dado en la siguiente figura:



A efectos prácticos, el polígono se construye siempre así: En primer lugar, se toma el punto (i_1, j_1) más a la izquierda (i.e. con i_1 mínimo) y más abajo (i.e. con el correspondiente j_1 mínimo), en nuestro caso el $(0, 6)$. Alrededor de este punto se hace girar en el sentido contrario a las agujas del reloj a una semirrecta vertical, hasta que toque el primer punto (i_2, j_2) del soporte, en nuestro caso, el punto $(1, 2)$ (si hubiera varios, se tomaría el que estuviera más abajo). Ahora alrededor de este nuevo punto se continúa girando la semirrecta, hasta que toque a un nuevo punto (i_3, j_3), en nuestro caso el $(5, 0)$ (está también el $(3, 1)$, pero hemos dicho que tomaríamos siempre el que estuviera más abajo). El polígono se termina cuando lleguemos al punto más bajo (y a la izquierda) del soporte, en nuestro caso el $(5, 0)$. Nótese que este proceso acaba siempre, porque los valores $j_1, j_2, \ldots$ son naturales estrictamente decrecientes.

Estudiemos las posibles raíces que pueden salir de cada uno de los lados:

1) Empezamos por el lado de vértices $(0, 6)$ y $(1, 2)$, es decir, la recta $i + \frac{1}{4}j = \frac{3}{2}$, que corresponde a los monomios $Y^6 - XY^2$. Esto debería producir alguna raíz que empezase como $p = cX^{\frac{1}{4}} + \ldots$, es decir, de la forma $p = X^{\frac{1}{4}}(c + p_1)$, donde p_1 es una serie de Puiseux con $p_1(0) = 0$. La parte de grado más pequeño de $f(X, p(X))$ será

$$(cX^{\frac{1}{4}})^6 - X(cX^{\frac{1}{4}})^2 = (c^6 - c^2)X^{\frac{3}{2}}$$

luego debe ser $c^6 - c^2 = 0$, es decir, tenemos las posibilidades $c = 1, -1, i, -i$ (recuérdese que queremos $c \neq 0$). Nótese que obtenemos cuatro soluciones, tantas como la altura del lado que estamos considerando.(*)

Escogemos de momento el valor $c = 1$ (es decir, buscamos ahora raíces de la forma $p = X^{\frac{1}{4}}(1 + p_1)$), y veamos que el modo de calcular p_1 es por recurrencia. En efecto, p_1 será ahora una raíz del polinomio

$$f(X, X^{\frac{1}{4}}(1 + Y_1)) = X^{\frac{3}{2}}(1 + Y_1)^6 - X^{\frac{3}{2}}(1 + Y_1)^2 + 2X^{\frac{13}{4}}(1 + Y_1) - X^5 + X^{\frac{11}{2}}(1 + Y_1)^2 =$$

$$= X^{\frac{3}{2}}\big((4Y_1 + 14Y_1^2 + 20Y_1^3 + 15Y_1^4 + 6Y_1^5 + Y_1^6) + 2X^{\frac{7}{4}}(1 + Y_1) - X^{\frac{7}{2}} + X^4(1 + 2Y_1 + Y_1^2)\big)$$

Buscamos entonces raíces del polinomio

$$f_1(X, Y_1) := (4Y_1 + 14Y_1^2 + 20Y_1^3 + 15Y_1^4 + 6Y_1^5 + Y_1^6) + 2X^{\frac{7}{4}}(1 + Y_1) - X^{\frac{7}{2}} + X^4(1 + 2Y_1 + Y_1^2)$$

que está en las hipótesis del Lema 6.15, luego tendrá una única raíz p_1 con $p_1(0) = 0$, que además estará en $k[[X^{\frac{1}{4}}]]$. Dicha raíz la podemos calcular o bien como en la demostración

(*) Es práctico observar que hay un modo rápido de obtener el inicio de esta raíz. Se iguala a cero la parte de f que corresponde al lado que estudiamos, es decir, hacemos $Y^6 - XY^2 = 0$. Si despejamos Y de aquí, obtendremos $Y^4 = X$, que da como solución $Y = cX^{\frac{1}{4}}$, con $c = 1, -1, i, -i$, que es el primer término de la raíz p que estamos hallando.

del Teorema de la Función Implícita Formal o bien usando el polígono de Newton de f_1 (que tiene sólo un lado, de vértices $(0,1)$ y $(\frac{7}{4},0)$). En concreto, p_1 empezará como $p_1 = -\frac{1}{2}X^{\frac{7}{4}} + \ldots$, luego la raíz p de f empezará como

$$p = X^{\frac{1}{4}}(1+p_1) = X^{\frac{1}{4}}(1 - \frac{1}{2}X^{\frac{7}{4}} + \ldots) = X^{\frac{1}{4}} - \frac{1}{2}X^2 + \ldots$$

que da lugar a la parametrización

$$(X,Y) = (T^4, T - \frac{1}{2}T^8 + \ldots)$$

El resto de raíces para los otros valores de c se pueden calcular de la misma forma, aunque hay un truco mucho más sencillo. Por el Teorema 6.10, las parametrizaciones equivalentes a la anterior se obtienen cambiando T por cT, con $c = 1, -1, i, -i$, luego son de la forma

$$(T^4, T - \frac{1}{2}T^8 + \ldots),\ (T^4, -T - \frac{1}{2}T^8 + \ldots),\ (T^4, iT - \frac{1}{2}T^8 + \ldots),\ (T^4, -iT - \frac{1}{2}T^8 + \ldots)$$

que correponden, respectivamente a las raíces

$$X^{\frac{1}{4}} - \frac{1}{2}X^2 + \ldots,\ -X^{\frac{1}{4}} - \frac{1}{2}X^2 + \ldots,\ iX^{\frac{1}{4}} - \frac{1}{2}X^2 + \ldots,\ -iX^{\frac{1}{4}} - \frac{1}{2}X^2 + \ldots$$

Resumiendo, este lado nos ha dado una única rama, precisamente en la dirección de $V(X)$ (el hecho de tener tangente vertical explica que no se haya podido parametrizar como $(T, q(T))$).

2) Estudiamos ahora el lado de vértices $(1,2),(3,1),(5,0)$, es decir, la recta $i+2j=5$, que corresponde ahora a los monomios $-XY^2 + 2X^3Y - X^5$. Usando el truco del pie de página anterior, debemos resolver $Y^2 - 2X^2Y + X^4 = 0$, que tiene una raíz doble $Y = X^2$. Es decir, al tener altura dos, nos esperábamos dos raíces, pero nos ha salido sólo una contada dos veces. Veamos qué consecuencias tiene ahora esto. La raíz que buscamos será entonces de la forma $p = X^2(1+p_1)$, con $p_1(0) = 0$, y p_1 será por tanto raíz de

$$f(X, X^2(1+Y_1)) = X^{12}(1+Y_1)^6 - X^5(1+Y_1)^2 + 2X^5(1+Y_1) - X^5 + X^9(1+Y_1)^2 =$$

$$= X^5\big(-Y_1^2 + X^4(1+2Y_1+Y_1^2) + X^7(1+6Y_1+15Y_1^2+20Y_1^3+15Y_1^4+6Y_1^5+Y_1^6)\big)$$

Para calcular ahora las raíces de

$$f_1(X,Y_1) := -Y_1^2 + X^4(1+2Y_1+Y_1^2) + X^7(1+6Y_1+15Y_1^2+20Y_1^3+15Y_1^4+6Y_1^5+Y_1^6)$$

observamos que no podemos aplicar el Lema 6.15. De hecho, el polígono de Newton de este nuevo polinomio tiene un solo lado, de vértices $(0,2)$ y $(4,0)$ (nótese que la altura del polígono de Newton es dos, igual a la multiplicidad de la solución anterior). Como

los vértices del polígono corresponden a los monomios $-Y_1^2 + X^4$, encontramos ahora dos posibles raíces $p_1 = \pm X^2 + \ldots$. Se deja al lector que compruebe que la sustitución $f_1(X, X^2(\pm 1 + Y_2))$ da lugar, para cada uno de los dos signos, una única raíz $Y_2 = p_2$ (usando el Teorema de la Función Implícita Formal, aunque se deducirá también de la próxima demostración). Obtenemos entonces dos raíces

$$p = X^2(1 + p_1) = X^2(1 \pm X^2 + \ldots) = X^2 \pm X^4 + \ldots$$

lo que da lugar a dos parametrizaciones no equivalentes

$$(X, Y) = (T, T^2 \pm T^4 + \ldots)$$

Por tanto, tenemos dos ramas distintas, ambas en la dirección de $V(Y)$.

Veamos ahora que el método anterior funciona siempre (es lo que se conoce como *algoritmo de Newton-Puiseux*, que se explicita en la siguiente demostración):

Teorema 6.18. *Sea $f \in k\{\{X\}\}[Y]$ un polinomio tal que $f(0, Y)$ es no nulo y divisible por Y. Entonces, si k es algebraicamente cerrado, existe alguna serie de Puiseux $p(X)$ que es raíz de f y tal que $p(0) = 0$.*

Demostración: Nuestras hipótesis sobre f son equivalentes a que f no tenga término independiente y contenga algún monomio de la forma Y^j (es decir, que algún punto del soporte es de la forma $(0, j)$). Podemos suponer también que el soporte de f contiene algún punto de la forma $(i, 0)$, ya que, en caso contrario, f sería divisible por Y, y en particular $Y = 0$ sería una raíz.

Tomamos ahora $q, d \in \mathbb{Q}$ tal que $\mathrm{sop}(f) \subset \{i + qj \geq d\}$ y la recta $i + qj = d$ corte a $\mathrm{sop}(f)$ en $(i_1, j_1), \ldots, (i_r, j_r)$ con $r \geq 2$ (es decir, la recta es un lado del polígono de Newton-Puiseux), y suponemos los r puntos ordenados de izquierda a derecha, es decir, $i_1 \leq \ldots \leq i_r$ y $j_1 \geq \ldots \geq j_r$. La parte de f que corresponde a los puntos de ese lado del polígono será entonces de la forma

$$a_1 X^{i_1} Y^{j_1} + \ldots + a_r X^{i_r} Y^{j_r}$$

con todos los a_i no nulos. Por tanto, haciendo la sustitución $Y = cX^q + \ldots$, la parte de grado más pequeño será (usando que $i_k + qj_k = d$ para $k = 1, \ldots, r$):

$$a_1 X^{i_1}(cX^q)^{j_1} + \ldots + a_r X^{i_r}(cX^q)^{j_r} = (a_1 c^{j_1} + \ldots + a_r c^{j_r}) X^d = c^{j_r}(a_1 c^{j_1 - j_r} + \ldots + a_r) X^d.$$

Como buscamos un c no nulo que anule el coeficiente X^d, entonces c debe ser una raíz del polinomio $g(T) := a_1 T^{j_1 - j_r} + \ldots + a_r$. Nótese que entonces el número de tales raíces,

contadas con multiplicidad, es $j_1 - j_r$, es decir, la altura del lado del polígono. Como observamos en el pie de página del Ejemplo 6.17, estas soluciones $Y = cX^q$ de cómo debe empezar la raíz de f se pueden obtener directamente de la parte de f que corresponde al lado del polígono escribiendo

$$a_1X^{i_1}Y^{j_1} + \ldots + a_rX^{i_r}Y^{j_r} = a_1X^{d-qj_1}Y^{j_1} + \ldots + a_rX^{d-qj_r}Y^{j_r} =$$

$$= X^d(a_1(\frac{Y}{X^q})^{j_1} + \ldots + a_r(\frac{Y}{X^q})^{j_r}) = X^d(\frac{Y}{X^q})^{j_r}g(\frac{Y}{X^q}) = X^{i_r}Y^{j_r}g(\frac{Y}{X^q})$$

que, efectivamente se anulará cuando $\frac{Y}{X^q}$ sea una de las raíces c de g.

Fijemos entonces una c raíz de g y tenemos entonces que, si existe la $p(X)$ buscada para esa c, se puede escribir como $p(X) = cX^q + X^qp_1(X)$, con $p_1(0) = 0$. Para ver cómo tendría que ser esta p_1 para que $f(X, p(X)) = 0$, llamamos m a la multiplicidad de c como raíz de g y escribimos entonces $g(T) = (T - c)^m h(T)$, con $h(c) \neq 0$. Si hacemos el cambio de variable $Y = X^q(c + Y_1)$, por la construcción del polígono de Newton-Puiseux, tal sustitución da grado en X estrictamente mayor que d en cada monomio distinto de los de $a_1X^{i_1}Y^{j_1} + \ldots + a_rX^{i_r}Y^{j_r}$ (expresión que vimos que era igual a $X^d(\frac{Y}{X^q})^{j_r}g(\frac{Y}{X^q})$). Tendremos entonces:

$$f(X, X^q(c + Y_1)) = X^d\big((c + Y_1)^{j_r}g(c + Y_1) + \ldots\big) = X^d((c + Y_1)^{j_r}Y_1^m h(c + Y_1) + \ldots)$$

donde los puntos suspensivos indican que todos los sumandos contienen alguna X. Por tanto, la serie p_1 que buscamos tiene que ser una raíz del polinomio

$$f_1(X, Y_1) := \frac{f(X, X^q(c + Y_1))}{X^d} = (c + Y_1)^{j_r}Y_1^m h(c + Y_1) + \ldots$$

que tiene un monomio en Y_1^m y ninguno con un exponente menor ($h(c+Y_1)$ tiene término independiente $h(c) \neq 0$). De este modo, hemos reducido el calcular una raíz p de f a calcular una raíz p_1 de f_1. La ventaja es que la altura del polígono de Newton-Puiseux de f_1 es ahora m (salvo que f_1 fuese divisible por Y_1, en cuyo caso la serie nula $p_1 = 0$ sería una raíz), en principio mucho menor que la altura del polígono de Newton-Puiseux de f, ya que $m \leq \deg(g) = j_1 - j_r$ y este último número es sólo la altura de un lado del polígono de f.

Aplicando este proceso a f_1 y reiterando, vamos encontrando una sucesión de polinomios $f_1(X, Y_1), f_2(X, Y_2), \ldots$ en que cada f_n está en $(k\{\{X\}\})[Y_n]$ y de modo que una raíz $Y_n = p_n(X)$ de f_n con $p_n(0) = 0$ proporciona automáticamente una raíz $Y = p(X)$ de f con $p(0) = 0$. El proceso se puede parar porque algún f_n sea divisible por Y_n, en cuyo caso $Y_n = 0$ es ya una raíz de f_n (en realidad, podríamos seguir calculando las demás posibles raíces de f_n escribiendo $f_n = Y_n^s g_n$, donde g_n ya no es divisible por Y_n y por tanto

le podemos seguir aplicando el algoritmo). También podemos parar el proceso en cuanto algún f_n tenga al punto $(0,1)$ en el soporte, ya que la Observación 6.16 nos garantiza que en tal caso f_n tiene una única raíz $Y_n = p_n(X)$ con $p_n(0) = 0$.

En caso contrario, como la sucesión de enteros positivos dada por la altura de los sucesivos polígonos de Newton-Puiseux de los f_n va decreciendo, y llegará un momento en que necesariamente estacione. Como estamos suponiendo que no llegamos a altura uno, estacionará en algún entero $m > 1$ (en realidad puede demostrarse que es un caso que se da sólo si f tiene algún factor múltiple). Entonces se llega a un polinomio f_n, cuyo polígono tiene sólo un lado de altura m, que debe corresponder a que se puede escribir $f_n = a(Y_n - c_n X^{q_n})^m + \ldots$, es decir que el lado viene dado por los puntos del soporte

$$(0,m),(q_n,m-1),(2q_n,m-2)\ldots,(mq_n,0).$$

Si $f_n \in (k[[X^{\frac{1}{r}}]])[Y_n]$, eso quiere decir que podemos escribir $q_n = \frac{b_n}{r}$, con $b_n \in \mathbb{N}$, y el lado del polígono tendrá de ecuación $i + \frac{b_n}{r} j = \frac{m b_n}{r}$. Como al reiterar se obtienen siempre polinomios de las mismas características, el nuevo polinomio

$$f_{n+1}(X, Y_{n+1}) := \frac{f_n(X, X^{\frac{b_n}{r}}(c_n + Y_{n+1}))}{X^{\frac{m b_n}{r}}} = a Y_n^m + \ldots,$$

cuyos coeficientes siguen en $k[[X^{\frac{1}{r}}]]$, tiene necesariamente de nuevo polígono de Newton-Puiseux de altura m y con un solo lado , que corresponderá al hecho de que se puede escribir $f_{n+1}(X, Y_{n+1}) = a(Y_{n+1} - c_{n+1} X^{\frac{b_{n+1}}{r}})^m + \ldots$. Reiterando el procedimiento llegamos a una raíz de f_n de la forma

$$Y = c_n X^{\frac{b_n}{r}} + c_{n+1} X^{\frac{b_n + b_{n+1}}{r}} + \ldots \in k[[X^{\frac{1}{r}}]]$$

y por tanto es una serie de Puiseux. □

El resultado anterior demuestra (haciendo una traslación al origen) que, dado cualquier punto (a,b) en una curva $V(f)$, existe siempre al menos una parametrización formal de $V(f)$ en el punto. Además, por el Lema 6.11, podemos tomarla siempre reducida. Como siempre, lo mismo vale para curvas proyectivas. En otras palabras, hemos visto que por cada punto de una curva tenemos al menos una rama (y que la rama es única si el punto es liso). Daremos más detalles en la sección siguiente, concretamente en el Teorema 7.3. Terminaremos esta sección con dos resultados más sobre las raíces de Puiseux.

Corolario 6.19. *Si k es algebraicamente cerrado, el cuerpo de fracciones de $k\{\{X\}\}$ es algebraicamente cerrado.*

Demostración: Sea $f = p_0(X) + p_1(X)Y + \ldots + p_n(X)Y^n$ un polinomio en la variable Y cuyos coeficientes son cocientes de series de Puiseux. Podemos quitar denominadores y

suponer que $p_0, p_1, \ldots, p_n$ son series de Puiseux, y –multiplicando todo por X, si hiciera falta– que $p_0(0) = 0$. Por otra parte, tomamos el mínimo valor a de $O(p_1)/1, \ldots, O(p_n)/n$. Entonces, si escribimos $f'(X, Y') := f(X, \frac{Y'}{X^a})$ tendremos que los coeficientes de f' como polinomio en Y' son series de Puiseux, y además una de ellas es una serie con término independiente. Por tanto, podemos aplicar el Teorema 6.18 y encontrar una raíz p de f'. Entonces $\frac{p}{X^a}$ es una raíz de f. □

Proposición 6.20. *Si $f \in k\{\{X\}\}[Y]$ es mónico en la variable Y, entonces todas las raíces de f están en $k\{\{X\}\}$.*

Demostración: Lo hacemos por inducción sobre el grado de f en la indeterminada Y, siendo trivial el caso en que el grado es uno. Si ahora f tiene grado $d > 1$ en Y, consideramos una raíz a de $f(0, Y)$. Entonces, el polinomio $g(X, Y) := f(X, Y + a)$ es mónico en Y y satisface $g(0, 0) = 0$, luego por el Teorema 6.18 existe $p \in k\{\{X\}\}$ tal que $g(X, p(X)) = 0$. Por tanto, $a + p(X) \in k\{\{X\}\}$ es una raíz de f. Por la regla de Ruffini, podemos escribir

$$f(X, Y) = \big(Y - a - p(X)\big)h(X, Y)$$

donde $h \in k\{\{X\}\}[Y]$ es mónico de grado $d - 1$ en Y. Por hipótesis de inducción, todas las raíces de h están en $k\{\{X\}\}$, es decir, todas las raíces de f están en $k\{\{X\}\}$, lo que concluye la demostración. □

7. Intersección de curvas. Teorema de Bézout

En esta sección podremos utilizar todo lo visto en la sección anterior para definir por fin formalmente multiplicidad de intersección de dos curvas en un punto. Como consecuencia podremos demostrar ya rigurosamente el Teorema de Bézout, del que veremos una primera aplicación, en concreto el contar el número de puntos de inflexión de una curva con singularidades sencillas.

Podemos empezar definiendo la multiplicidad de intersección de una curva con una rama de una curva, ya que una rama no es más que una clase de parametrización. Así que, de la misma forma que para curvas parametrizadas, está bien definida la siguiente noción (que no depende de representantes o de cambio de variable):

Definición. Se llama *multiplicidad de intersección de una rama con una curva* $V(g)$ *en un punto* (a, b) al orden de $g(p, q)$, donde (p, q) es un representante de la rama.

Como en el caso de curvas, a partir de la multiplicidad de intersección de una rama con las distintas rectas que pasan por el punto correspondiente, se puede definir la noción tanto de multiplicidad de una rama como de tangente a una rama (a diferencia del caso de curvas, la tangente a una rama será única), a partir del siguiente:

Lema 7.1. *Sea* $(a + c_r T^r + \ldots, b + d_r T^r + \ldots)$ *un representante de una rama de una curva en el punto* (a, b)*, con al menos uno entre* $c_r, d_r \neq 0$*. Entonces la multiplicidad de intersección de la rama con cualquier recta que pase por* (a, b) *es mayor o igual que* r*, dándose la igualdad si y sólo si la recta no es la que pasa por* (a, b) *en la dirección del vector* (c_r, d_r)*.*

Demostración: Una recta que pasa por (a, b) tiene la forma $V(\lambda(X - a) + \mu(Y - b))$. Para calcular su multiplicidad de intersección con la rama en (a, b) hay que calcular el orden de

$$\lambda(c_r T^r + \ldots) + \mu(d_r T^r + \ldots) = (\lambda c_r + \mu d_r)T^r + \ldots$$

Por tanto, el orden es siempre al menos r, y es igual a r exactamente cuando $\lambda c_r + \mu d_r \neq 0$, que corresponde al hecho de que la dirección de la recta no es la del vector (c_r, d_r). □

Definición. Se llama *multiplicidad de una rama en un punto* a la mínima multiplicidad de intersección de la rama con las distintas rectas que pasan por el punto. Se llama *recta tangente a una rama* R de multiplicidad $\text{mult}(R)$ en un punto a la única recta $\mathbb{T}R$ cuya multiplicidad de intersección con la rama en el punto es mayor que $\text{mult}(R)$.

Observación 7.2. Si consideramos la curva $V(Y^6 - XY^2 + 2X^3Y - X^5 + X^5Y^2)$ del Ejemplo 6.17, cuyo cono tangente en $(0, 0)$ tiene ecuación XY^2, encontramos que había

tres ramas, la dada por la parametrización $(T^4, T - \frac{1}{2}T^8 + \ldots)$, de multiplicidad uno con recta tangente $V(X)$, y las dada por $(T, T^2 \pm T^4 + \ldots)$, ambas de multiplicidad uno con recta tangente $V(Y)$, lo que explica que el factor Y aparezca dos veces en la ecuación del cono tangente. En el caso de la cúbica $V(Y^2 - X^3)$, el cono tangente es $V(Y^2)$, pero esta vez existe una sola rama en $(0,0)$: la dada por (T^2, T^3), que tiene multiplicidad dos y recta tangente $V(Y)$. En este caso, el exponente dos del factor Y en la ecuación del cono tangente se debe a que la rama tiene multiplicidad dos.

Comprobemos que lo observado en estos ejemplo es general, entendiendo siempre como ecuación del cono tangente aquella con multiplicidades en el sentido de la Observación 5.2.

Teorema 7.3. *Sea C una curva plana. Entonces la ecuación del cono tangente a C en un punto p es el producto de las distintas rectas tangentes a las distintas ramas de C en p, cada una de ellas elevada a la multiplicidad de la rama. En particular, hay un número finito de ramas en p, y la suma de sus multiplicidades es la multiplicidad del punto en la curva.*

Demostración: Haciendo un cambio de coordenadas en que C (o su completado proyectivo) no pase por $(0:0:1)$ y que el punto p sea $(1:0:0)$, podemos suponer que C es afín con ecuación minimal $f \in k[X,Y]$ mónica en Yy $p = (0,0)$. Por la Proposición 6.20, las raíces de f como polinomio en la variable Y son series de Puiseux (distintas, al no tener f factores múltiples), y podemos escribir

$$f(X,Y) := \prod_{p(X)} (Y - p(X))$$

donde $p(X)$ recorre el conjunto de raíces de f. Como la ecuación del cono tangente es la parte homogénea de grado menor de f, será igual al producto de las partes homogéneas de cada $Y - p(X)$. Recordemos primero que, por la Observación 6.12(ii) cada raíz de la forma

$$p(X) := a_0 + a_1 X^{\frac{1}{r}} + a_2 X^{\frac{2}{r}} + \ldots$$

viene junto al conjunto de raíces, cuando ω recorre el conjunto de raíces r-ésimas de la unidad,

$$p_\omega(X) := a_0 + a_1 \omega X^{\frac{1}{r}} + a_2 \omega X^{\frac{2}{r}} + \ldots$$

y estas r raíces se corresponden con la rama R de C en el punto $(0, a_0)$ definida por la parametrización $(T^r, a_0 + a_1 T + a_2 T^2 + \ldots)$. Si $a_0 \neq 0$, entonces la rama no es en el punto $(0,0)$, y la parte homogénea de grado menor en cada $Y - p_\omega(X)$ es la constante no nula $-a_0$, lo que no aporta nada a la ecuación del cono tangente. Si, en cambio, $a_0 = 0$, la rama R lo es del punto $p = (0,0)$ que estamos estudiando. En este caso, si

a_s es el primer coeficiente no nulo de $p(X)$, la rama R viene dada por la parametrización $(T^r, a_sT^s + \ldots a_{s+1}T^{s+1} + \ldots)$. Distinguimos ahora tres casos:

–Si $s < r$, entonces R tiene multiplicidad s, y su recta tangente es $V(X)$. Por otra parte, la parte de grado menor de $\Pi_w(Y - p_\omega(X)) = \Pi_w(Y - a_s\omega^s X^{\frac{s}{r}} - a_{s+1}\omega^{s+1}X^{\frac{s+1}{r}} - \ldots)$ es $\Pi_\omega(-a_s\omega^s X^{\frac{s}{r}})$, que es un múltiplo no nulo de X^s.

–Si, en cambio, $s > r$, entonces R tiene multiplicidad r, y su recta tangente es $V(Y)$. Ahora, la parte de grado menor de $\Pi_w(Y - p_\omega(X))$ es Y^r.

–Finalmente, si $s = r$, la rama R tiene multiplicidad $r = s$ y su recta tangente es $(Y - a_rX)$, y la parte de grado menor de $\Pi_w(Y - p_\omega(X))$ es $(Y - a_rX)^r$.

En cualquiera de los tres casos, obtenemos exactamente la ecuación de la recta tangente a la rama R elevada a la multiplicidad de R, lo que demuestra el resultado. □

Podemos ya definir de forma precisa multiplicidad de intersección de dos curvas en un punto:

Definición. Se llama *multiplicidad de intersección de dos curvas C y D en un punto* $p \in C \cap D$ a la suma de las multiplicidades de intersección en p de cada rama de C en p con D. Denotaremos por $\text{mult}_p(C, D)$ a tal multiplicidad.

Nótese que, cuando C es una recta, tiene una única rama en cada punto, y esta nueva definición coincide con la dada al final de la sección 4.

Obsérvese que en principio la multiplicidad de intersección depende del orden en que consideremos C y D, aunque pronto demostraremos que no es así. Para ello, relacionaremos esta multiplicidad de intersección con la multiplicidad de las raíces de la resultante que obteníamos en el Teorema Débil de Bézout, lo que nos permitirá acabar demostrando el Teorema de Bézout en su totalidad.

Empezamos con un par de propiedades útiles, que nos pueden permitir saber la multiplicidad de intersección sin necesidad de hacer ningún cálculo.

Proposición 7.4. *Si a es un punto de intersección de dos curvas C y D, entonces para toda rama R de C en p se tiene* $\text{mult}_p(R, D) \geq \text{mult}(R)\,\text{mult}_p(D)$*, con igualdad si y sólo si $\mathbb{T}_pR$ no es una de las rectas del cono tangente de D en p.*

Demostración: Mediante un cambio de variables y paso al afín podemos suponer $p = (0, 0)$ y $\mathbb{T}R = V(Y)$. Por tanto, una parametrización reducida de R es de la forma $(T^r, cT^s + \ldots)$, con $s > r = \text{mult}(R)$. Por otra parte, la descomposición de una ecuación minimal de D será de la forma $g(X, Y) = g_m(X, Y) + \ldots + g_d(X, Y)$, con $m = \text{mult}_p(D)$. Por tanto, el término de menor grado de $g(T^r, cT^s + \ldots)$ sólo puede ser un T^{rm}, que aparecerá si y sólo

si g_m tiene término en X^m, es decir, si y sólo si g_m, que es la ecuación del cono tangente no es divisible por Y. □

Proposición 7.5. *Si a es un punto de intersección de dos curvas C y D, entonces* $\text{mult}_a(C,D) \geq \text{mult}_a(C)\,\text{mult}_p(D)$, *con igualdad si y sólo si C y D no comparten ninguna recta tangente en p.*

Demostración: Sean $R_1, \ldots, R_s$ las ramas de C en p, y sean $m_1, \ldots, m_s$ sus multiplicidades respectivas. Entonces, por la Proposición 7.4, se tiene $\text{mult}_p(R_i, D) \geq m_i\,\text{mult}_p(D)$, con igualdad si y sólo si la tangente a R_i en p no es tangente a D en p. Como, por definición, $\text{mult}_p(C,D) = \Sigma_{i=1}^{s}\,\text{mult}_p(R_i,D)$ y, por el Teorema 7.3, será $\text{mult}_p(C) = m_1 + \ldots + m_s$, el resultado se sigue sumando las s desigualdades anteriores. □

Ya finalmente, demostramos un lema técnico que será crucial a la hora de demostrar el Teorema de Bézout, ya que nos indica que la multiplicidad de intersección que hemos definido coincide con la multiplicidad que nos aparecía en la demostración del Teorema Débil de Bézout.

Lema 7.6. *Si $F, G \in k[X_0, X_1, X_2]$ son polinomios homogéneos primos entre sí, F y G son mónicos en la variable X_2, y $\text{res}_{X_2}(F,G) = \Pi_i(a_iX_0 + b_iX_1)^{s_i}$ es la descomposición en factores irreducibles de $R_{X_2}(F,G)$, entonces cada s_i es la suma de las multiplicidades de intersección de $V(F)$ y $V(G)$ en los puntos de la recta $V(a_iX_0 + b_iX_1)$.*

Demostración: Obviamente, si hacemos un cambio de variable en X_0, X_1, entonces la resultante de los polinomios correspondientes se obtiene haciendo el mismo cambio de variable en el polinomio resultante. Por tanto, bastará ver que, si X_1^s es la máxima potencia de X_1 que divide a $R_{X_2}(F,G)$, entonces s es la suma de las multiplicidades de intersección de $V(F)$ y $V(G)$ en los puntos de la recta $V(X_1)$. Si llamamos $f, g \in k[X,Y]$ a los deshomogeneizados respectivos de F y G, entonces es claro que el deshomogeneizado de $res_{X_2}(F,G)$ es $R_Y(f,g)$. Por tanto, hay que ver que, si X^s es la máxima potencia de X que divide a $R_Y(f,g)$, entonces s es la suma de las multiplicidades de intersección de $V(f)$ y $V(g)$ en los puntos de la forma $(0,b)$.

Por otra parte (ver Ejercicio 2.2), sabemos que

$$R_Y(f,g) = \prod_{p(X)} g(X, p(X))$$

donde $p(X)$ son las raíces de f como polinomio en Y, que sabemos que son series de Puiseux (por la Proposición 6.20). Usamos ahora la estrategia de la demostración del Teorema 7.3. Por la Observación 6.12(ii), cada raíz de la forma

$$p(X) = a_0 + a_1X^{\frac{1}{r}} + a_2X^{\frac{2}{r}} + \ldots$$

viene en un conjunto de r raíces conjugadas, al variar ω en el conjunto de las r raíces r-ésimas de la unidad,

$$p_\omega(X) = a_0 + a_1\omega X^{\frac{1}{r}} + a_2\omega^2 X^{\frac{2}{r}} + \dots$$

y todas ellas corresponden a una misma rama R en el punto $(0, a_0)$ representada por cualquiera de las parametrizaciones equivalentes

$$(T^r, a_0 + a_1\omega T + a_2\omega^2 T^2 + \dots).$$

Recíprocamente, cada rama en un punto de la curva sobre la recta $V(X)$ viene de un conjunto de raíces conjugadas de esa forma (obviamente, el valor r puede ser distinto para cada rama). Por tanto, vamos que estudiar cuál es la máxima potencia de X que divide a cada subproducto

$$\prod_\omega g(X, p_\omega(X))$$

es decir, debemos calcular

$$O\big(\prod_\omega g(X, p_\omega(X))\big) = \sum_\omega O\big((g(X, p_\omega(X))\big) =$$

$$= \sum_\omega \frac{O\big(g(T^r, a_0 + a_1\omega T + a_2\omega^2 T^2 + \dots)\big)}{r} = \sum_\omega \frac{\mathrm{mult}_{(0,a_0)}(R, V(g))}{r} = \mathop{\mathrm{mult}}_{(0,a_0)}(R, V(g))$$

Por tanto, la máxima potencia de X que divide al subproducto de $\prod_{p(X)} g(X, p(X))$ que corresponde a las ramas en un punto concreto $(0, b)$ es precisamente $\mathrm{mult}_{(0,b)}(V(f), V(g))$, y la máxima potencia de X que divide al producto total es la suma de todas las multiplicidades de intersección en los puntos de $V(X)$, como queríamos. □

Teorema 7.7 (Bézout)**.** *Sean $C, D \subset \mathbb{P}^2_k$ dos curvas sin componentes comunes. Entonces* $\sum_{p \in C \cap D} \mathrm{mult}_p(C, D) = \deg(C)\deg(D)$.

Demostración: Basta rehacer la demostración del Teorema Débil de Bézout (Corolario 2.9), pero usando ya el Lema 7.6. En efecto, tomamos coordenadas de modo que el punto $(0 : 0 : 1)$ no esté ni en C ni en D ni en ninguna recta que una dos puntos de intersección de C y D. Entonces, podemos tomar ecuaciones minimales F y G de C y D respectivamente que sean mónicas en X_2. Por el Teorema 2.8, la resultante de F y G respecto de X_2 es un polinomio homogéneo de grado $\deg(F)\deg(G)$ en X_0, X_1. Entonces factorizará como

$$\mathrm{res}_{X_2}(F, G) = \Pi_i (a_i X_0 + b_i X_1)^{s_i}$$

y evidentemente $\sum_i s_i = \deg(F)\deg(G) = \deg(C)\deg(D)$. Basta por tanto ver que los s_i son las multiplicidades de intersección de las curvas C y D en los distintos puntos. Esto es así porque cada punto de intersección está en alguna de las rectas $V(a_iX_0 + b_iX_1)$, y además, por la elección de coordenadas, cada recta $V(a_iX_0 + b_iX_1)$ contiene un único punto de intersección p_i. Pero el Lema 7.6 implica que $\mathrm{mult}_{p_i}(C, D) = s_i$, lo que concluye la demostración. □

Observación 7.8. Obsérvese que la demostración anterior demuestra que el orden de las curvas no influye a la hora de calcular multiplicidades de intersección. En efecto, la multiplicidad de intersección de D y C en un punto p_i es la multiplicidad de la raíz $(-b_i : a_i)$ en $\mathrm{res}_{X_2}(G, F)$. Y, como $\mathrm{res}_{X_2}(F, G)$ y $\mathrm{res}_{X_2}(G, F)$ difieren como mucho en el signo, se tiene $\mathrm{mult}_{p_i}(D, C) = \mathrm{mult}_{p_i}(C, D)$.

Apliquemos ahora el Teorema de Bézout a un caso concreto. Vimos en el Teorema 5.16 que los puntos de la intersección de una curva con su curva hessiana nos da los puntos de inflexión más los puntos singulares de la curva. Si la curva es de grado d, su curva hessiana es de grado $3(d-2)$, luego $3d(d-2)$ es el número de puntos de inflexión más el número de puntos singulares, cada uno de ellos contados con cierta multiplicidad de intersección (la ecuación H_F de la curva hessiana podría no ser minimal; de todas formas, entenderemos la multiplicidad de intersección de la curva con su hessiana la suma de las multiplicidades de intersección con cada una de las componentes de la hessiana, contadas tantas veces como se repitan). Nuestro objetivo ahora es determinar las multiplicidades de intersección que obtenemos. Empecemos con los puntos de inflexión.

Lema 7.9. *Si $a \in C \subset \mathbb{P}^2_k$ es un punto liso tal que $\mathrm{mult}_a(C, \mathbb{T}_aC) = r$, entonces $\mathrm{mult}_a(C, H_F(a)) = r - 2$, donde F es una ecuación minimal de C. En particular, si C no contiene rectas entonces tiene un número finito de puntos de inflexión.*

Demostración: Haciendo un cambio de coordenadas podemos suponer que $a = (1 : 0 : 0)$ y $\mathbb{T}_aC = V(X_2)$. Esto quiere decir, deshomogeneizando respecto de X_0, que una ecuación minimal de la correspondiente curva afín tiene el aspecto $F(X, Y) = Y + cX^r$ con $c \neq 0$, y una parametrización formal en a es de la forma

$$\begin{cases} X = T \\ Y = -cT^r + \dots \end{cases}$$

Homogeneizando, una ecuación minimal de C es de la forma $F(X_0, X_1, X_2) = X_0^{d-1}X_2 + cX_0^{d-r}X_1^r + \dots$, y una parametrización formal de C en a es de la forma

$$\begin{cases} X_0 = 1 \\ X_1 = T \\ X_2 = -cT^r + \dots \end{cases}$$

Entonces

$$F_{00} = (d-1)(d-2)X_0^{d-3}X_2 + c(d-r)(d-r-1)X_0^{d-r-2}X_1^r + \dots$$

$$F_{01} = cr(d-r)X_0^{d-r-1}X_1^{r-1} + \dots$$

$$F_{02} = (d-1)X_0^{d-2} + \dots$$

$$F_{11} = cr(r-1)X_0^{d-r}X_1^{r-2} + \dots$$

y, por tanto,

$$H_F(1, T, -cT^r + \dots) = \begin{vmatrix} bT^r & cr(d-r)T^{r-1} + \dots & (d-1) + \dots \\ cr(d-r)T^{r-1} + \dots & cr(r-1)T^{r-2} + \dots & \\ (d-1) + \dots & & \end{vmatrix}$$

donde $b = -c(d-1)(d-2) + c(d-r)(d-r-1)$ (aunque no importe cuál es el valor concreto). Como es claro que el término de menor grado es $-cr(r-1)(d-1)^2T^{r-2}$, se sigue que $\mathrm{mult}_a(C, H_F(a)) = r-2$. En particular, es un valor finito, luego hay un número finito de puntos de inflexión. El hecho de que C no contenga rectas es precisamente lo que implica que r sea un valor finito para cualquier punto de inflexión. □

Definición. Se llama *punto de inflexión ordinario* a un punto de inflexión a de una curva C tal que $\mathrm{mult}_a(C, \mathbb{T}_a C) = 3$.

Veamos ahora qué ocurre con los puntos singulares más sencillos. Para ver cuáles son, estudiemos las curvas de grado más pequeño que tengan puntos singulares. Como una cónica irreducible es lisa, tendremos que considerar cúbicas:

Ejemplo 7.10. Sea $C \subset \mathbb{P}_k^2$ una cúbica irreducible. Observamos en primer lugar que C tiene como mucho un punto singular, ya que, si no, la recta que pasa por dos puntos singulares cortaría a C con multiplicidad al menos dos en cada punto singular (por la Proposición 7.4), contradiciendo el Teorema de Bézout. De nuevo por la Proposición 7.4 y el Teorema de Bézout, el punto singular no puede tener multiplicidad mayor estrictamente que dos, así que necesariamente es un punto doble, y por el Teorema 7.3 tendrá o bien dos ramas lisas o una rama doble. Estudiemos separadamente los dos casos:

–Supongamos primero que el punto singular tiene dos ramas lisas. Las tangentes a las ramas no pueden ser iguales, pues en tal caso la recta tangente cortaría a C al menos con multiplicidad cuatro en el punto singular. Por el mismo motivo, ninguna de las rectas tangentes a C en el punto singular puede ser de inflexión.

–Si en cambio el punto singular tiene una única rama que es doble, de nuevo por el Teorema de Bézout la recta tangente a la rama corta con multiplicidad exactamente tres.

Esto motiva las siguientes definiciones:

Definición. Se llama *nodo ordinario* de una curva C a un punto doble $a \in C$ con dos tangentes distintas, y de forma que cada una de ellas corte a la curva con multiplicidad tres en a (o dicho de otro modo, que cada recta tangente corte a la rama correspondiente con multiplicidad dos, es decir, que ninguna de las ramas es de inflexión). Más en general, un *nodo* es un punto singular en que todas las ramas tienen multiplicidad uno y las rectas tangentes a ellas son todas distintas entre sí.

Definición. Se llama *cúspide* a un punto singular que tenga una sola rama. Una *cúspide ordinaria* es una cúspide que es un punto doble tal que la recta tangente corta a la curva en el punto con multiplicidad tres.

Veamos las multiplicidades de intersección en estos puntos entre la curva y su hessiana.

Lema 7.11. *Si $a \in C \subset \mathbb{P}^2_k$ es un nodo ordinario, entonces* $\mathrm{mult}_a(C, H_F(a)) = 6$*, donde F es una ecuación minimal de C.*

Demostración: Mediante un cambio de variable suponemos $a = (1 : 0 : 0)$ y el cono tangente a C en a es $V(X_1X_2)$. Pasando al afín, la ecuación minimal de la curva será de la forma $f(X, Y) = XY$+términos de mayor grado. Además, como $\mathrm{mult}_{(0,0)}(V(f), V(X)) = 3$, necesariamente Y^3 es la máxima potencia de Y que divide a $f(0, Y)$, y simétricamente X^3 es la máxima potencia de X que divide a $f(X, 0)$. Por tanto, f tiene monomios de la forma c_1X^3 y c_2Y^3, con $c_1, c_2 \neq 0$. Homogeneizando, una ecuación minimal de C tiene el aspecto $F = X_0^{d-2}X_1X_2 + c_1X_0^{d-3}X_1^3 + c_2X_0^{d-3}X_2^3 \ldots$ con $c_1, c_2 \neq 0$ y las ramas de C en a se pueden parametrizar como

$$\begin{cases} X_0 = 1 \\ X_1 = T \\ X_2 = -c_1T^2 + \ldots \end{cases} \qquad \begin{cases} X_0 = 1 \\ X_1 = -c_2T^2 + \ldots \\ X_2 = T \end{cases}$$

Entonces tendremos:

$$F_0 = (d-2)X_0^{d-3}X_1X_2 + (d-3)c_1X_0^{d-4}X_1^3 + (d-3)c_2X_0^{d-4}X_2^3 + \ldots$$
$$F_1 = X_0^{d-2}X_2 + 3c_1X_0^{d-3}X_1^2 + \ldots$$
$$F_2 = X_0^{d-2}X_1 + 3c_2X_0^{d-3}X_2^2 + \ldots$$
$$F_{00} = (d-2)(d-3)X_0^{d-4}X_1X_2 + (d-3)(d-4)c_1X_0^{d-5}X_1^3 + (d-3)(d-4)c_2X_0^{d-5}X_2^3 + \ldots$$
$$F_{01} = (d-2)X_0^{d-3}X_2 + 3(d-3)c_1X_0^{d-4}X_1^2 + \ldots$$
$$F_{02} = (d-2)X_0^{d-3}X_1 + 3(d-3)c_2X_0^{d-4}X_2^2 + \ldots$$
$$F_{11} = 6c_1X_0^{d-3}X_1 + \ldots$$

$F_{12} = X_0^{d-2} + \dots$

$F_{22} = 6c_2 X_0^{d-3} X_2 + \dots$

Por tanto, sustituyendo la parametrización de la primera rama en la ecuación del determinante hessiano tendremos:

$$H_F(1, T, -c_1T^2 + \dots) = \begin{vmatrix} -2c_1(d-3)T^3 + \dots & c_1(2d-7)T^2 + \dots & (d-2)T + \dots \\ c_1(2d-7)T^2 + \dots & 6c_1T + \dots & 1 + \dots \\ (d-2)T + \dots & 1 + \dots & -6c_1c_2T^2 + \dots \end{vmatrix} =$$

$$= \big(2c_1(d-2)(2d-7) - 6c_1(d-2)^2 + 2c_1(d-3)\big)T^3 + \dots = -2c_1(d-1)^2T^3 + \dots$$

lo que demuestra que la multiplicidad de intersección de dicha rama con la curva hessiana en el punto a es tres. Por simetría, la otra rama corta también con multiplicidad tres, lo que concluye el resultado. □

Lema 7.12. *Si $a \in C \subset \mathbb{P}^2_k$ es una cúspide ordinaria, entonces* $\text{mult}_a(C, H_F(a)) = 8$, *donde F es una ecuación minimal de C.*

Demostración: De nuevo, podemos suponer que $a = (1 : 0 : 0)$ y que el cono tangente es $V(X_2^2)$. Entonces la rama de C en a se puede parametrizar

$$\begin{cases} X_0 = 1 \\ X_1 = T^2 \\ X_2 = cT^3 + \dots \end{cases}$$

con $c \neq 0$, con lo que una ecuación minimal de C tiene el aspecto

$$F = X_0^{d-2}X_2^2 - c^2X_0^{d-3}X_1^3 + \dots$$

luego

$F_0 = (d-2)X_0^{d-3}X_2^2 - (d-3)c^2X_0^{d-4}X_1^3 + \dots$

$F_1 = -3c^2X_0^{d-3}X_1^2 + \dots$

$F_2 = 2X_0^{d-2}X_2 + \dots$

$F_{00} = (d-2)(d-3)X_0^{d-4}X_2^2 - (d-3)(d-4)c^2X_0^{d-5}X_1^3 + \dots$

$F_{01} = -3(d-3)c^2X_0^{d-4}X_1^2 + \dots$

$F_{02} = 2(d-2)X_0^{d-3}X_2 + \dots$

$F_{11} = -6c^2X_0^{d-3}X_1 + \dots$

$F_{22} = 2X_0^{d-2} + \dots$

(y además cada monomio de F_{12} contiene algún X_1 o X_2). Sustituyendo la parametrización de la rama en la ecuación de la curva hessiana en el punto obtenemos:

$$H_F(1,T^2,cT^3+\ldots)=\begin{vmatrix} 2(d-3)c^2T^6+\ldots & -3(d-3)c^2T^4+\ldots & 2(d-2)cT^3+\ldots \\ -3(d-3)c^2T^4+\ldots & -6c^2T^2+\ldots & (\text{orden}\geq 2) \\ 2(d-2)cT^3+\ldots & (\text{orden}\geq 2) & 2+\ldots \end{vmatrix}$$

$$=\big(-24(d-3)c^4+24(d-2)^2c^4-18(d-3)^2c^4\big)T^8+\ldots=6(d-1)^2c^4T^8+\ldots$$

de donde se obtiene el resultado. □

Podemos ya por fin contar el número de puntos de inflexión de una curva:

Teorema 7.13. *Si una curva irreducible $C\subset\mathbb{P}^2_k$ tiene como únicas singularidades δ nodos ordinarios y κ cúspides ordinarias, y sus puntos de inflexión son todos ordinarios, entonces tiene exactamente $i=3d(d-2)-6\delta-8\kappa$ puntos de inflexión distintos.*

Demostración: Basta juntar el Teorema 5.16 con los Lemas 7.9, 7.11 y 7.12. □

Ejemplo 7.14. Podemos aplicar ahora el Teorema 7.13 para calcular el número de puntos de inflexión de cada tipo de cúbica irreducible (ver Ejemplo 7.10). Observemos en primer lugar que los puntos de inflexión son todos ordinarios, ya que, por el Teorema de Bézout, una recta no puede cortar a una cúbica con multiplicidad mayor que tres en ningún punto. Por tanto tendremos que:

–si la cúbica es lisa, tendrá nueve puntos de inflexión;

–si la cúbica es nodal, tendrá tres puntos de inflexión;

–si la cúbica es cuspidal, tendrá un solo punto de inflexión.

Se puede deducir de aquí que todas las cúbicas nodales son proyectivamente equivalentes, y lo mismo ocurre para las cúbicas cuspidales:

Teorema 7.15. *Toda cúbica irreducible nodal se puede escribir, en un adecuado sistema de coordenadas como $V(X_0X_1^2-X_0X_2^2-X_1^3)$.*

Demostración: Dada una cúbica nodal, podemos escoger coordenadas de modo que el nodo sea $(1:0:0)$ con cono tangente $V(X_1^2-X_2^2)$ y que un punto de inflexión sea $(0:0:1)$ con tangente $V(X_0)$. La condición sobre el nodo es equivalente a que una ecuación minimal de la curva sea de la forma $F=X_0(X_1^2-X_2^2)+$ términos de grado tres en X_1,X_2, y la condición sobre la inflexión es equivalente a que los términos de grado tres en X_1,X_2 consistan sólo en un monomio de la forma cX_1^3, con $c\neq 0$. Por tanto, una ecuación minimal es de la

forma $F = X_0(X_1^2 - X_2^2) + cX_1^3$. Haciendo el cambio $(X_0 : X_1 : X_2) = (-cX_0' : X_1' : X_2')$ se llega al resultado. □

Teorema 7.16. *Toda cúbica irreducible cuspidal se puede escribir, en un adecuado sistema de coordenadas como* $V(X_0X_2^2 - X_1^3)$.

Demostración: Dada una cúbica cuspidal, podemos escoger coordenadas de modo que la cúspide sea $(1 : 0 : 0)$ con recta tangente $V(X_2)$ y que su único punto de inflexión sea $(0 : 0 : 1)$ con recta tangente $V(X_0)$. Como antes, estas condiciones son equivalentes a que una ecuación minimal de la cúbica sea de la forma $F = X_0X_2^2 + cX_1^3$, y un cambio de variable $(X_0 : X_1 : X_2) = (-cX_0' : X_1' : X_2')$ demuestra que cada cúbica cuspidal es proyectivamente equivalente a $V(X_0X_2^2 - X_1^3)$. □

Para las cúbicas lisas, la situación ya no es la misma, ya que existen infinitas clases de equivalencia de cúbicas lisas módulo equivalencia proyectiva, como veremos en el Teorema 8.18.

8. Curva dual. Fórmulas de Plücker

Intentaremos imitar ahora lo que ocurre para cónicas proyectivas irreducibles: que el conjunto de sus rectas tangentes forma otra cónica en el plano proyectivo dual. La primera diferencia sustancial es que no tiene que ser cierto que el conjunto de rectas tangentes de una curva irreducible de grado d sea una curva en el dual del mismo grado; de hecho tal grado no sólo no es d en general, sino que dependerá de más cosas que del grado d de la curva de partida, en concreto de los tipos de puntos singulares que tenga. Esto mismo ocurría en el cálculo del número de puntos de inflexión de una curva. Las fórmulas de este tipo es lo que se llama *fórmulas de Plücker*.

Veamos en primer lugar la existencia de curva dual como curva en el plano proyectivo dual, para lo cual será crucial el siguiente:

Teorema 8.1. *Dada una curva $C \subset \mathbb{P}^2_k$ de grado d, existe un polinomio homogéneo $G \in k[U_0, U_1, U_2]$ de grado $d(d-1)$ tal que $G(u_0, u_1, u_2) = 0$ si y sólo si la recta $V(u_0X_0 + u_1X_1 + u_2X_2)$ corta con multiplicidad al menos dos a C en algún punto. En particular, por el Teorema de Bézout, $G(u_0, u_1, u_2) \neq 0$ si y sólo si la recta $V(u_0X_0 + u_1X_1 + u_2X_2)$ corta a C exactamente en d puntos distintos.*

Demostración: La demostración guarda muchas similitudes con la del Teorema 4.9. Dada una recta $V(u_0X_0 + u_1X_1 + u_2X_2)$ hay distintas formas de parametrizarla, dependiendo de qué valor u_0, u_1, u_2 sea no nulo. En concreto, se trata de escoger dos puntos entre las filas de la matriz

$$\begin{pmatrix} 0 & u_2 & -u_1 \\ -u_2 & 0 & u_0 \\ u_1 & -u_0 & 0 \end{pmatrix}.$$

De este modo, tenemos los siguientes polinomios que se obtienen al sustituir en una ecuación minimal F de C las posibles parametrizaciones:

$$A_0(T_0, T_1) := F\Big(\begin{pmatrix} T_0 & T_1 \end{pmatrix} \begin{pmatrix} -U_2 & 0 & U_0 \\ U_1 & -U_0 & 0 \end{pmatrix} \Big) = F(-U_2T_0 + U_1T_1, -U_0T_1, U_0T_0)$$

$$A_1(T_0, T_1) := F\Big(\begin{pmatrix} T_0 & T_1 \end{pmatrix} \begin{pmatrix} U_1 & -U_0 & 0 \\ 0 & U_2 & -U_1 \end{pmatrix} \Big) = F(U_1T_0, -U_0T_0 + U_2T_1, -U_1T_1)$$

$$A_2(T_0, T_1) := F\Big(\begin{pmatrix} T_0 & T_1 \end{pmatrix} \begin{pmatrix} 0 & U_2 & -U_1 \\ -U_2 & 0 & U_0 \end{pmatrix} \Big) = F(-U_2T_1, U_2T_0, -U_1T_0 + U_0T_1)$$

dependiendo, respectivamente, de si u_0, u_1, u_2 son distintos de cero. La idea sería tomar en cada uno de los casos el discriminante del correspondiente polinomio, que será homogéneo de grado $2d(d-1)$ en U_0, U_1, U_2 (los coeficientes de cada A_i son homogéneos de grado d en U_0, U_1, U_2, y la matriz del discriminante es de orden $2(d-1)$). La clave es que estos

discriminantes están relacionados mediante el polinomio común G buscado de la siguiente forma:

$$\mathrm{Disc}(A_i) = U_i^{d(d-1)} G$$

En efecto, por ejemplo, usando que

$$\begin{pmatrix} U_1 & -U_0 & 0 \\ 0 & U_2 & -U_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ \frac{-U_1}{U_0} & \frac{-U_2}{U_0} \end{pmatrix} \begin{pmatrix} -U_2 & 0 & U_0 \\ U_1 & -U_0 & 0 \end{pmatrix}$$

quitando denominadores tenemos la igualdad

$$A_0\big(\begin{pmatrix} T_0 & T_1 \end{pmatrix} \begin{pmatrix} 0 & U_0 \\ -U_1 & -U_2 \end{pmatrix} \big) = F\big(\begin{pmatrix} T_0 & T_1 \end{pmatrix} \begin{pmatrix} 0 & U_0 \\ -U_1 & -U_2 \end{pmatrix} \begin{pmatrix} -U_2 & 0 & U_0 \\ U_1 & -U_0 & 0 \end{pmatrix} \big) =$$

$$= F\big(U_0 \begin{pmatrix} T_0 & T_1 \end{pmatrix} \begin{pmatrix} U_1 & -U_0 & 0 \\ 0 & U_2 & -U_1 \end{pmatrix} \big) = U_0^d A_1(T_0, T_1),$$

luego el Ejercicio 4.8(iv) implica

$$(U_0 U_1)^{d(d-1)} \mathrm{Disc}(A_0) = U_0^{2d(d-1)} \mathrm{Disc}(A_1)$$

lo que implica la existencia de un polinomio G de grado $d(d-1)$ tal que $\mathrm{Disc}(A_0) = U_0^{d(d-1)} G$ y $\mathrm{Disc}(A_1) = U_1^{d(d-1)} G$. De la misma forma, usando que

$$\begin{pmatrix} 0 & U_2 & -U_1 \\ -U_2 & 0 & U_0 \end{pmatrix} = \begin{pmatrix} \frac{-U_1}{U_0} & \frac{-U_2}{U_0} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -U_2 & 0 & U_0 \\ U_1 & -U_0 & 0 \end{pmatrix}$$

obtenemos

$$A_0\big(\begin{pmatrix} T_0 & T_1 \end{pmatrix} \begin{pmatrix} -U_1 & -U_2 \\ U_0 & 0 \end{pmatrix} \big) = U_0^d A_2(T_0, T_1),$$

y de nuevo por el Ejercicio 4.8(iv) obtenemos

$$(U_0 U_2)^{d(d-1)} \mathrm{Disc}(A_0) = U_0^{2d(d-1)} \mathrm{Disc}(A_2)$$

y por tanto también $\mathrm{Disc}(A_2) = U_2^{d(d-1)} G$.

A la vista de esto, dada una recta $V(u_0 X_0 + u_1 X_1 + u_2 X_2)$ con $u_i \neq 0$, se tiene que corta a C con multiplicidad dos en algún punto si y sólo si A_i tiene una raíz múltiple, y por el Teorema 4.4 eso es equivalente a que su discriminante sea cero, lo que es equivalente a que $G(u_0, u_1, u_2)$ sea cero, como queríamos. □

Obsérvese que, a priori, el polinomio G del enunciado anterior podría ser cero, cosa que descartaremos en breve (ver Corolario 8.8).

Ejemplo 8.2. Al igual que ocurre en el caso de la ecuación implícita de una parametrización (Teorema 4.9), la ecuación G podría no ser una ecuación reducida, con un exponente indicando el número de veces que se recorre la curva dual (ver Ejemplo 4.11). En realidad, eso ocurre sólo en el caso de las curvas extrañas, que ya dijimos en la Observación 5.9 que se daba sólo para cónicas en característica dos. En efecto, tomemos $F := X_0X_2 - X_1^2$. Entonces, si tomamos

$$A_0 := F(-U_2T_0 + U_1T_1, -U_0T_1, U_0T_0) = -U_0U_2T_0^2 + U_0U_1T_0T_1 - U_0^2T_1^2$$

se tiene

$$(A_0)_0 = -2U_0U_2T_0 + U_0U_1T_1$$

$$(A_0)_1 = U_0U_1T_0 - 2U_0^2T_1$$

$$\mathrm{Disc}(A_0) = Res((A_0)_0, (A_0)_1) = \begin{vmatrix} -2U_0U_2 & U_0U_1 \\ U_0U_1 & -2U_0^2 \end{vmatrix} = U_0^2(4U_0U_2 - U_1^2)$$

Por el Teorema 8.1, la ecuación de la cónica dual es $4U_0U_2 - U_1^2$ (que es la que se obtendría usando Geometría Proyectiva). Sin embargo, si el cuerpo base es de característica dos, esa ecuación se convierte en $-U_1^2$, es decir, obtenemos el haz doble de las rectas que pasan por $(0:1:0)$, tal y como vimos en la Observación 5.9.

Ejemplo 8.3. Nótese que la ecuación G del Teorema 8.1 no es todavía la ecuación del conjunto de rectas tangentes a la curva C. En efecto, si C tiene un punto singular, cualquier recta que pase por dicho punto singular cortará a C con multiplicidad al menos dos en dicho punto. Por tanto G contendrá como factores a las ecuaciones (lineales) de los haces de rectas que pasan por los puntos singulares de C. Por ejemplo, si C es la cúbica de ecuación $F := X_0X_2^2 - X_1^3$, entonces tendremos

$$A_0 := F(-U_2T_0 + U_1T_1, -U_0T_1, U_0T_0) = -U_0^2U_2T_0^3 + U_0^2U_1T_0^2T_1 + U_0^3T_1^3$$

$$(A_0)_0 = -3U_0^2U_2T_0^2 + 2U_0^2U_1T_0T_1$$

$$(A_0)_1 = U_0^2U_1T_0^2 + 3U_0^3T_1^2$$

$$\mathrm{Disc}(A_0) = \begin{vmatrix} -3U_0^2U_2 & 2U_0^2U_1 & 0 & 0 \\ 0 & -3U_0^2U_2 & 2U_0^2U_1 & 0 \\ U_0^2U_1 & 0 & 3U_0^3 & 0 \\ 0 & U_0^2U_1 & 0 & 3U_0^3 \end{vmatrix} = 3U_0^9(27U_0U_2^2 + 4U_1^3)$$

Según el Teorema 8.1, el conjunto de rectas que cortan a C con multiplicidad al menos dos en algún punto tiene ecuación $G = 3U_0^3(27U_0U_2^2 + 4U_1^3)$. El factor U_0 corresponde al haz de rectas que pasan por el punto $(1:0:0)$, que es el punto singular de C. Por tanto, la curva dual tendrá ecuación $27U_0U_2^2 + 4U_1^3$ (que es la que tiene que haberse obtenido

en el Ejercicio 5.10). Nótese que en esta curva dual hay un punto que corresponde a una recta que pasa por el punto singular $(1:0:0)$ de C. En efecto, si hacemos $U_0 = 0$, obtenemos el punto $(u_0 : u_1 : u_2) = (0:0:1) \in \mathbb{P}_k^{2^*}$, que corresponde a la recta $V(X_2)$, que es precisamente la recta tangente a C en el punto singular $(1:0:0)$. Por tanto, esta curva dual $V(27U_0U_2^2 + 4U_1^3) \subset \mathbb{P}_k^{2^*}$es exactamente el conjunto de rectas tangentes a C en algún punto, sea singular o no. De hecho, aunque el punto $(1:0:0) \in \mathbb{P}_k^2$ sea singular para C, el correspondiente punto $(0:0:1) \in \mathbb{P}_k^{2^*}$ no es singular para la curva dual (y más precisamente, es un punto de inflexión). Obsérvese que sin embargo esta curva dual sí que tiene un punto singular, que es el punto $(1:0:0) \in \mathbb{P}_k^{2^*}$, que es una cúspide y corresponde a la recta $V(X_0)$, que es la recta tangente a C en el punto $(0:0:1) \in \mathbb{P}_k^2$, que es un punto de inflexión de C (el único punto de inflexión, según el Teorema 7.13). Esta dualidad inflexión/cúspide no es una casualidad, como veremos más adelante.

Definición. Se llama *curva dual* de una curva $C \subset \mathbb{P}_k^2$ a la curva $C^* \subset \mathbb{P}_k^{2^*}$ de ecuación $G' \in k[U_0, U_1, U_2]$, donde G' es el polinomio obtenido a partir de G (del Teorema 8.1) quitando todos los factores lineales que correspondan a haces de rectas que pasan por los puntos singulares de C. Se llama *clase de una curva* C al grado d^* de su curva dual.

Puede demostrarse (aunque no es inmediato) que, como ocurre en el Ejemplo 8.3, la curva C^* es exactamente el conjunto de rectas tangentes a C en algún punto, singular o no (desde luego, en C^* están todas las rectas tangentes a C que no pasan por ningún punto singular de C).

Nótese también que, en el Ejemplo 8.3, el grado de la curva dual coincide con el grado de F, lo que en general no será lo habitual. De hecho, en caso de no tener puntos singulares, el grado de la curva dual habría sido seis. Si hemos llegado a grado tres es porque la ecuación del haz de rectas por el punto singular (que es una cúspide) ha aparecido con multiplicidad tres. Como ocurre en el caso de los puntos de inflexión, cada tipo de singularidad dará lugar a una multiplicidad distinta del factor lineal correspondiente.

Como el lector imaginará, intentar calcular la multiplicidad que corresponde a cada tipo de singularidad parece una tarea complicada (ya es suficientemente complicado el modo de calcular la ecuación G, como para ahora adivinar con qué exponente aparecen sus posibles factores lineales). Intentaremos otro camino bastante más directo que nos permitirá usar de nuevo multiplicidades de intersección:

Observación 8.4. Dado que una recta en el plano dual consiste en un haz de rectas en $\mathbb{P}_k^2$, es decir, el conjunto de rectas de $\mathbb{P}_k^2$ que pasan por un punto dado $a = (a_0 : a_1 : a_2)$, vamos a intentar calcular más a mano cuántas rectas tangentes a una curva pasan por un punto a suficientemente general (que será entonces lo mismo que intersecar la presunta curva dual con una recta suficientemente general, es decir, deberíamos obtener el grado de la curva dual). Si F es una ecuación minimal de la curva, entonces la recta tangente a

$b = (b_0 : b_1 : b_2) \in V(F)$ (que supondremos que es un punto liso de la curva) pasa por a si y sólo si $F_0(b)a_0 + F_1(b)a_1 + F_2(b)a_2 = 0$. Por tanto, los puntos (lisos) de $V(F)$ cuya tangente pasa por a son los puntos que están además en la curva de ecuación $a_0F_0 + a_1F_1 + a_2F_2$ (que tiene grado $d-1$).

Ejemplo 8.5. En el caso en que la curva es una cónica de matriz simétrica M (ver Ejemplo 5.8), ya vimos que, si F es la ecuación de la cónica, entonces se tiene

$$(\, F_0 \;\, F_1 \;\, F_2 \,) = 2\,(\, X_0 \;\, X_1 \;\, X_2 \,)\, M.$$

Por tanto, la ecuación $a_0F_0 + a_1F_1 + a_2F_2$ de la observación anterior se puede escribir como

$$(\, X_0 \;\, X_1 \;\, X_2 \,)\, M \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$$

que es la ecuación de lo que, en Geometría Proyectiva, se llama *recta polar del punto a respecto de la cónica*.

Damos, pues, la siguiente:

Definición. Dada una curva C de ecuación minimal F, se llama *curva polar del punto $a = (a_0 : a_1 : a_2)$ respecto de la curva C* a la curva

$$P(a, C) = V(a_0F_0 + a_1F_1 + a_2F_2).$$

Observación 8.6. La noción de curva polar no depende de la elección de coordenadas. En efecto, si hacemos un cambio de coordenadas

$$(\, X_0 \;\, X_1 \;\, X_2 \,) = (\, X_0' \;\, X_1' \;\, X_2' \,) \begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{10} & m_{11} & m_{12} \\ m_{20} & m_{21} & m_{22} \end{pmatrix}$$

que escribiremos, por brevedad, como $\bar{X} = \bar{X}'M$, entonces el punto a tendrá coordenadas

$$\begin{pmatrix} a_0' \\ a_1' \\ a_2' \end{pmatrix} = (M^t)^{-1} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$$

mientras que la curva C tendrá como ecuación minimal

$$F'(X_0', X_1', X_2') = F'(\bar{X}') := F(\bar{X}'M) =$$

$$= F(m_{00}X_0' + m_{10}X_1' + m_{20}X_2', m_{01}X_0' + m_{11}X_1' + m_{21}X_2', m_{02}X_0' + m_{12}X_1' + m_{22}X_2')$$

y, por la regla de la cadena, será

$$\begin{pmatrix} F_0'(\bar{X}') & F_1'(\bar{X}') & F_2'(\bar{X}') \end{pmatrix} = \begin{pmatrix} F_0(\bar{X}'M) & F_1(\bar{X}'M) & F_2(\bar{X}'M) \end{pmatrix} \begin{pmatrix} m_{00} & m_{10} & m_{20} \\ m_{01} & m_{11} & m_{21} \\ m_{02} & m_{12} & m_{22} \end{pmatrix}.$$

Por tanto, la ecuación de la curva polar en las nuevas coordenadas es

$$\begin{pmatrix} F_0'(\bar{X}') & F_1'(\bar{X}') & F_2'(\bar{X}') \end{pmatrix} \begin{pmatrix} a_0' \\ a_1' \\ a_2' \end{pmatrix} = \begin{pmatrix} F_0(\bar{X}'M) & F_1(\bar{X}'M) & F_2(\bar{X}'M) \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}$$

que no es otra cosa que hacer el cambio de coordenadas en la ecuación original de la curva polar.

En las consideraciones que hemos hecho antes necesitábamos trabajar con puntos no singulares de la curva. De hecho, se tiene:

Proposición 8.7. *Dado un punto $a \in \mathbb{P}^2$, si definimos $\Sigma_a = \{b \in C \setminus Sing(C) \mid a \in \mathbb{T}_b C\}$, entonces*

$$C \cap P(a, C) = \Sigma_a \cup \mathrm{Sing}(C).$$

Demostración: Evidentemente los puntos singulares de C están en cualquier $P(a, C)$, ya que anulan todas las derivadas de F. Por tanto, hay que ver que para un punto $b \in C$ no singular se tiene que $b \in P(a, C)$ si y sólo si $a \in \mathbb{T}_b C$. Pero esto es precisamente lo que hemos visto en la Observación 8.4. □

Este primer resultado ya nos permite demostrar que el polinomio que define la curva dual no es idénticamente nulo. Lo haremos en el caso irreducible de grado al menos dos, aunque en realidad, con un poco más de esfuerzo, se puede demostrar para curvas que no sean unión de rectas.

Corolario 8.8. *Si $C \subset \mathbb{P}_k^2$ un curva irreducible de grado $d \geq 2$. Entonces el polinomio G del Teorema 8.1 no es cero. En particular:*

(i) La curva dual $C^* \subset \mathbb{P}_k^{2^*}$ es un subconjunto propio.

(ii) El conjunto de rectas cuya intersección con C no son d puntos distintos forma una curva en $\mathbb{P}_k^{2^*}$.

Demostración: Tomamos por ejemplo $a = (1 : 0 : 0)$ (en realidad sirve cualquier punto). Entonces $P(a, C)$ viene definido por F_0, que necesariamente es no nulo (si $F_0 = 0$, entonces[(*)] F sería un polinomio homogéneo de grado d en X_1, X_2, luego definiría una unión

[(*)] En este punto es fundamental que la característica del cuerpo sea cero o suficientemente grande, para evitar que F_0 pueda se cero a pesar de que F dependa de X_0.

de rectas, en contra de la hipótesis). Como F es irreducible, F_0 (que tiene grado menor) no puede compartir componentes con F, luego $V(F) \cap V(F_0)$ es un conjunto finito de puntos (por el Teorema Débil de Bézout). Por tanto, la Proposición 8.7 implica que hay sólo una cantidad finita de rectas que pasan por a y que cortan a C con multiplicidad al menos dos en algún punto. Por tanto hay infinitas rectas que pasan por a que no están en $V(G)$, lo que demuestra que G no es el polinomio nulo.

La consecuencia (i) se sigue de que, por definición, la ecuación de la curva dual es un divisor de G. La consecuencia (ii) es simplemente porque, por definición de G, el conjunto de rectas cuya intersección con C no son d puntos distintos es precisamente $V(G)$. □

Hemos llegado con la Proposición 8.7 al punto de partida. Para calcular el grado de la curva dual o bien calculamos la ecuación G del Teorema 8.1 o bien calculamos el número de puntos de intersección de la curva con una curva polar general. En ambos casos obtenemos como resultado $d(d-1)$, pero debemos descontar la contribución de los puntos singulares de la curva. Es esperable, aunque no lo demostraremos, que la contribución a la ecuación G de un punto singular de la curva sea la misma que la mutiplicidad de intersección en ese punto de la curva con la curva polar. Un primer indicio es que, para puntos lisos que no sean de inflexión, tal multiplicidad de intersección sea uno, como indica el siguiente:

Lema 8.9. *Si $b \in C$ es un punto liso tal que $\mathrm{mult}_b(C, \mathbb{T}_b C) = r$, entonces para cada $a \in \mathbb{T}_b C$ se tiene:*

$$\mathrm{mult}_b(C, P(a, C)) = \begin{cases} r-1 \text{ si } a \neq b \\ r \text{ si } a = b. \end{cases}$$

Demostración: Haciendo un cambio de coordenadas podemos suponer que $b = (1:0:0)$ y $\mathbb{T}_b C = V(X_2)$. Esto quiere decir (véase la demostración del Lema 7.9) que una parametrización formal de C en b es de la forma

$$\begin{cases} X_0 = 1 \\ X_1 = T \\ X_2 = -cT^r + \dots \end{cases}$$

con $c \neq 0$, y una ecuación minimal de C tiene el aspecto

$$F(X_0, X_1, X_2) = X_0^{d-1} X_2 + c X_0^{d-r} X_1^r + \dots$$

Un punto $a \in \mathbb{T}_b C$ tiene coordenadas $(a_0 : a_1 : 0)$, con lo que la ecuación de la polar a a respecto de C está definida por

$$a_0 F_0 + a_1 F_1 = a_0\big((d-1)X_0^{d-2} X_2 + c(d-r) X_0^{d-r-1} X_1^r + \dots\big) + a_1\big(rc X_0^{d-r} X_1^{r-1} + \dots\big)$$

Sustituyendo en esta ecuación la parametrización formal de la curva en el punto tenemos que el término de menor grado es

$$rca_1T^{r-1} \text{ si } a_1 \neq 0$$
$$-(r-1)ca_0T^r \text{ si } a_1 = 0$$

Como $a_1 = 0$ es equivalente a $a = b$ se sigue el resultado. □

Pasamos ahora a la contribución de los puntos singulares dependiendo del tipo de singularidad.

Lema 8.10. *Si b es un punto doble de C con dos tangentes distintas, entonces se tiene* $\text{mult}_b(C, P(a, C)) \geq 2$ *con igualdad si y sólo si a no está en ninguna recta tangente a C en b.*

Demostración: Mediante un cambio de variable suponemos $b = (1 : 0 : 0)$ y el cono tangente a C en b es $V(X_1X_2)$. Esto quiere decir que una ecuación minimal de C tiene el aspecto $F = X_0^{d-2}X_1X_2 + \ldots$. La curva polar de un punto $a = (a_0 : a_1 : a_2)$ respecto de C tiene ecuación

$$a_0F_0 + a_1F_1 + a_2F_2 = a_0((d-2)X_0^{d-3}X_1X_2 + \ldots) + a_1(X_0^{d-2}X_2 + \ldots) + a_2(X_0^{d-2}X_1 + \ldots)$$

Entonces la recta tangente a $P(a, C)$ en b es $V(a_2X_1 + a_1X_2)$ que es distinta de $V(X_1)$ y $V(X_2)$ si $a_1, a_2 \neq 0$ (que es nuestra hipótesis de que a no está ni en $V(X_1)$ ni en $V(X_2)$). El resultado se sigue ahora de la Proposición 7.5. □

Lema 8.11. *Si b es una cúspide ordinaria de C, entonces* $\text{mult}_b(C, P(a, C)) \geq 3$, *con igualdad si y sólo si a no está en la recta tangente a C en b.*

Demostración: Como en la demostración del Lema 7.12, podemos suponer que $b = (1 : 0 : 0)$ y que el cono tangente es $V(X_2^2)$. Entonces la rama de C en b se puede parametrizar

$$\begin{cases} X_0 = 1 \\ X_1 = T^2 \\ X_2 = cT^3 + \ldots \end{cases}$$

con $c \neq 0$, y una ecuación minimal de C tiene el aspecto

$$F = X_0^{d-2}X_2^2 - c^2X_0^{d-3}X_1^3 + \ldots$$

de donde

$$F_0 = (d-2)X_0^{d-3}X_2^2 - (d-3)c^2X_0^{d-4}X_1^3 + \ldots$$

$F_1 = -3c^2X_0^{d-3}X_1^2 + \ldots$

$F_2 = 2X_0^{d-2}X_2 + \ldots$

Entonces la curva polar de un punto $a = (a_0 : a_1 : a_2)$ respecto de C tiene ecuación

$$a_0((d-2)X_0^{d-3}X_2^2 - (d-3)c^2X_0^{d-4}X_1^3 + \ldots) + a_1(-3c^2X_0^{d-3}X_1^2 + \ldots) + a_2(2X_0^{d-2}X_2 + \ldots).$$

Sustituyendo en esta ecuación la parametrización de C en b se obtiene $2a_2cT^3 + \ldots$, luego $\mathrm{mult}_b(C, P(a, C)) \geq 3$, con igualdad si y sólo si $a_2 \neq 0$, es decir, si y sólo si a no está en la recta tangente a C en b. □

Observación 8.12. Los resultados anteriores nos indican ya (aunque sólo en modo intuitivo) cuál debería ser el grado de la curva dual en el caso de que las únicas singularidades de la curva original sean nodos y cúspides ordinarias. En efecto, sabemos que la ecuación G del Teorema 8.1 factoriza como

$$G = G' \cdot \prod_{b \in \mathrm{Sing}(C)} H_b^{m_b}$$

donde H_b es la ecuación (lineal) del haz de rectas que pasan por b, que aparece con cierta multiplicidad. El Lema 8.10 nos dice que, si b es un nodo ordinario, m_b debe ser dos. Además, como las rectas tangentes a C en b cuentan con multiplicidad mayor, deben anularse en G', es decir, que están en la curva dual. De la misma forma, el Lema 8.11 indica que, si b es una cúspide ordinaria, m_b debe ser tres, y la recta tangente a C en b también está en la curva dual. Por tanto, si las singularidades de C son exactamente δ nodos ordinarios y κ cúspides ordinarias, debería ser $\deg(G') = d(d-1) - 2\delta - 3\kappa$.

Como lo que hemos afirmado en la observación anterior no es evidente (por muy intuitivo que parezca), calculemos el grado de la curva dual usando el Teorema 8.1 (sabiendo ya que G es un polinomio no nulo), es decir, que el grado de una curva es el número de puntos distintos que se obtiene al cortar la curva con una recta suficientemente general (en concreto, que no pase por ningún punto singular y que no sea tangente a la curva, es decir, que no corresponda a un punto de la curva dual). Para aplicar esto a C^*, necesitaremos saber quiénes son sus puntos singulares y, sobre todo, saber cuál es su curva dual.

Teorema 8.13. *Si $C \subset \mathbb{P}^2_k$ es una curva irreducible de grado $d \geq 2$, entonces:*

(i) $(C^*)^* = C$.

(ii) Cada punto de inflexión ordinario de C da lugar a una rama de C^* que es una cúspide ordinaria.

(iii) Cada bitangente (en exactamente dos puntos, y que no son de inflexión) de C da lugar a un nodo ordinario de C^*.

(iv) Cada cúspide ordinaria de C da lugar a una rama de C^* que es una inflexión ordinaria.

(v) Cada nodo ordinario de C da lugar a una bitangente de C^*.

Demostración: Sea $\mathbb{T}_b C$ un punto de C^* que corresponde a un punto liso $b \in C$. Las rectas que pasan por ese punto de ${\mathbb{P}^2_k}^*$ son los haces de rectas de $\mathbb{P}^2_k$ que pasan por un punto $a \in \mathbb{T}_b C$. La intersección de cada haz con C^* son las rectas tangentes a C que pasan por a. Por el Lema 8.9, si $r := mult_p(C, \mathbb{T}_b C)$, la multiplicidad de intersección del haz con C^* es $r-1$, salvo que $a = b$, en que la multiplicidad de intersección es r. Eso demuestra que C^* tiene en $\mathbb{T}_b C$ un punto de multiplicidad $r-1$ con recta tangente dada por el haz de rectas que pasan por b. Por tanto, $b \in (C^*)^*$, y todos los puntos, salvo una cantidad finita, de $(C^*)^*$ se obtienen de esa forma, es decir, están en C. Como C es irreducible, se concluye que $(C^*)^*$ y C coinciden, lo que demuestra (i).

De paso, particularizando la demostración anterior cuando b es un punto de inflexión ordinario (es decir, $r = 3$), se obtiene una cúspide ordinaria de C^* (o más bien una rama, ya que la tangente en el punto de inflexión puede ser tangente en más puntos de C, y por tanto dar lugar al mismo punto de C^*). Esto demuestra (ii).

La parte (iii) es clara, y las partes (iv) y (v) son las duales respectivas de (ii) y (iii), usando (i) □

Definición. Llamaremos *curva ordinaria* a una curva irreducible $C \subset \mathbb{P}^2_k$ tal que las únicas singularidades de C y C^* son nodos y cúspides ordinarias, es decir, que sus puntos de inflexión son ordinarios y sus bitangentes lo son sólo en dos puntos, ninguno de ellos de inflexión. Obsérvese que el número de bitangentes (y de puntos de inflexión) es necesariamente finito, ya que dan puntos singulares de C^*.

Podemos ya por fin calcular el grado de la curva dual:

Teorema 8.14. *Sea $C \subset \mathbb{P}^2_k$ una curva ordinaria de grado $d \geq 2$, y cuyas únicas singularidades son δ nodos ordinarios y κ cúspides ordinarias. Entonces C^* tiene grado*

$$d^* = d(d-1) - 2\delta - 3\kappa.$$

Demostración: Por el Corolario 8.8(ii) aplicado a C^*, el grado de C^* será el número de puntos distintos que se obtengan al cortar C^* con una recta de ${\mathbb{P}^2_k}^*$ que no esté en cierta curva de $({\mathbb{P}^2_k}^*)^*$. En concreto, tal recta no debe estar ni en la curva dual de C^* ni pasar por un punto singular de C^*. Como una recta de ${\mathbb{P}^2_k}^*$ es el haz de rectas que pasan por un cierto punto $a \in \mathbb{P}^2_k$, la condición es (por el Teorema 8.13), que a no esté ni en C (que es la curva dual a C^*), ni en ninguna recta bitangente o de inflexión (que son las rectas que son puntos singulares de C^*). Por simplicidad, supondremos también que a no esté en ninguna recta tangente en los puntos singulares.

Por la Proposición 8.7 y los Lemas 8.9, 8.10 y 8.11, habrá exactamente d^* puntos en C cuya tangente pase por a, que además serán puntos lisos de C. Como a no está en C, cada una de tales rectas tangentes es necesariamente la recta que pasa por a y el correspondiente punto de C encontrado. Además, como a no está en ninguna recta bitangente, dos puntos distintos de C darán lugar a dos rectas tangentes distintas que pasen por a. De este modo, encontramos exactamente d^* rectas tangentes distintas a C que pasan por a, por lo que d^* es el grado de C^*. □

Podemos agrupar entonces todas las fórmulas que tenemos y sus duales:

Teorema 8.15 (Fórmulas de Plücker)**.** *Sea $C \subset \mathbb{P}^2_k$ una curva ordinaria de grado $d \geq 2$, clase d^*, con δ nodos ordinarios, κ cúspides ordinarias, i puntos de inflexión y b rectas bitangentes. Entonces:*

(i) $d^* = d(d-1) - 2\delta - 3\kappa$.

(ii) $i = 3d(d-2) - 6\delta - 8\kappa$

(iii) $d = d^*(d^*-1) - 2b - 3i$

(iv) $\kappa = 3d^*(d^*-2) - 6b - 8i$

Demostración: La fórmula (i) es el Teorema 8.14, y la fórmula (ii) es el Teorema 7.13. Las fórmulas (iii) y (iv) son las duales respectivas de (i) y (ii) (es decir, las dos primeras fórmulas aplicadas a C^*). □

Ejemplo 8.16. Se pueden hacer más combinaciones con las fórmulas de Plücker. Consideremos, por ejemplo, una curva C irreducible ordinaria lisa de grado $d \geq 2$. Entonces, las dos primeras fórmulas de Plücker dan

$$d^* = d(d-1)$$
$$i = 3d(d-2)$$

y sustituyendo estos valores en la tercera, tendremos

$$d = (d^2-d)(d^2-d-1) - 2b - 9d(d-2).$$

De aquí se deduce

$$b = \frac{1}{2}(d^4 - 2d^3 - 9d^2 + 18d) = \frac{1}{2}d(d-2)(d-3)(d+3).$$

En concreto, si $d = 4$, se obtiene que una cuártica lisa con todos sus puntos de inflexión ordinarios tiene 28 rectas bitangentes.

Terminamos esta sección volviendo a la clasificación de cúbicas irreducibles, observando que en el caso liso hay infinitos tipos. Comenzamos por un lema técnico que nos será además útil más adelante.

Lema 8.17. *Si $C \subset \mathbb{P}^2_k$ es una cúbica lisa (y por tanto, irreducible) y $a \in C$ es un punto de inflexión, entonces existen exactamente 4 rectas tangentes a C que pasan por a.*

Demostración: Los puntos de tangencia serán los puntos b de la intersección de C con $P(a, C)$. Sabemos que nos deben quedar seis puntos contados con multiplicidad. Distinguimos dos casos:

–Si $b = a$, entonces, por el Lema 8.9, como $\text{mult}_a(C, \mathbb{T}_a C) = 3$ (recordemos que los puntos de inflexión deben ser ordinarios), se tiene que $\text{mult}_a(C, P(a, C)) = 3$.

–Si $b \neq a$, el punto b no puede ser de inflexión, ya que entonces $\mathbb{T}_b C$ cortaría a C en b con multiplicidad al menos tres, y además cortaría en el punto a, contradiciendo el Teorema de Bézout. Por tanto $\text{mult}_b(C, \mathbb{T}_b C) = 2$, y el Lema 8.9 implica que $\text{mult}_b(C, P(a, C)) = 1$.

Por tanto, aparte de $b = a$, hay otros tres puntos $b \in C$ tales que $\mathbb{T}_b C \ni a$. Por el Teorema de Bézout, las rectas tangentes en estos tres puntos son distintas, y además son distintas de $\mathbb{T}_a C$, con lo que obtenemos exactamente cuatro rectas tangentes a C que pasen por a. □

Teorema 8.18. *Toda cúbica lisa se puede escribir, en un adecuado sistema de coordenadas como $V(X_0X_2^2 - X_1(X_1 - X_0)(X_1 - \lambda X_0))$ para algún $\lambda \neq 0, 1$.*

Demostración: Dada una cúbica irreducible lisa C, tomamos coordenadas de forma que $a = (0 : 0 : 1)$ sea un punto de inflexión y su recta tangente sea $V(X_0)$. Esto quiere decir que una ecuación minimal de C es de la forma $F = X_0G - X_1^3$. Usando el Lema 8.17, podemos escoger entonces coordenadas de modo que las rectas tangentes a C que pasen por a sean $V(X_0)$, $V(X_1)$, $V(X_1 - X_0)$ y $V(X_1 - \lambda X_0)$ (nótese que λ no lo podemos fijar, ya que es precisamente la razón doble de las cuatro rectas, que puede tomar un valor arbitrario).

Como $P(a, C)$ tiene de ecuación $F_2 = X_0G_2$, eso quiere decir que los puntos $b \neq a$ tales que $\mathbb{T}_b C \ni a$ están en la recta $V(G_2)$. Además, G_2 no puede depender sólo de X_0, X_1, porque en tal caso la recta $V(G_2)$ contendría también al punto $(0 : 0 : 1)$. Podemos entonces hacer un cambio de coordenadas que deje fijos X_0, X_1 pero que transforme G_2 en $2X_2$. Entonces, en estas nuevas coordenadas, $G = X_2^2 + H(X_0, X_1)$, luego podemos escribir la ecuación F como

$$F = X_0X_2^2 - X_1^3 + X_0H(X_0, X_1).$$

Como al cortar con $V(X_2)$ debemos obtener los puntos $(1 : 0 : 0)$, $(1 : 1 : 0)$ y $(1 : \lambda : 0)$, necesariamente $-X_1^3 + X_0H(X_0, X_1) = -X_1(X_1 - X_0)(X_1 - \lambda X_0)$, lo que termina la demostración. □

Observación 8.19. Obsérvese que, en la demostración hemos visto un hecho para nada evidente: que, dado un punto de inflexión a, los tres puntos distintos de a cuya tangente pasa por a están alineados. En la siguiente sección demostraremos este hecho sin coordenadas.

Como hay infinitos valores de λ y el número de puntos de inflexión y el de las posibles permutaciones de las rectas tangentes que pasan por un punto de inflexión son siempre un número finito, esto demuestra que hay infinitos tipos de cúbicas lisas. De hecho, el tipo de cúbica viene dado por λ salvo permutación en las rectas. Recordemos que, al permutar cuatro puntos (o hiperplanos), la razón doble λ cambia a $\frac{1}{\lambda}$, $1-\lambda$, $\frac{1}{1-\lambda}$, $\frac{\lambda}{\lambda-1}$, $\frac{\lambda-1}{\lambda}$. Puede comprobarse que, definiendo $j(\lambda) = \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$, se tiene que $j(\lambda) = j(\lambda')$ si y sólo si λ' es uno de los valores λ, $\frac{1}{\lambda}$, $1-\lambda$, $\frac{1}{1-\lambda}$, $\frac{\lambda}{\lambda-1}$, $\frac{\lambda-1}{\lambda}$. Por tanto, dos cúbicas lisas son proyectivamente equivalentes si y sólo si tienen el mismo invariante j.

9. Curvas de género bajo

La topología ha jugado siempre un papel importante en la geometría. De hecho, los teoremas más importantes de la geometría suelen tener trasfondo topológico. En esta sección veremos que también la geometría de las curvas depende fuertemente de su topología, más en concreto del género topológico de las mismas, para cuya definición daremos por supuestos algunos resultados topológicos que recordaremos brevemente.

La construcción general se hace para curvas proyectivas complejas. Dada una curva $C \subset \mathbb{P}^2_{\mathbb{C}}$ irreducible, consideraremos $\tilde{C}$ el conjunto de ramas de C, y llamaremos $\pi : \tilde{C} \to C$ a la aplicación que manda cada rama de C al punto de C en el que está definida la rama. Entonces para cada punto de $\tilde{C}$ tenemos la correspondiente parametrización de la rama, que puede demostrarse que es analítica, y por tanto tenemos una biyección entre un disco complejo y un entorno pequeño de $\tilde{C}$. Cuando la curva es irreducible, esto dota a $\tilde{C}$ de una estructura de superficie topológica (llamada *superficie de Riemann* asociada a la curva C), que es conexa, compacta, orientable y sin borde. Es un hecho conocido de topología que toda superficie topológica conexa, compacta, orientable y sin borde es homeomorfa a una superficie esférica con g asas, y se dice que g es el *género topológico* de la superficie. Por ejemplo, si $g = 1$ la superficie es homemomorfa a un toro, es decir, la superficie de un donut (o de una rosquilla, si queremos ser más castizos).

Definición. Se llama *género de una curva proyectiva irreducible* $C \subset \mathbb{P}^2_{\mathbb{C}}$ al género topológico de $\tilde{C}$.

Hay un modo práctico de calcular el género topológico de una superficie topológica. Consideremos una triangulación de la misma. Esto consiste, a grandes rasgos, en poner la superficie como unión de polígonos cerrados, con la condición de que la intersección de dos polígonos es o bien una arista o bien un vértice o bien el vacío. Por ejemplo, dar una triangulación en una superficie esférica es lo mismo que considerar un poliedro. En tiempos era un resultado que se explicaba incluso en Primaria que, dado cualquier poliedro, se satisfacía el famoso Teorema de Euler

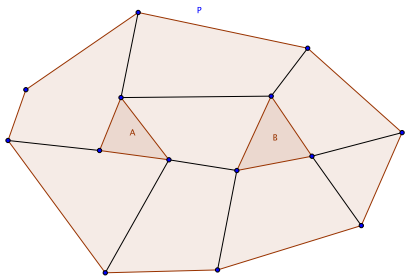
$$v + c = a + 2$$

donde v, a, c son respectivamente el número de vértices, aristas y caras del poliedro. Es decir, el número $v - a + c$ es siempre dos, independientemente del poliedro, es decir, independientemente de la triangulación. En realidad, este resultado es cierto para cualquier superficie topológica S (e incluso para cualquier variedad topológica de cualquier dimensión): Dada cualquier triangulación de S, el número $v-a+c$ es independiente de la triangulación, y se llama *característica de Euler* de S, y se denota por $\chi(S)$.

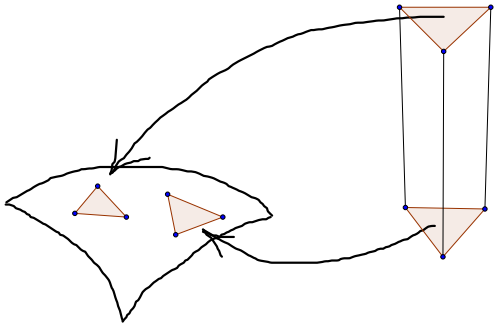
El teorema siguiente permite caracterizar el género topológico de una superficie topológica conexa, compacta, orientable y sin borde a partir de su característica de Euler:

Teorema 9.1. *La característica de Euler de una esfera con g asas es $2-2g$.*

Demostración: Lo haremos por inducción sobre g. El caso $g=0$ es precisamente el clásico Teorema de Euler. Supongamos ahora $g>0$ y que el teorema es cierto para una esfera con $g-1$ asas. Consideramos entonces una superficie S' que sea homeomorfa a una esfera con $g-1$ asas. La idea es pegarle una nueva asa. Para ello, tomamos una triangulación de S' suficientemente fina como para que contenga dos polígonos disjuntos, que podemos tomar que sean triángulos; por ejemplo, si P es un polígono de cualquier triangulación de S', tomamos dos triángulos disjuntos A y B en su interior, y añadiendo adecuadamente aristas podemos llegar a una triangulación como la que queremos (ver figura).



Quitamos esos dos triángulos y tapamos los huecos pegando un prisma triangular (sin base ni tapa), haciendo coincidir la base del prisma con un triángulo y la tapa del prisma con el otro (ver figura).



Obtenemos entonces una esfera con g asas con una triangulación en que:

–El número de caras de esta triangulación es el de la triangulación de S', menos los dos triángulos que hemos quitado más las tres paredes del prisma (la base y la tapa del prisma no cuentan, ya que no estaban). Por tanto, $c=c'-2+3=c'+1$.

–El número de aristas de la nueva triangulación es el de la triangulación de S' (aunque hayamos quitado dos triángulos, sus aristas siguen siendo aristas de la nueva triangulación) más las tres aristas verticales del prisma. Por tanto, $a=a'+3$.

–El número de vértices no varía, ya que ni desaparecen los vértices de los triángulos que hemos quitado ni el prisma aporta vértices nuevos (puesto que los vértices del prisma son exactamente los vértices de esos dos triángulos). Por tanto, $v = v'$.

Podemos calcular entonces la característica de Euler de la nueva superficie topológica S, que será

$$\chi(S) = v - a + c = v' - (a' + 3) + (c' + 1) = v' - a' + c' - 2 = 2 - 2(g-1) - 2 = 2 - 2g$$

(donde hemos usado la hipótesis de inducción $\chi(S') = 2 - 2(g-1)$). □

Aplicamos ahora el resultado anterior para calcular el género topológico de una curva con singularidades ordinarias.

Teorema 9.2. *El género de una curva irreducible compleja C de grado d cuyas únicas singularidades son δ nodos ordinarios y κ cúspides ordinarias es $\frac{(d-1)(d-2)}{2} - \delta - \kappa$.*

Demostración: Observamos primero que hay una cantidad finita de cada uno de los siguientes tipos de recta:

–tangentes en un punto de inflexión,

–tangentes en un punto singular,

–que pase por un punto singular y que sea tangente en otro punto de C (basta observar que la intersección de C con la polar del punto singular da una cantidad finita de puntos),

–tangente en dos puntos distintos de C,

-recta que pase por dos puntos singulares.

Tomamos entonces un punto $a \in \mathbb{P}^2_k$ que no esté ni en C ni en ninguna de las rectas anteriores. Tomamos L una recta que no pase por a y consideramos la composición $\varphi : \tilde{C} \xrightarrow{\pi} C \xrightarrow{\pi_a} L$, donde π_a es la proyección desde a sobre L. Por nuestras hipótesis, $P(a, C)$ corta a C en $d^* := d(d-1) - 2\delta - 3\kappa$ puntos lisos $p_1, \ldots, p_{d^*}$ (con multiplicidad uno por el Lema 8.9), en los δ nodos $r_1, \ldots, r_\delta$ (con multiplicidad dos por el Lema 8.10) y en las κ cúspides $s_1, \ldots, s_\kappa$ (con multiplicidad tres por el Lema 8.11). Observamos entonces que la imagen inversa por φ de un punto de L consiste en d puntos, excepto para $\pi_a(p_1), \ldots, \pi_a(p_{d^*}), \pi_a(s_1), \ldots, \pi_a(s_\kappa)$, en que la imagen inversa consiste en $d-1$ puntos distintos (nótese que, aunque la imagen inversa por π_a de la imagen de un nodo son $d-1$ puntos de C, cada nodo da lugar a dos puntos de $\tilde{C}$).

Fijamos una triangulación en L suficientemente fina para que tenga como vértices los puntos $\pi_a(p_1), \ldots, \pi_a(p_{d^*}), \pi_a(r_1), \ldots, \pi_a(r_\delta), \pi_a(s_1), \ldots, \pi_a(s_\kappa)$ y de forma que la imagen inversa por φ de cada arista o cara sean d aristas o caras. En particular, la imagen inversa

de la triangulación será una triangulación de $\tilde{C}$. Si la triangulación en L tiene v vértices, entonces, por lo observado anteriormente, la triangulación de $\tilde{C}$ tendrá $\tilde{v}$ vértices, donde

$$\tilde{v} = dv - d^* - \kappa = dv - d(d-1) + 2\delta + 2\kappa.$$

Por construcción, si a es el número de aristas de la triangulación de L, entonces el número de aristas de la triangulación de $\tilde{C}$ es $\tilde{a} = da$, y, si c es el número de caras de la triangulación de L, entonces el número de caras de la triangulación de $\tilde{C}$ es $\tilde{c} = dc$. Teniendo en cuenta que, por ser L una superficie esférica (ya que es $\mathbb{P}^1_{\mathbb{C}}$), $v-a+c = 2$, entonces la característica de Euler de $\tilde{C}$ es

$$\chi(\tilde{C}) = \tilde{v}-\tilde{a}+\tilde{c} = d(v-a+c)-d(d-1)+2\delta+2\kappa = 2d-d^2+d+2\delta+2\kappa = -d^2+3d+2\delta+2\kappa$$

luego, por el Teorema 9.1, el género de C es

$$g = \frac{2-\chi(\tilde{C})}{2} = \frac{d^2-3d+2-2\delta-2\kappa}{2} = \frac{(d-1)(d-2)}{2} - \delta - \kappa$$

lo que demuestra el resultado. □

La demostración anterior deja bastante claro que el mismo tipo de cálculo se puede hacer para una curva con singularidades arbitrarias. De hecho, basta ver simplemente cuánto hace disminuir el género cada tipo de singularidad. Lo que está claro es que $\frac{(d-1)(d-2)}{2} - g$ es el número de puntos singulares, cada uno contado un cierto número de veces. Por tanto, el número de puntos singulares nunca puede superar $\frac{(d-1)(d-2)}{2}$, y cuando se alcanza entonces $g = 0$.

Por otra parte, el hecho de que el género sea cero es una condición necesaria para que una curva se pueda parametrizar. En efecto, si tenemos una parametrización buena de una curva C, es decir, que no recorra la curva varias veces, (ver Ejemplo 4.11), entonces tendremos un homeomorfismo de $\mathbb{P}^1_{\mathbb{C}}$ con $\tilde{C}$, y por tanto $\chi(\tilde{C}) = \chi(\mathbb{P}^1_{\mathbb{C}}) = 2$. Como indicamos al inicio de la sección, esta simple condición topológica caracteriza el hecho de que una curva se pueda parametrizar, es decir, que la condición de tener género cero es suficiente para que la curva se pueda parametrizar. Este profundo resultado se puede demostrar sin usar directamente la topología (y por tanto sin trabajar sobre el cuerpo de los números complejos). Ésta es la idea subyacente al resultado siguiente:

Teorema 9.3. *Si C es una curva irreducible de grado d, entonces el máximo número de puntos singulares que puede tener es $\frac{1}{2}(d-1)(d-2)$. Además, una curva con tal número de puntos singulares se puede parametrizar.*

Demostración: El resultado es inmediato para $d = 1, 2$, así que supondremos $d \geq 3$. Supongamos que C tiene $1 + \frac{1}{2}(d-1)(d-2) = \frac{d^2-3d+4}{2}$ puntos singulares. Como $\mathbb{P}_{d-2}$

tiene dimensión $\binom{d}{2} - 1 = \frac{d^2-d-2}{2}$ podemos siempre encontrar una curva D de grado $d-2$ que pase por los $\frac{d^2-3d+4}{2}$ puntos singulares y otros $\frac{d^2-d-2}{2} - \frac{d^2-3d+4}{2} = d-3$ puntos de C. Como la multiplicidad de intersección de C y D en los puntos singulares de C es al menos dos, obtenemos, contando multiplicidades, al menos $(d^2-3d+4)+(d-3) = d^2-2d+1 = d(d-2)+1$ puntos de intersección entre C y D. Como C es irreducible, esto contradice el Teorema de Bézout.

Supongamos ahora que C tiene exactamente $\frac{1}{2}(d-1)(d-2) = \frac{d^2-3d+2}{2}$ puntos singulares. Con el mismo razonamiento anterior, el sistema lineal Λ de curvas de grado $d-2$ que pasan por los $\frac{d^2-3d+2}{2}$ puntos singulares y otros $d-3$ puntos de C tiene dimensión por lo menos $\frac{d^2-d-2}{2} - \frac{d^2-3d+2}{2} - (d-3) = 1$, y el número de puntos de intersección entre C y cualquiera de esas curvas es por lo menos $(d^2-3d+2)+(d-3) = d(d-2)-1$. Tomando entonces dos puntos más $a, a' \in C$, una curva de Λ que pase por a, a' cortaría a C por lo menos en $d(d-2)+1$ puntos contados con multiplicidad, lo que es absurdo. Por tanto no existen curvas de Λ que pasen por a, a', luego el Lema 3.10 implica que Λ es un haz de curvas, y podemos definir una parametrización $\Lambda \to C$ que asocia a cada curva D en Λ el punto que queda al quitar de $C \cap D$ los $d(d-2)-1$ puntos fijos. □

Como vimos en el Ejemplo 4.12, una parametrización restringida a una curva afín se obtiene ya a partir de cocientes de polinomios en $k[T]$, que es lo que se llama funciones racionales. Es por esto que se suele dar la siguiente:

Definición. Una *curva racional* es una curva de género cero (es decir, una curva parametrizable).

Observación 9.4. Es claro que la hipótesis de que la curva sea irreducible es fundamental en el Teorema 9.3. Por ejemplo, un par de rectas tiene un punto singular (y de hecho una recta doble tiene todos los puntos singulares), o una cúbica formada por la unión de una recta y una cónica irreducible tiene dos puntos singulares (si la recta no es tangente a la cónica). De hecho, la unión de d rectas en "posición general" es una curva de grado d con $\binom{d}{2} = \frac{1}{2}d(d-1)$ puntos singulares (los puntos de intersección de dos de las rectas).

Veamos un ejemplo no trivial de parametrización, usando el Teorema 9.3 (y su demostración, que es constructiva):

Ejemplo 9.5. Consideramos la cuártica de ecuación $F := X_0^2X_1^2 + X_0^2X_2^2 - 2X_1^2X_2^2$. Esta ecuación es irreducible aplicando el criterio de Eisenstein (ver Teorema 2.16(ii)) viendo F como polinomio en la indeterminada X_0, y tomando como elemento irreducible $p = X_1 + iX_2$. Claramente los puntos $(1:0:0), (0:1:0), (0:0:1)$ son singulares (y no puede haber más por el Teorema 9.3). Consideramos el punto $(1:1:1)$, que también pertenece a la curva. El haz de cónicas que pasan por $(1:0:0), (0:1:0), (0:0:1), (1:1:1)$ consiste

en las cónicas de ecuación $G := t_0X_2(X_0 - X_1) + t_1X_1(X_0 - X_2)$. Usando la resultante de F y G respecto de X_2, obtenemos

$$X_0^2X_1^2(X_0 - X_1)(t_0^2X_0 + t_1^2X_0 - t_0^2X_1 - 2t_0t_1X_1 + t_1^2X_1).$$

Las primeras soluciones corresponden a $(1 : 0 : 0), (0 : 1 : 0), (1 : 1 : 1)$ (no sale el punto $(0 : 0 : 1)$ por haber hecho la resultante respecto de X_2), mientras que la última solución

$$(X_0 : X_1) = (t_0^2 + 2t_0t_1 - t_1^2 : t_0^2 + t_1^2)$$

corresponde al restante punto de intersección. Para calcular la última coordenada podemos tomar otra resultante, esta vez respecto de X_1, y obtenemos

$$X_0^2X_2^2(X_0 - X_2)(t_0^2X_0 + t_1^2X_0 + t_0^2X_2 - 2t_0t_1X_2 - t_1^2X_2)$$

que ahora nos da como solución

$$(X_0 : X_2) = (-t_0^2 + 2t_0t_1 + t_1^2 : t_0^2 + t_1^2).$$

Poniendo juntas ambas soluciones tenemos que el punto que obtenemos es

$$\big((t_0^2 + 2t_0t_1 - t_1^2)(-t_0^2 + 2t_0t_1 + t_1^2) : (t_0^2 + t_1^2)(-t_0^2 + 2t_0t_1 + t_1^2) : (t_0^2 + t_1^2)(t_0^2 + 2t_0t_1 - t_1^2)\big)$$

que nos da la parametrización buscada.

Observación 9.6. Volvamos ahora a la topología, y consideremos una cúbica irreducible C. Por el Ejemplo 7.10, tenemos tres casos:

–Si C es lisa, entonces el Teorema 9.2 nos dice que su género es uno (tales curvas se llaman *elípticas*), es decir, es homeomorfa a un toro. Si pinchamos un toro por un punto y desde ahí recortamos un meridiano y un paralelo, podemos ver un toro como un rectángulo en el que identificamos lados paralelos. Otra forma de verlo es ir repitiendo los rectángulos, pegándolos uno junto a otro hasta embaldosar con ellos todo el plano. Esto es lo mismo que ver el toro como el cociente de $\mathbb{R}^2$ por $\mathbb{Z}^2$, que tiene estructura de grupo abeliano. Eso sí, esta estructura no es única, ya que el elemento neutro es precisamente el punto por el que hemos pinchado, así que parece que lo hemos podido escoger.

–Si C es una cúbica cuspidal, entonces tiene género cero, y está en biyección con $\mathbb{P}^1_k$ (para esto no hace falta suponer que $k = \mathbb{C}$), y si a C le quitamos el punto singular entonces está en biyección con $\mathbb{P}^1_k$ menos un punto, que es la recta afín $\mathbb{A}^1_k$. La recta afín está en biyección con la recta vectorial subyacente una vez fijado un origen de la recta, y entonces, con la suma del espacio vectorial, volvemos a encontrar una estructura de grupo abeliano.

–Si C es una cúbica nodal, entonces tiene de nuevo género cero, y ahora es parametrizable pero de modo que dos puntos distintos de $\mathbb{P}^1_k$ van a parar al nodo. En este caso, tendremos que el conjunto de puntos lisos de C está en biyección con $\mathbb{P}^1_k$ menos dos puntos. A su vez, este conjunto está en biyección con $k \setminus \{0\}$ (que ahora con el producto tiene estructura de grupo abeliano) una vez que hayamos escogido un punto unitario $(1:1)$ en $\mathbb{P}^1_k$ y de forma que los dos puntos que hemos quitado son $(0:1)$ y $(1:0)$.

En cualquiera de los casos, parece que el conjunto de puntos lisos de una cúbica irreducible tenga de forma bastante natural (una vez escogido un elemento que hará de neutro) una estructura de grupo. Una primera tentación natural de definir una operación en una cúbica C sería la siguiente: dados dos puntos $a, b \in C$, se le puede asociar de forma natural un tercer punto, considerando el tercer punto de intersección de la recta ab con C. Aunque no haremos los detalles, esto vale también en los casos límite. Por ejemplo, si $a = b$, entonces habría que considerar la recta tangente a C en a y considerar el otro punto de intersección de dicha recta con C (en a tenemos que la multiplicidad de intersección ya es dos, y podría ser incluso tres, en cuyo caso el tercer punto volvería a ser a). Los puntos singulares sí que dan problemas. Por ejemplo, si C tiene un nodo, en ese punto en realidad habría dos ramas, y no se puede decir cómo sumar una rama con la otra (o sumar el punto con él mismo, si decidimos no separar el punto en dos). Sin embargo, es claro que la recta que une dos puntos de una cúbica no puede pasar además por un punto singular, luego el tercer punto de una recta generada por dos puntos lisos es siempre un punto liso. Restringiremos por tanto nuestra operación a los puntos lisos de C, y demos las definiciones precisas (omitiendo los casos límite):

Definición. Dada una cúbica irreducible $C \subset \mathbb{P}^2_k$ y C_0 su conjunto de puntos lisos, definimos la operación $* : C_0 \times C_0 \to C_0$ que asocia a cada par de puntos $a, b \in C_0$ el punto $a * b \in C_0$ de la recta ab distinto de a y b. Se podría decir con más precisión diciendo que $a * b$ es el único punto tal que existe una recta que corta a C en $a, b, a * b$, cada punto con multiplicidad igual a tantas veces como lo hemos repetido.

Observación 9.7. De la definición de $*$ se sigue que $a * b = c$ es equivalente también a $b = a * c$ o a $a = b * c$. Por tanto, si $a * b = a' * b$, se seguirá que $a = a'$.

Claramente la operación es conmutativa, pero es evidente que no tiene elemento neutro. De hecho, si queremos dar estructura de grupo, el neutro lo debemos fijar a priori (como ya hemos observado en los distintos tipos de cúbica) y dar una definición algo más complicada:

Definición. Dada una cúbica irreducible $C \subset \mathbb{P}^2_k$, su lugar liso C_0 y un punto $o \in C_0$, definimos la operación $+ : C_0 \times C_0 \to C_0$ que asocia a cada par de puntos $a, b \in C_0$ el punto $a + b := o * (a * b) \in C_0$.

Teorema 9.8. *Dada una cúbica irreducible $C \subset \mathbb{P}^2_k$ y un punto $o \in C_0$, la operación $+$ apenas definida da a C_0 una estructura de grupo abeliano en que o es el elemento neutro.*

Demostración: La conmutatividad de $*$ implica inmediatamente la conmutatividad de $+$. Además, es evidente que, para cualquier $a \in C_0$, $a + o$ es, por definición el tercer punto de C en la recta generada por o y $a * o$. Como por definición $a * o$ está alineado con a y o, ese tercer punto es necesariamente a. Por tanto, $a + o = a$ para cualquier $a \in C_0$, luego en efecto o es el elemento neutro de la suma.

Para la existencia de inverso de cualquier $a \in C_0$, buscamos un elemento $a' \in C_0$ tal que $a + a' = o$, es decir, $(a * a') * o = o$. Por la Observación 9.7, esto es equivalente a $a * a' = o * o$. Luego, llamando $o' = o * o$, la condición $a * a' = o'$ es equivalente, de nuevo por la Observación 9.7, a $a' = a * o'$. Tendremos entonces que $a' = a * o'$ es el opuesto de a.

Finalmente, para ver la asociatividad, tomamos tres puntos $a, b, c \in C_0$, y bastará ver $(a + b) * c = a * (b + c)$. Consideramos la cúbica D unión de las rectas generadas por a, b; $c, a + b$ y $o, b * c$, que corta a C además en los puntos $a * b, (a + b) * c, b + c$. Consideramos también la cúbica D' unión de las rectas generadas por b, c; $a, b + c$ y $o, a * b$, que corta además a C en $b * c, a * (b + c), a + b$. Por tanto, D' pasa por ocho de los nueve puntos de intersección de C y D, luego por el Corolario 3.15$^{(*)}$ debe pasar también por $(a + b) * c$. Eso quiere decir que $(a + b) * c = a * (b + c)$, como queríamos. □

En la demostración de la existencia de opuesto aparece un punto extra o'. Puede ser natural evitarse tal punto haciendo que coincida con o. Esto es equivalente a decir que o es un punto de inflexión. En tal caso, tenemos la siguiente buena propiedad:

Teorema 9.9. *Sea C una cúbica irreducible, y sea $+$ la suma en el que el neutro es un punto de inflexión o. Entonces tres puntos $a, b, c \in C_0$ están alineados si y sólo si $a + b + c = o$.*

Demostración: Decir que a, b, c estén alineados es lo mismo que decir $a * b = c$, o equivalentemente $a + b = o * c$. Según la demostración del Teorema 9.8 y teniendo en cuenta que $o' = o$ por ser o un punto de inflexión, $o * c$ es el opuesto de c, luego $a + b = o * c$ es equivalente a decir $a + b + c = o$, como queríamos. □

$^{(*)}$ En realidad, en el Corolario 3.15, los nueve puntos eran distintos todos entre sí, mientras que en nuestro caso puede haber repeticiones; el resultado sigue siendo cierto para puntos repetidos (es un teorema de Chasles), pero eso ya no lo demostraremos. De todas formas, la asociatividad puede demostrarse dando la fórmula precisa de la suma (basta darla para las formas canónicas de los Teoremas 7.15, 7.16 y 8.18)

Teorema 9.10. *Sea C una cúbica irreducible y sean $a, b \in C$ puntos de inflexión de C. Entonces $a * b$ es también un punto de inflexión de C.*

Demostración: Si tomamos una suma en C_0 en que el neutro sea un punto de inflexión o, entonces se tendrá, por el Teorema 9.9, que un punto $c \in C_0$ es de inflexión si y sólo si $c + c + c = o$. Por tanto, como tenemos a, b de inflexión será $a + a + a = o$ y $b + b + b = o$. También, como $a, b, a * b$ están alineados, será $a + b + (a * b) = o$. Sumando tres veces, tendremos

$$(a + a + a) + (b + b + b) + (a * b + a * b + a * b) = o + o + o.$$

Como $a + a + a = o$, $b + b + b = o$ y $o + o + o = o$, se sigue $a * b + a * b + a * b = o$, luego $a * b$ también es un punto de inflexión. □

Observación 9.11. Particularicemos ahora todo lo que hemos visto a los distintos tipos de cúbica. Fijamos para ello una suma en que el neutro o es un punto de inflexión, y sabemos que entonces los puntos de inflexión son aquellos puntos a tales que $a+a+a = o$, es decir, los puntos de torsión de orden tres. Vimos en la Observación 9.6 de dónde debería venir la estructura de grupo, luego podíamos haber anticipado cuántos elementos de torsión de orden tres hay en cada caso:

–Si C es la cúbica cuspidal, entonces la estructura de grupo es la aditiva de k, cuyo único punto de torsión (de cualquier orden) es el neutro. Esto coincide con el hecho de que C tiene un único punto de inflexión, con lo que el Teorema 9.10 no dice nada.

–Si C es la cúbica nodal, la estructura de grupo es la multiplicativa de $k \setminus \{0\}$, cuyos elementos de torsión de orden tres son las tres raíces cúbicas de la unidad. En efecto, C tiene tres puntos de inflexión, y el Teorema 9.10 dice que están alineados.

–Si C es una cúbica lisa, su estructura de grupo es la de $\mathbb{R}^2/\mathbb{Z}^2$, y los puntos de torsión de orden tres son las clases de $(0,0), (\frac{1}{3}, 0), (\frac{2}{3}, 0), (0, \frac{1}{3}), (\frac{1}{3}, \frac{1}{3}), (\frac{2}{3}, \frac{1}{3}), (0, \frac{2}{3}), (\frac{1}{3}, \frac{2}{3}), (\frac{2}{3}, \frac{2}{3})$, es decir, nueve puntos, que coincide con el número de puntos de inflexión. El hecho de que esos nueve puntos tengan una configuración tan especial como dice el Teorema 9.10 (dados dos cualesquiera de ellos hay un tercero que está alineado con ellos) implica que como mucho hay tres puntos de inflexión reales, todos ellos alineados. Aunque no sea una demostración, el lector puede convencerse de ello intentando dibujar nueve puntos en el plano con tal propiedad: ya verá que es imposible.

Observación 9.12. Para la cúbica lisa, usando de nuevo la estructura de grupo de $\mathbb{R}^2/\mathbb{Z}^2$, se obtiene que el número de puntos de torsión de orden n es n^2. Por ejemplo, hay cuatro puntos de torsión de orden dos. Un punto b es de torsión de orden dos si y sólo si $b + b = o$, es decir, $b + b + o = o$, lo que quiere decir, por el Teorema 9.9, que o está

en la recta tangente a C en b. Como vimos en el Lema 8.17, hay efectivamente cuatro de esos puntos: el punto o y otros tres puntos b_1, b_2, b_3 cuya tangente pasa por o. Podemos redemostrar ahora el hecho (ver Observación 8.19) de que b_1, b_2, b_3 están alineados. En efecto, si llamamos $b_3' = b_1 + b_2$, es claro que b_3' es otro punto de torsión dos y que no es ni b_1 ni b_2. Tampoco puede ser $b_3' = o$, ya que entonces $b_1 = -b_2 = b_2$. Por tanto, $b_1 + b_2 = b_3 = -b_3$, y el Teorema 9.9 implica que b_1, b_2, b_3 están alineados.

Observación 9.13. El Teorema 9.9 puede generalizarse, en el sentido de que, si $+$ es la suma en una cúbica lisa C en que el neutro o es un punto de inflexión, entonces $a_1 + \ldots + a_{3n} = o$ si y sólo si existe una curva de grado n que corta a C precisamente en $a_1, \ldots, a_{3n}$ (donde cada punto aparece repetido tantas veces como su multiplicidad de intersección). Para demostrarlo (que dejamos como ejercicio), hace falta una generalización del Teorema de Chasles. Más concretamente, se puede demostrar que, dada una curva D de grado n, otra curva de grado n que pase por $3n - 1$ de los puntos de intersección de C y D pasa necesariamente por el restante punto de intersección. Esto es un caso particular del Teorema de Cayley-Bacharach que afirma que, dadas dos curvas C y D sin factores comunes y de grados respectivos d y e, con C irreducible, se satisface que cualquier curva de grado $d+e-3$ que pase por $de-1$ de los puntos de intersección de C y D pasa también por el punto restante (para $d = e = 3$, esto es el Corolario 3.15).

10. Geometría de dimensión superior

A lo largo de estas notas hemos estudiado curvas algebraicas planas, es decir, subconjuntos del plano afín o proyectivo definidos por una única ecuación. En esta última sección, daremos una mínima introducción a la geometría algebraica, que consiste en el estudio de variedades algebraicas, i.e. definidas por un número arbitrario de polinomios en espacios afines o proyectivos de cualquier dimensión. Empezamos con la definición precisa:

Definición. Se llama *conjunto afín* a un subconjunto de $\mathbb{A}_k^n$ definido por los ceros de un ciertos polinomios de $k[X_1, \ldots, X_n]$. En otras palabras, dado cualquier subconjunto $S \subset k[X_1, \ldots, X_n]$, define el conjunto afín

$$V(S) = \{a \in \mathbb{A}_k^n \mid f(a) = 0 \text{ para todo } f \in S\}.$$

De la misma forma, para el caso proyectivo tenemos:

Definición. Se llama *conjunto proyectivo* a un subconjunto de $\mathbb{P}_k^n$ definido por los ceros de un ciertos polinomios homogéneos de $k[X_0, \ldots, X_n]$. En otras palabras, dado cualquier subconjunto $S \subset k[X_0, \ldots, X_n]$ de polinomios homogéneos, define el conjunto proyectivo

$$V(S) = \{a \in \mathbb{P}_k^n \mid F(a) = 0 \text{ para todo } F \in S\}.$$

Ya vimos en el Ejemplo 3.6 cómo de forma natural aparecían conjuntos proyectivos, en concreto dentro del espacio proyectivo $\mathbb{P}_d$ que parametriza las curvas de grado d de $\mathbb{P}_k^2$. Vamos a estudiar algún ejemplo más representativo:

Ejemplo 10.1. Podemos generalizar lo visto en la sección 4, en el sentido de que cualquier curva parametrizada se puede expresar en ecuaciones implícitas. Por ejemplo, consideremos el conjunto

$$C := \{(t_0^3 : t_0^2 t_1 : t_0 t_1^2 : t_1^3) \in \mathbb{P}_k^3 \mid (t_0 : t_1) \in \mathbb{P}_k^1\}.$$

Claramente, los puntos de C satisfacen las ecuaciones

$$S := \{X_0X_2 - X_1^2 \ , \ X_0X_3 - X_1X_2 \ , \ X_1X_3 - X_2^2\}.$$

Recíprocamente, supongamos que un punto $a = (a_0 : a_1 : a_2 : a_3) \in \mathbb{P}_k^3$ satisface esas tres ecuaciones. Si fuera $a_0 = 0$, entonces de $a_0a_2 - a_1^2 = 0$ deduciríamos $a_1 = 0$, y entonces de $a_1a_3 - a_2^2 = 0$ se concluye $a_2 = 0$. Por tanto, $a = (0 : 0 : 0 : 1)$, y por tanto está en C tomando $(t_0 : t_1) = (0 : 1)$. Si, por el contrario, $a_0 \neq 0$, llamamos $t := \frac{a_1}{a_0}$, y se tendrá, usando las ecuaciones que satisface a:

$$t^2 = \frac{a_1^2}{a_0^2} = \frac{a_0a_2}{a_0^2} = \frac{a_2}{a_0}$$

$$t^3 = tt^2 = \frac{a_1}{a_0}\frac{a_2}{a_0} = \frac{a_1a_2}{a_0^2} = \frac{a_0a_3}{a_0^2} = \frac{a_3}{a_0}$$

y por tanto

$$a = (1 : \frac{a_1}{a_0} : \frac{a_2}{a_0} : \frac{a_3}{a_0}) = (1 : t : t^2 : t^3)$$

lo que implica que a están en C, tomando $(t_0 : t_1) = (1 : t)$. Hemos demostrado, por tanto, $C = V(S)$, luego es un conjunto proyectivo. Es natural decir que C es una curva, es decir, que tiene dimensión uno (esta curva se llama *cúbica alabeada*). Además, su grado debe ser tres, ya que si cortamos con un plano $V(u_0X_0 + u_1X_1 + u_2X_2 + u_3X_3)$, obtendremos los puntos $(t_0^3 : t_0^2t_1 : t_0t_1^2 : t_1^3)$ en los que $(t_0 : t_1)$ es una raíz de $u_0T_0^3+u_1T_0^2T_1+u_2T_0T_1^2+u_3T_1^3$, que tiene tres raíces contadas con multiplicidad; por tanto, la intersección de C con un plano son tres puntos contados con multiplicidad.

Ejercicio 10.2. Generalizar el ejercicio anterior demostrando que

$$C = \{(t_0^n : t_0^{n-1}t_1 : \ldots : t_0t_1^{n-1} : t_1^n) \in \mathbb{P}_k^n \mid (t_0 : t_1) \in \mathbb{P}_k^1\}$$

es un conjunto proyectivo, y que un conjunto de ecuaciones viene dado por los menores de orden dos de la matriz

$$\begin{pmatrix} X_0 & X_1 & \ldots & X_{n-2} & X_{n-1} \\ X_1 & X_2 & \ldots & X_{n-1} & X_n \end{pmatrix}$$

(tal conjunto proyectivo se llama *curva racional normal de grado* n).

La pregunta clave es: ¿cómo se puede deducir en general cuáles deberían ser la dimensión y el grado de un conjunto proyectivo mirando sólo al conjunto S de ecuaciones que lo definen? Porque desde luego, en el Ejemplo 10.1 uno se esperaría que tres ecuaciones "independientes" (en un sentido que habría que precisar) definieran algo de codimensión tres, mientras que hemos observado que se obtiene una curva, que sólo tiene codimensión dos. Más complicado aún parece la cuestión de determinar el grado: ¿cómo es posible que tres ecuaciones de grado dos den lugar a algo de grado tres? En realidad, lo primero que habría que pensar es si hemos escogido las ecuaciones adecuadas. De hecho, en el caso de curvas planas, teníamos para cada curva una ecuación minimal (única salvo multiplicación por contante). El resultado clave es el Corolario 2.13 (o 2.12 en el caso afín), en el que se dice que los polinomios que se anulan en una curva son precisamente los múltiplos de su ecuación minimal. En otras palabras, en el caso afín, los polinomios que se anulan en una curva forman un ideal, y una ecuación minimal no es sino un generador de tal ideal. Esto nos lleva a lo siguiente:

Definición. Se llama *ideal de un conjunto afín* $X \subset \mathbb{A}_k^n$ a

$$I(X) = \{f \in k[X_1, \ldots, X_n] \mid f(a) = 0 \text{ para todo } a \in X\}.$$

En el caso proyectivo, en que sólo las ecuaciones homogéneas tienen sentido, la definición hay que cambiarla ligeramente:

Definición. Se llama *ideal de un conjunto proyectivo* $X \subset \mathbb{P}_k^n$ a

$$I(X) = \text{ideal generado por } \{F \in k[X_0, \ldots, X_n] \mid F(a) = 0 \text{ para todo } a \in X\}.$$

El resultado clave ahora es:

Teorema 10.3 (de la base de Hilbert)**.** *Todo ideal de un anillo de polinomios admite un número finito de generadores.*

A raíz de este resultado (que no demostraremos), se concluye que todo conjunto algebraico (afín o proyectivo) puede determinarse por un número finito de ecuaciones (en el caso proyectivo no es difícil ver que los generadores finitos de $I(X)$ pueden tomarse homogéneos). Sin embargo, esto no resuelve nuestro problema. Se puede demostrar que el conjunto S del Ejemplo 10.1 genera $I(C)$ (más en general, lo mismo es cierto para la curva racional normal del Ejercicio 10.2). Además, no es excesivamente difícil demostrar (el lector puede intentar demostrarlo como desafío) que $I(C)$ no puede generarse por dos elementos, con lo que seguimos con el mismo problema de saber cómo calcular dimensión y grado a partir de las ecuaciones.

Un problema añadido es el siguiente: si esperamos obtener la información de un conjunto algebraico X a partir de $I(X)$, ¿cómo determinar cuál es este ideal y sus generadores? En el caso de curvas planas, de nuevo la clave es el Corolario 2.12 o 2.13 (según estemos en el caso afín o proyectivo): dada una curva definida por un polinomio, el ideal de la curva son los polinomios tales que una potencia suya esté en el ideal generado por el polinomio dado. Además, el ideal de la curva está generado por un polinomio que consiste en quitar los factores repetidos del polinomio de partida. Sin embargo, volviendo al Ejemplo 10.1, sabemos que C está definida por los tres polinomios de S, pero ¿cómo calcular a partir de ellos $I(C)$? (ya hemos dicho antes que puede demostrarse que en este caso se da la "casualidad" de que el ideal generado por los elementos de S es precisamente $I(C)$). La respuesta general a esta pregunta viene dada por la generalización de los Corolarios 2.12 y 2.13, para lo que necesitaremos primero recordar una definición de Álgebra:

Definición. Se llama *radical de un ideal* I de un anillo A a:

$$\sqrt{I} = \{f \in A \mid f^r \in I \text{ para algún } r \in \mathbb{N}\}$$

(es un simple ejercicio comprobar que $\sqrt{I}$ es un ideal de A). Un *ideal radical* es un ideal I tal que $\sqrt{I} = I$.

Teorema 10.4 (de los ceros de Hilbert[(*)])**.** *Sea k un cuerpo algebraicamente cerrado, sea $S \subset k[X_1, \ldots, X_n]$ y sea $X = V(S) \subset \mathbb{A}^n_k$. Entonces, si I es el ideal generado por S en $k[X_1, \ldots, X_n]$, se tiene $I(X) = \sqrt{I}$.*

En el caso proyectivo hay que tener una pequeña precaución con el conjunto vacío, debido a que se puede obtener de dos formas distintas:

Teorema 10.5 (de los ceros proyectivo)**.** *Sea k un cuerpo algebraicamente cerrado, sea $S \subset k[X_0, \ldots, X_n]$ un subconjunto de polinomios homogéneos, sea I el ideal generado por S en $k[X_0, \ldots, X_n]$ y sea $X = V(S) \subset \mathbb{P}^n_k$. Entonces:*

(i) $X = \emptyset$ si y sólo si existe $d_0 \in \mathbb{N}$ tal que I contiene todos los polinomios homogéneos de grado $d \geq d_0$ (que es lo mismo que decir que $\sqrt{I}$ contiene a $X_0, \ldots, X_n$).

(ii) Si $X \neq \emptyset$, se tiene $I(X) = \sqrt{I}$.

El Teorema de los Ceros nos da una biyección entre conjuntos algebraicos e ideales radicales (en el caso proyectivo hay que tener la precaución de que el conjunto vacío puede corresponder a dos ideales radicales, el total y el generado por $X_0, \ldots, X_n$). Esto es la generalización de lo que vimos para curvas planas de que hay una biyección entre el conjunto de curvas planas y el conjunto de ecuaciones minimales, salvo multiplicación por constante no nula. De hecho dos polinomios generan el mismo ideal si y sólo si difieren en la multiplicación por una constante no nula; y el ideal generado por un polinomio es radical si y sólo si el polinomio es una ecuación minimal (es decir, no tiene factores múltiples). Recordemos que, a la hora de hablar de sistemas lineales, tuvimos que considerar también ecuaciones no minimales (y por tanto ideales no radicales), a fin de que el conjunto de curvas de un mismo grado forme un espacio proyectivo. De este modo, también eran curvas objetos como rectas dobles, por ejemplo. En el caso de conjuntos algebraicos generales, también deberemos considerar a veces objetos más generales (llamados *esquemas*) que, esencialmente, consiste en considerar ideales que no son radicales. Esto también permite que los conjuntos que parametrizan variedades algebraicas del mismo tipo sean más "completas", como ya vimos en la sección 3, en que, permitiendo curvas no reducidas, el conjunto de curvas de grado d formaba todo un especio proyectivo, y no sólo una parte.

Ejemplo 10.6. Retomemos el Ejemplo 10.1 de la cúbica alabeada.

$$C = \{(t_0^3 : t_0^2 t_1 : t_0 t_1^2 : t_1^3) \in \mathbb{P}^3_k \mid (t_0 : t_1) \in \mathbb{P}^1_k\}.$$

Dijimos que un plano corta a C en tres puntos contados con multiplicidad. Si queremos que nos aparezca multiplicidad mayor que uno, podemos cortar con el plano $V(X_3)$, que

(*) Conviene indicar que el nombre original en alemán del teorema es Nullstellensatz, ya que en los textos en inglés no está traducido, y hay que buscarlo por ese nombre

nos da la raíz $t_1 = 0$ triple, es decir, que obtendremos el punto $(1:0:0:0)$ contado tres veces. Como las ecuaciones de C eran

$$S = \{X_0X_2 - X_1^2\ ,\ X_0X_3 - X_1X_2\ ,\ X_1X_3 - X_2^2\}$$

las ecuaciones del punto triple serán

$$S' := \{X_0X_2 - X_1^2\ ,\ X_0X_3 - X_1X_2\ ,\ X_1X_3 - X_2^2,\ X_3\}$$

o, equivalentemente

$$S'' := \{X_0X_2 - X_1^2\ ,\ X_1X_2\ ,\ X_2^2,\ X_3\}.$$

Por tanto, el ideal I generado por S'' representará al punto $(1:0:0:0)$ con multiplicidad tres. Obsérvese que no es un ideal radical, ya que $X_2^2 \in I$ (es decir, $X_2 \in \sqrt{I}$), pero $X_2 \notin I$. Podemos identificar el plano $V(X_3)$ con el plano proyectivo $\mathbb{P}_k^2$ de coordenadas X_0, X_1, X_2, luego del mismo modo se ve que el ideal generado por $X_0X_2 - X_1^2\ ,\ X_1X_2\ ,\ X_2^2$ define el punto $(1:0:0)$ con multiplicidad tres. Si en lugar de ver esas ecuaciones en $\mathbb{P}_k^2$ las vemos en k^3 (que identificaremos con $\mathbb{A}_k^3$, y usaremos coordenadas X, Y, Z en lugar de X_0, X_1, X_2), podemos decir que el ideal generado por $XZ - Y^2, YZ, Z^2$ representa a la recta $V(Y, Z)$ con multiplicidad tres. Podemos ver esto como la generalización de la noción de recta doble. Tenemos ahora un esquema en $\mathbb{A}_k^3$ que define una recta triple.

En realidad, a efectos prácticos, el Teorema de los Ceros no ayuda mucho, ya que no es tarea fácil (salvo para programas especializados de ordenador) calcular el radical de un ideal. Evitaremos pues los métodos algebraicos de cálculo de dimensión y grado a partir del ideal, y nos centraremos en su descripción geométrica. La idea es el Corolario 8.8(ii), que indica que una curva corta a una recta general en un número d de puntos distintos, y este número d es precisamente el grado. Nos basaremos en esta idea, aunque de momento sea imprecisa:

Definición. Se llama *dimensión* de un conjunto algebraico X a $r \in \mathbb{N}$ tal que un subespacio lineal "general" de codimensión r corte a X en un número finito de puntos. El número de tales puntos se llama *grado* de X.

Obsérvese que esta definición, aparte de coincidir con la que tenemos en el caso de curvas planas, hace que en el Ejemplo 10.1 el conjunto C tenga dimensión uno y grado tres, ya que cualquier plano $V(u_0X_0 + u_1x_1 + u_2X_2 + u3X_3) \subset \mathbb{P}_k^3$ corta a C en tres puntos (que serán distintos si el discriminante de $u_0T_0 + u_1T_1 + u_2T_2 + u_3T_3$ es distinto de cero). Del mismo modo, la curva racional normal del Ejercicio 10.2 es, en efecto, una curva y tiene grado n.

Para que la definición anterior sea precisa, necesitamos decir qué entendemos por subespacio lineal "general". En el caso de curvas proyectivas, el subespacio es un hiperplano de $\mathbb{P}^n$, así que, generalizando la situación del Corolario 8.8(ii), un hiperplano general será un elemento de $\mathbb{P}_k^{n\,*}$ que esté fuera de un conjunto proyectivo. Para ser precisos en el caso general, necesitaríamos conocer en primer lugar el conjunto de los subespacios lineales de un espacio proyectivo. Para ver cómo podríamos hacer eso, analicemos el caso conocido del espacio dual:

Observación 10.7. Todos sabemos que al espacio dual $\mathbb{P}_k^{n\,*}$ le podemos dar coordenadas $(u_0 : \ldots : u_n)$ representando el hiperplano de ecuación $u_0X_0 + \ldots + u_nX_n$. Hay una forma alternativa de ver estas coordenadas, si el hiperplano lo tenemos descrito como generado por n puntos independientes. En efecto, si un hiperplano está generado por los puntos $a_1, \ldots, a_n$, y escribimos $a_i = (a_{i0} : \ldots : a_{in})$, entonces la ecuación del hiperplano es

$$\begin{vmatrix} X_0 & X_1 & \ldots & X_n \\ a_{10} & a_{11} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n0} & a_{n1} & \ldots & a_{nn} \end{vmatrix}$$

y por tanto los coeficientes del hiperplano son, salvo el orden y el signo, los menores de orden máximo de la matriz

$$A = \begin{pmatrix} a_{10} & a_{11} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n0} & a_{n1} & \ldots & a_{nn} \end{pmatrix}$$

cuyas filas son las coordenadas de los puntos que generan el hiperplano. Evidentemente, si cambiamos los puntos que generan el hiperplano, la ecuación nos tiene que quedar la misma (o un múltiplo). Esto se puede ver de la siguiente forma: Cada punto del hiperplano se obtiene mediante una combinación lineal de las filas de A, es decir, multiplicando A a la izquierda por un vector fila (en el que ponemos los coeficientes de la combinación lineal. Entonces, un nuevo sistema de puntos que generen el hiperplano se obtiene multiplicando A a la izquierda por una matriz invertible P de orden n. Los menores de orden n de la nueva matriz PA serán entonces los menores de orden n de A multiplicados por el determinante de P, que es una constante distinta de cero. Por tanto, los coeficientes de la ecuación del hiperplano son los mismos que antes, pero multiplicados todos por $\det(P)$.

En general, esta idea de tomar los menores de orden máximo de una matriz cuyas filas generan el subespacio sirve para dar coordenadas al conjunto de subespacios lineales de dimensión dada en un espacio proyectivo. Hagamos en detalle el primer caso no trivial:

Ejemplo 10.8. Sea X el conjunto de todas las rectas de $\mathbb{P}^3$. Cada recta L estará generada por las filas de una matriz

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix}.$$

Para cada par de columnas $i, j \in \{0, 1, 2, 3\}$ (tomaremos siempre $i < j$) definimos

$$p_{ij} = \begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix}.$$

Como hemos observado antes, cualquier otro par de puntos que generen la misma recta se podrán escribir como las filas de

$$A' = \begin{pmatrix} a'_0 & a'_1 & a'_2 & a'_3 \\ b'_0 & b'_1 & b'_2 & b'_3 \end{pmatrix} = \begin{pmatrix} \lambda_0 & \lambda_1 \\ \mu_0 & \mu_1 \end{pmatrix} \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix}$$

con $\begin{vmatrix} \lambda_0 & \lambda_1 \\ \mu_0 & \mu_1 \end{vmatrix} = \lambda \neq 0$ (la matriz $\begin{pmatrix} \lambda_0 & \lambda_1 \\ \mu_0 & \mu_1 \end{pmatrix}$ juega el papel de P en la observación anterior). Se tendrá entonces

$$p'_{ij} = \begin{vmatrix} a'_i & a_j \\ b'_i & b_j \end{vmatrix} = \left| \begin{pmatrix} \lambda_0 & \lambda_1 \\ \mu_0 & \mu_1 \end{pmatrix} \begin{pmatrix} a_i & a_j \\ b_i & b_j \end{pmatrix} \right| = \begin{vmatrix} \lambda_0 & \lambda_1 \\ \mu_0 & \mu_1 \end{vmatrix} \begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix} = \lambda p_{ij}.$$

Por tanto, $(p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23})$ y $(p'_{01} : p'_{02} : p'_{03} : p'_{12} : p'_{13} : p'_{23})$ determinan el mismo punto de $\mathbb{P}^5_k$ (como los dos puntos que determinan la recta son distintos, necesariamente algún p_{ij} es no nulo). Tenemos, por tanto, una aplicación

$$g_{1,3} : X \to \mathbb{P}^5_k$$

y nos preguntamos si es inyectiva (es decir, si cada recta queda determinada unívocamente a partir de los p_{ij}) y si es suprayectiva, es decir, si cualquier elección de coordenadas p_{ij} corresponde a una recta de $\mathbb{P}^3_k$. Estudiemos ambas cuestiones al mismo tiempo, es decir, tomemos $(p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23}) \in \mathbb{P}^5_k$ y veamos cuándo corresponde a una recta de $\mathbb{P}^3_k$, y si esa recta es única. Supongamos, por ejemplo, $p_{01} \neq 0$. Esto quiere decir que la matriz $\begin{pmatrix} a_0 & a_1 \\ b_0 & b_1 \end{pmatrix}$ es invertible. Multiplicando A a la izquerda por la inversa de dicha matriz, obtenemos que la recta a la que corresponda $(p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23})$ se puede generar por las filas de una matriz

$$A' = \begin{pmatrix} 1 & 0 & a'_2 & a'_3 \\ 0 & 1 & b'_2 & b'_3 \end{pmatrix}.$$

Tendremos entonces

$$(p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23}) = (1 : b'_2 : b'_3 : -a'_2 : -a'_3 : a'_2 b'_3 - a'_3 b'_2)$$

y por tanto

$$\begin{cases} \dfrac{p_{02}}{p_{01}} = b'_2 \\ \dfrac{p_{03}}{p_{01}} = b'_3 \\ \dfrac{p_{12}}{p_{01}} = -a'_2 \\ \dfrac{p_{13}}{p_{01}} = -a'_3 \\ \dfrac{p_{23}}{p_{01}} = a'_2 b'_3 - a'_3 b'_2 \end{cases}$$

lo que demuestra dos cosas:

–En primer lugar, mirando las cuatro primeras igualdades anteriores, un elemento $(p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23}) \in \mathbb{P}^5_k$ sólo puede provenir de una recta de $\mathbb{P}^3_k$, en concreto la generada por los puntos $(1 : 0 : -\frac{p_{12}}{p_{01}} : -\frac{p_{13}}{p_{01}})$ y $(0 : 1 : \frac{p_{02}}{p_{01}} : \frac{p_{03}}{p_{01}})$.

–En segundo lugar, mirando ahora también la quinta y última igualdad, el elemento $(p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23})$ viene de una recta si y sólo si

$$\frac{p_{23}}{p_{01}} = -\frac{p_{12}}{p_{01}}\frac{p_{03}}{p_{01}} + \frac{p_{13}}{p_{01}}\frac{p_{02}}{p_{01}}$$

es decir

$$p_{01}p_{23} - p_{02}p_{13} + p_{03}p_{12} = 0.$$

Si cambiásemos la hipótesis $p_{01} \neq 0$ por otra coordenada, los puntos que generan la recta cambiarían, pero lo que no cambia es la ecuación que deben satisfacer las coordenadas. Llegamos entonces a que la imagen de $g_{1.3}$ es la cuádrica $V(p_{01}p_{23} - p_{02}p_{13} + p_{03}p_{12})$, llamada *cuádrica de Klein.*

En general, tenemos lo siguiente:

Ejercicio 10.9. Sea $\mathbb{G}(k, n)$ el conjunto de subespacios lineales de dimensión k de $\mathbb{P}^n_k$ (llamado *grassmannina de k-espacios en* $\mathbb{P}^n_k$). Sea $\Lambda \in \mathbb{G}(k, n)$ un subespacio generado por las filas de la matriz

$$A = \begin{pmatrix} a_{00} & a_{01} & \dots & a_{0n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k0} & a_{k1} & \dots & a_{kn} \end{pmatrix}$$

y, para cada elección de $k+1$ columnas $i_0 < i_1 < \ldots < i_k$ (obsérvese que hay $\binom{n+1}{k+1}$ elecciones) sea

$$p_{i_0,\ldots,i_k} = \begin{vmatrix} a_{0,i_0} & \dots & a_{0,i_k} \\ \vdots & \ddots & \vdots \\ a_{k,i_0} & \dots & a_{k,i_k} \end{vmatrix}.$$

Demostrar que la aplicación (llamada *inmersión de Plücker*) $\mathbb{G}(k,n) \to \mathbb{P}_k^{\binom{n+1}{k+1}-1}$ que manda cada subespacio Λ al punto cuyas coordenadas son los $p_{i_0,\ldots,i_k}$ (llamadas *coordenadas de Plücker*) está bien definida, es inyectiva, y tiene como imagen un conjunto proyectivo (esta última parte es complicada, y el lector no debe desmoralizarse si no logra una demostración). Como modo alternativo para obtener ecuaciones de la imagen si $k = 1$, demostrar que un punto está en la imagen de la inmersión de Plücker si y sólo si la matriz

$$\begin{pmatrix} 0 & p_{01} & \cdots & p_{0n} \\ -p_{01} & 0 & \cdots & p_{1n} \\ \vdots & & \ddots & \vdots \\ -p_{0n} & -p_{1n} & \cdots & 0 \end{pmatrix}$$

tiene rango dos, en cuyo caso la recta correspondiente de $\mathbb{P}_k^n$ es la generada por las filas de la matriz (este hecho ya lo hemos encontrado, para $n = 2$, en la demostración del Teorema 8.1).

Con todo lo anterior, ya podemos precisar la definición de dimensión y grado, basada en la siguiente generalización del Corolario 8.8(ii):

Teorema 10.10. *Sea $X \subset \mathbb{P}_k^n$ un conjunto proyectivo. Entonces, existen números naturales r y d y un conjunto proyectivo $Z \subsetneq \mathbb{G}(n-r,n) \subset \mathbb{P}^{\binom{n+1}{n-r+1}-1}$ (i.e. Z es un subconjunto propio del conjunto del conjunto de todos los subespacios de codimensión r en $\mathbb{P}_k^n$) tal que, si $\Lambda \in \mathbb{G}(n-r,n) \setminus Z$, entonces la intersección de X y Λ consiste exactamente en d puntos distintos.*

Aunque esta definición está enunciada sólo para conjuntos proyectivos, puede hacerse también para conjuntos afines, sin más que tomar su *completado proyectivo*. No entraremos en detalles (la construcción del completado proyectivo requiere alguna sutileza), más que nada porque, como el caso de curvas tendría que haber demostrado ya a estas alturas, la geometría que funciona bien es la proyectiva sobre un cuerpo algebraicamente cerrado. A este caso nos ceñiremos sobre todo.

Ejemplo 10.11. Si consideramos en $\mathbb{P}_k^2$ el conjunto X definido por las ecuaciones X_0X_2, X_1X_2, nos damos cuenta de que obtenemos la unión de la recta $V(X_2)$ y el punto $(0:0:1)$. Obsérvese que cualquier recta $V(u_0X_0 + u_1X_1 + u_2X_2)$ distinta de $V(X_2)$ (i.e. u_0, u_1 no se anulan los dos) y que no pase por $(0:0:1)$ (i.e. $u_2 \neq 0$) corta a X en un solo punto. Por tanto, en el Teorema 10.10 podemos tomar, por ejemplo, $Z = V(U_0U_2)$, y llegamos a que X tiene dimensión uno y grado uno. Nótese que, en cambio, una recta que pase por $(0:0:1)$ corta a X en dos puntos. Esto indica que tanto la dimensión como el grado de una variedad algebraica los determinan las partes "más grandes" de la misma. Esta noción de descomponer en partes es la generalización de las componentes irreducibles que vimos para curvas:

Definición. Un conjunto proyectivo $X \subset \mathbb{P}_k^n$ se dice que es *irreducible* si la única forma de escribir X como $X = X_1 \cup X_2$, con X_1, X_2 conjuntos proyectivos, es tomando $X_1 = X$ o $X_2 = X$. La misma definición vale cambiando la palabra "proyectivo" por "afín".

La generalización de la Proposición 2.14 es ahora:

Ejercicio 10.12. Demostrar que un conjunto algebraico (afín o proyectivo) es irreducible si y sólo si $I(X)$ es un ideal primo.

La descomposición en componentes irreducibles es más complicada, y se basa en la descomposición primaria de cualquier ideal de un anillo de polinomios (o al menos, en la noetherianidad de tales anillos). El motivo esencial de tal dificultad se explica en parte por el hecho de que, para variedades arbitrarias, las componentes irreducibles pueden tener entre ellas distintas dimensiones, como hemos visto en el Ejemplo 10.11.

Observación 10.13. Con estas definiciones, ya podemos estudiar el caso de codimensión uno. Ya vimos en el Ejemplo 10.11 una curva (ya que tiene dimensión uno) que no está definida por una ecuación. Lo que puede demostrarse es que el ideal de un conjunto afín o proyectivo está generado por una sola ecuación si y sólo si todas sus componentes tienen codimensión uno. Un conjunto asíes lo que propiamente hay que llamar hipersuperficie, o, en el caso de dimensión uno, curva.

Veamos ahora hasta qué punto se puede generalizar el estudio local en un punto. En el caso de curvas, aunque el algoritmo es mucho más complicado que en el caso de curvas planas, se puede hablar de ramas en un punto como clases de equivalencia de parametrizaciones formales (que se ve que existen siempre), y por tanto de rectas tangentes. Para dimensión superior, la situación no es tan simple. Estudiemos primero un ejemplo, y tomaremos, como siempre en estos casos, el origen de un conjunto afín:

Ejemplo 10.14. Consideremos $X = V(f) \subset \mathbb{A}_k^3$, con $f = XZ - Y^2 + X^3$, y estudiemos el punto $(0,0,0)$ (el único punto en el que se anulan todas las derivadas parciales de f). Cortemos X con cualquier recta que pase por el origen. Tal recta se podrá parametrizar como $(X,Y,Z) = (at, bt, ct)$, con $(a,b,c) \neq (0,0,0)$. La multiplicidad de intersección de X con la recta en el punto será la multiplicidad de la raíz $T = 0$ del polinomio

$$f(aT, bT, cT) = (ac - b^2)T^2 + a^3T^3$$

es decir, la multiplicidad es siempre al menos dos, y es mayor precisamente para las rectas en que $ac - b^2 = 0$. Llegamos, por tanto, a la misma noción de cono tangente que teníamos para curvas, y de nuevo la ecuación de tal cono es la parte homogénea de grado menor de la ecuación de la hipersuperficie f. Ahora bien, hay serias diferencias con el caso de curvas. En primer lugar, el cono tangente ahora no es la unión de los planos tangentes

a X en $(0,0,0)$. De hecho, bien pensado, X debería tener infinitos planos tangentes en el punto, precisamente los planos tangentes al cono $V(XZ-Y^2)$ (que se puede ver que son límite de planos tangentes a X en los puntos lisos). El cono tangente es, sin embargo, unión de rectas (y no planos) que pasan por $(0,0,0)$. Puede demostrarse que dichas rectas son las rectas tangentes a las distintas curvas contenidas en X que pasan por $(0,0,0)$.

Podemos dar ya la siguiente:

Definición. Dado un conjunto algebraico X y un punto $a \in X$, se llama *cono tangente* de X en a, a la unión de las rectas tangentes en a a las curvas de X que pasan por a.

Tal vez la definición quede más clara con un ejemplo más:

Ejemplo 10.15. Consideremos la curva $C = \{(t^3, t^4, t^5) \in \mathbb{A}^3_k \mid t \in k\}$. Se comprueba sin dificultad que $C = V(Y^2 - XZ, Z^2 - X^2Y, X^3 - YZ)$, y de hecho puede llegar a demostrarse que $I(C)$ está generado por esos tres polinomios. Sin herramientas de cono tangente, sino directamente con la parametrización, está claro que el punto $(0,0,0)$ es triple y con una sola recta tangente, en concreto $V(Y,Z)$, que debería contar tres veces. Efectivamente, si tomamos las partes homogéneas de grado menor de los generadores del ideal, tendríamos que el cono tangente sería $V(Y^2 - XZ, Z^2, YZ)$, que ya vimos en el Ejemplo 10.6 que define esa recta tres veces.

Ejemplo 10.16. Calcular el cono tangente en el origen de la curva $V(X^2Y - X^8, XY^2 + Z^9) \subset \mathbb{A}^3_k$ [La moraleja del ejercicio es que no basta con calcular las partes homogéneas de los generadores del ideal, sino que hay que considerar todo posible polinomio del ideal].

Podemos ya dar las definiciones, aunque no sean muy precisas:

Definición. Se llama *cono tangente a un conjunto algebraico X en un punto $a \in X$* a la unión de las rectas tangentes en a a todas las curvas de X que pasan por a. Se llama *múltiplicidad de un punto de una variedad algebraica* al grado de su cono tangente (que puede contar con multiplicidad, como vimos en el Ejemplo 10.15). Un *punto liso de una variedad algebraica* es un punto para el que el cono tangente tiene grado uno, en cuyo caso se llama *espacio tangente*. Si a es liso en X, denotaremos por $\mathbb{T}_a X$ al espacio tangente a X en a. Se puede demostrar que la dimensión del cono tangente coincide con la dimensión máxima de las componentes de X que pasan por a, y si a es un punto liso entonces X tiene una única componente que pasa por a, de dimensión igual a la de $\mathbb{T}_a X$.

A efectos prácticos, $\mathbb{T}_a X$ es la intersección, cuando F recorre el conjunto de polinomios homogéneos de $I(X)$ (o, en este caso, basta tomar un sistema de generadores), de $V(F_0(a)X_0 + \ldots + F_n(a)X_n)$ (donde, como siempre, F_i indica la derivada parcial de F respecto de X_i). De nuevo, la definición análoga se puede hacer para el caso afín. Cuando a no es liso, tal intersección da un espacio lineal que contiene al cono tangente, y que se llama *espacio tangente de Zariski*.

El teorema más importante que hemos visto en estas notas, el de Bézout, se puede generalizar a conjuntos proyectivos. El Ejemplo 10.11 nos muestra que necesitamos tener cuidado sobre la dimensión de las componentes. Damos aquí un enunciado bastante general atendiendo a estas precauciones:

Teorema 10.17. *Sean $X_1, \ldots, X_s \subset \mathbb{P}_k^n$ conjuntos proyectivos de dimensión pura (i.e. para cada $i = 1, \ldots, s$, cada componente de X_i tiene la misma dimensión r_i). Sea $c_i := n - r_i$ la codimensión de X_i. Entonces:*

(i) Cada componente irreducible de $X_1 \cap \ldots \cap X_s$ tiene codimensión como mucho $c_1 + \ldots + c_s$.

(ii) Si $c_1 + \ldots + c_s = n$ y $X_1 \cap \ldots \cap X_s$ es un número finito de puntos, entonces tal número de puntos es, contando multiplicidades, $\deg(X_1) \cdots \deg(X_s)$.

La noción de multiplicidad de intersección es muy difícil de definir en general (ya lo ha sido para la intersección de dos curvas planas). De hecho, la topología algebraica, y en concreto los grupos de homología fueron introducidos con la finalidad de definir con precisión la noción de multiplicidad de intersección para conjuntos proyectivos complejos (como en la sección 9, considerados como variedades topológicas, y por tanto definiendo ciclos en el espacio proyectivo complejo, visto como espacio topológico ambiente).

El modo de entender el Teorema 10.17 es el siguiente: la codimensión esperada de la intersección de conjuntos proyectivos es la suma de las codimensiones, y cuando eso ocurre entonces se puede "calcular" la intersección. Obsérvese en particular que el ideal de un conjunto proyectivo de codimensión c tiene que estar generado necesariamente por al menos c ecuaciones. Ya en el primer ejemplo que hemos visto (Ejemplo 10.1) el ideal no puede generarse por tantas ecuaciones como la codimensión, salvo en el caso de codimensión uno (ver Ejemplo 10.13). De hecho, es muy especial que el ideal de un conjunto proyectivo esté generado por tantos elementos como la codimensión (un conjunto proyectivo así se llama *intersección completa*). Probablemente la conjetura abierta más importante en geometría proyectiva (debida a Hartshorne) sea que toda variedad proyectiva lisa de dimensión r en $\mathbb{P}_k^n$ es intersección completa si $r > \frac{2}{3}n$.

Finalmente, analicemos brevemente algo que el lector debería haber echado de menos. En cualquier materia matemática merecedora de tal calificativo, después de introducir los objetos con los que se va a trabajar, se introducen los morfismos entre ellos, que son aplicaciones que respetan la estructura (aplicaciones lineales de espacios vectoriales, homomorfismos de grupos o anillos, aplicaciones continuas de espacios topológicos, aplicaciones diferenciables de variedades diferenciables,...). Para variedades algebraicas definidas por polinomios, lo esperable sería definir morfismo como una aplicación polinomial. Sin embargo, no es tan simple como eso:

Ejemplo 10.18. La biyección $\mathbb{P}^1_k \to \mathbb{P}^2_k$ definida por $(t_0 : t_1) \mapsto (t_0^2 : t_0t_1 : t_1^2)$ del Ejercicio 1.7 debería ser un isomomorfismo entre $\mathbb{P}^1$ y $V(X_0X_2 - X_1^2)$. Sin embargo, la única forma de definir su inversa es mediante

$$(a_0 : a_1 : a_2) \mapsto \begin{cases} (a_0 : a_1) \text{ si } (a_0 : a_1 : a_2) \neq (0 : 0 : 1) \\ (a_1 : a_2) \text{ si } (a_0 : a_1 : a_2) \neq (1 : 0 : 0) \end{cases}$$

(obsérvese que $(a_0 : a_1) = (a_1 : a_2)$ en $V(X_0X_2 - X_1^2)$).

Este ejemplo indica que la noción de morfismo debe ser local, en el sentido de que alrededor de cada punto puede definirse mediante polinomios, aunque globalmente no tenga por qué poderse definir por polinomios (aunque puede demostrarse que, a posteriori, un morfismo entre conjuntos afines se puede definir globalmente por polinomios). No daremos la definición precisa de morfismo, sino que nos limitaremos a ver la diferencia fundamental entre los conjuntos afines y proyectivos. En el caso proyectivo, puede demostrarse que la imagen por un morfismo de un conjunto proyectivo sigue siendo un conjunto proyectivo (por eso la imagen de cualquier parametrización es siempre un conjunto proyectivo). Sin embargo, en el caso afín, los morfismos no conservan conjuntos afines: basta pensar en la imagen de la hipérbola $V(XY - 1)$ sobre cualquiera de los ejes coordenados, que es toda la recta menos un punto. La situación puede ser más complicada aún:

Ejemplo 10.19. Consideremos la aplicación $\mathbb{A}^2_k \to \mathbb{A}^2_k$ definida por $(x, y) \mapsto (x, xy)$. La imagen de la recta $V(Y - \lambda)$ es la recta $V(Y - \lambda X)$. Por tanto, la imagen de la aplicación es la unión de las rectas que pasan por $(0, 0)$ con pendiente finita (es decir, todas las rectas excepto la recta vertical $V(X)$). Podemos escribir entonces la imagen como $\mathbb{A}^2_k \setminus \big[V(X) \setminus V(X, Y)\big]$. En general, se llama *conjunto constructible* a un conjunto afín menos un conjunto afín al que previamente se le ha quitado otro conjunto afín, al que a su vez previamente se le ha quitado... (y así una cantidad finita de veces). Lo que sí puede llegar a demostrarse es que la imagen por un morfismo de un conjunto constructible es siempre constructible.

Terminamos analizando lo que pasa en el caso en que el cuerpo no sea algebraicamente cerrado, en concreto cuando tomamos $k = \mathbb{R}$. En tal caso, los morfismos hacen cosas más complicadas. Por ejemplo, la imagen de la circunferencia $V(X^2 + Y^2 - 1)$ al proyectar sobre cualquiera de los ejes coordenados es el intervalo $[-1, 1]$, que ya hay que definirlo por desigualdades. Un conjunto definido por igualdades y desigualdades polinomiales es lo que se llama un *conjunto semialgebraico*, y el estudio de tales conjuntos es el objeto de la llamada *geometría algebraica real*. El resultado clave en este campo es que la imagen por un morfismo de un conjunto semialgebraico es un conjunto semialgebraico.