Equivalencia Entre Curvas Elípticas y Números Congruentes

Richard Fabian Arteaga Ospina

Universidad de Antioquia
Facultad de Ciencias Exactas y Naturales
Instituto de Matemáticas
Medellín, Colombia
2018

Equivalencia Entre Curvas Elípticas y Números Congruentes

Richard Fabian Arteaga Ospina

Tesis presentada como requisito parcial para optar al título de:
Matemático

Director:
Ph.D. Pedro Hernandez Rizzo

Universidad de Antioquia
Facultad de Ciencias Exactas y Naturales
Instituto de Matemáticas
Medellín, Colombia
2018

Contenido

1. Introducción

La matemática de los griegos y los árabes han dejado varios problemas abiertos. Problemas que en la búsqueda de su solución han posibilitado el avance de la misma matemática. Basta ver toda la teoría creada en el siglo XVIII para demostrar la imposibilidad de las famosas construcciones griegas con regla y compás. Otro problema, muy famoso, es el problema de los números congruentes. El armamento matemático que en la actualidad hay detrás de este problema es "tremendo", sólo por mencionar algunas ramas de la matemática de las que se vale: álgebra, análisis, geometría algebraica y teoría de números lo cual muestra entre otras cosas, el uso combinado de herramientas matemáticas para su solución.

Para aclarar la complejidad que encierra el inocente problema del número congruente, empecemos por su definición. Un número natural n es un número congruente si existe un triángulo rectángulo de lados racionales tal que su área es n. Desde un punto de vista histórico, el problema de estudiar si un número dado es congruente proviene de los árabes, aunque siendo ellos herederos activos de la tradición matemática griega, posiblemente haya sido planteado mucho antes. El primer registro data del siglo X cuando el matemático Al-Karaji se hizo la siguiente pregunta: ¿Para qué enteros n existe un número racional ω tal que $\omega - n$, ω y $\omega + n$ sean cuadrados perfectos racionales? [2]

Distintos matemáticos se han enfrentado a este problema y han dado aportes parciales o particulares, o han encontrado definiciones equivalentes. Por citar algunos, Fibonacci mostró que 5 es un número congruente, Fermat mostró que 1 no es congruente, Euler dio la definición actual de número congruente.

El matemático Jerrold Tunnell [12] conjeturo una caracterización de número congruente, en su trabajo asegura que un entero n libre de cuadrados es congruente, ya que el ser congruente es independiente de factor cuadrado, si y solo si la cantidad de soluciones de cierta ecuación diofántica es el doble que otra, por ejemplo si n es impar las ecuaciones son

$$2X^2 + Y^2 + 8Z^2 = n$$
$$2X^2 + Y^2 + 32Z^2 = n$$

El inconveniente es que Tunnell en una de las implicaciones de la prueba utilizó como hipótesis uno de los problemas del milenio, la conjetura de Birch y Swinnerton-Dyer. Esta conjetura proporciona un criterio para que una curva elíptica tenga solo un número finito de puntos

racionales.

El estudio de las curvas elípticas no es realmente nuevo. Se definen mediante ecuaciones polinomiales de tercer grado. El papel de estas curvas ha sido central en matemáticas desde el siglo XVIII. Sus propiedades geométricas y aritméticas encontraron aplicación en múltiples problemas y campos matemáticos. Por ejemplo, el Algoritmo de Lenstra [9] que sirve para factorizar enteros grandes y por tanto útil en la criptografía; o como herramienta en la demostración del último teorema de Fermat. Las curvas elípticas tienen una faceta algebraica, además de la geométrica. Así que parara su comprensión se necesita hablar primero de geometría algebraica.

La geometría algebraica es una rama de las matemáticas que combina la geometría analítica con el álgebra abstracta, especialmente el algebra conmutativa. Estudia las propiedades de sistemas de ecuaciones algebraicas y su interpretación geométrica. Es esencial para llegar a definir y entender la estructura de grupo en curvas elípticas, estructura importante para el objetivo principal del presente trabajo.

Este trabajo pretende caracterizar los números congruentes a partir de la estructura de grupo de ciertas curvas elípticas, restringido a los puntos racionales, que se construyen a partir de la definición de número congruente. Más específicamente con la existencia de elementos de orden infinito en el grupo. Utilizando como hipótesis el teorema Mordell-Weil, el cual afirma que el grupo es finitamente generado.

Es interesante mencionar que, aunque todos los resultados a utilizar en la caracterización que se pretende hacer están demostrados y ofrece un método sencillo de encontrar el triangulo rectángulo que demuestra la congruencia del número, el realizado por Tunnell es superior, en el sentido de que ofrece un algoritmo más eficiente para comprobar el ser congruente, ya que es mas sencillo encontrar las soluciones enteras a las ecuaciones de Tunnell que la existencia de un punto racional de orden infinito en la curva elíptica.

Para la comprensión de este trabajo se recomienda principalmente tener algún conocimiento sobre teoría de cuerpos y álgebras de polinomios. Se iniciará por una revisión de geometría algebraica en el plano afín estudiando cómo traducir definiciones algebraicas como irreductibilidad, divisibilidad, derivadas de polinomios y otras desde un punto de vista más geométrico y llevar los elementos del plano afín al espacio proyectivo, permitiendo la aplicación del teorema de Bézout. Posteriormente se realizará un estudio de curvas racionales para establecer la buena definición a la operación de grupo definida sobre las curvas elípticas.
Cabe aclarar, que este trabajo es una monografía principalmente sobre el artículo [8], para el cual, fue necesario consultar libros como [13] para justificar y explicar todos los resultados y argumentos que en dicho artículo se presentaban.

2. Curvas algebraicas planas afines

En este capítulo se estudiarán algunos conceptos básicos de geometría algebraica, como se dijo en la introducción, se describe como se interpretan la propiedades algebraicas de los polinomios de dos variables en un sentido geométrico. Cuando son polinomios de varias variables, aparece la interpretación geométrica en el trazo del conjunto de soluciones.

2.1. Introducción

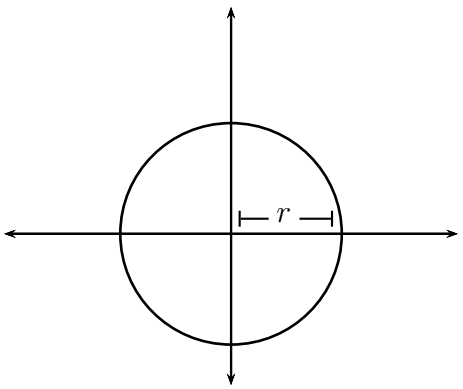
Sea K un cuerpo, se denotará por $\mathbb{A}^2_(K)$ a $K \times K$ sin ninguna estructura algebraica, es decir, $\mathbb{A}^2(K)$ es el conjunto de 2-tuplas de elementos de K. Lo llamaremos *plano afín* y a sus elementos *puntos*.

Definición 2.1. Una curva algebraica plana afín $V_K(f)$, o simplemente curva, es un subconjunto de $\mathbb{A}^2(K)$ formado por los ceros de $f \in K[X,Y]\backslash K$, esto es

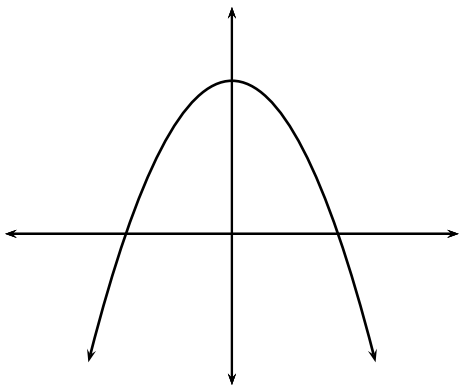
$$V_K(f) = \big\{(x,y) \in \mathbb{A}^2(K)/f(x,y) = 0\big\}$$

se escribe $V(f)$ si K es sobrentendido.

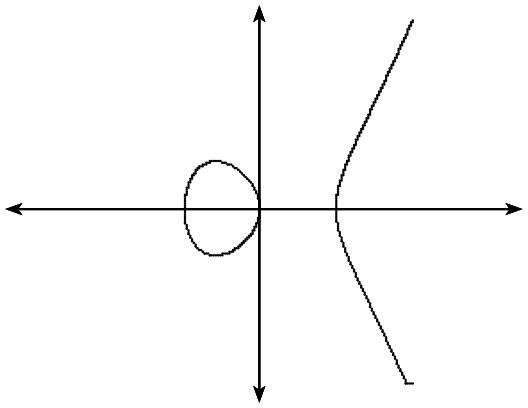
Ejemplo 2.2. Sea $K = \mathbb{R}$:



(a) $V(X^2 + Y^2 - r^2)$



(b) $V(X^2 + Y - 2)$



(c) $V(\,Y^2 - X(X-1)(X+1)\,)$

Polinomios distintos pueden definir el mismo conjunto de ceros. Por ejemplo, $V(f) = V(f^m)$, con $m > 1$. Para esto será necesario encontrar una noción de "minimalidad"que permita asociarle a una curva el menor polinomio que la genere.
De ahora en adelante, a menos que se mencione lo contrario, los puntos están sobre un cuerpo K algebraicamente cerrado y de característica cero. Por ejemplo, $K = \mathbb{C}$ el cuerpo de números complejos.

Proposición 2.3. *Sean $p, f \in K[X,Y]\backslash K$ tal que p es irreducible. Entonces $V(p) \subseteq V(f)$ si y solo si $p|f$ en $K[X,Y]$.*

Demostración. Sin perdida de generalidad supongamos que Y aparece en p. Defina $A = K[X]$ y $L = K(X)$ el cuerpo de fracciones de A. Por hipótesis p es irreducible en $A[Y]$, entonces p también lo es en $L[Y]$ como consecuencia del lema de Gauss (pag. 143 de [13]). Por absurdo se supone que $p \nmid f$ en $K[X,Y]$, por tanto $\mathrm{mcd}(p,f) = 1$ en $L[Y]$, nuevamente por el lema de Gauss. Dado que $L[Y]$ es un dominio de ideales principales, entonces existen $a, b \in L[Y]$ tales que

$$ap + bf = 1.$$

Se puede escribir $a = a'/c$ y $b = b'/c$ con $a, b \in A[Y]$ y $c \in A$ no nulo, por tanto

$$a'p + b'f = c.$$

Como K es algebraicamente cerrado y Y aparece en p, la ecuación $p(x,Y) = 0$ para $x \in K$ tiene solución, excepto para un número finito de x. Sabiendo que $V(p) \subseteq V(f)$ entonces existe una infinidad de $x \in K$ tal que $c(x) = 0$, por tanto $c = 0$; contradicción. Se sigue que $p|f$ en $K[X,Y]$.
El reciproco es consecuencia de que $V(gh) = V(g) \cup V(h)$ para todo $g, h \in K[X,Y]\backslash K$. □

De la anterior proposición se deduce que una curva $V(f)$ esta totalmente determinada, como conjunto y a menos de factor constante, por el producto de los factores irreducible de f. Es decir, $V(f) = V(\prod_{i=1}^{d} p_i)$ donde los p_i son todos los factores irreducible distintos de f.

Una curva $V(f)$ se dice *irreducible* si f es un polinomio irreducible. El *grado* de $V(f)$ se define como el grado del polinomio f, se denota por $\mathrm{d}^\circ f$. Las *componentes irreducibles* de una curva $V(f)$ son las curvas definidas por los factores irreducibles de f. Por último, la *multiplicidad* de una componente p de f es el mayor exponente de p que divide a f; cuando es mayor que 1, se dice que p es una componente *múltiple* de f.

Observaciones:

- Las curvas que aparecen en el ejemplo 2.2 son irreducibles. Note que (c) siendo irreducible su gráfico esta formado por dos partes disyuntas. Además ninguna de ellas es una curva, de no ser así se contradice la irreducibilidad de (c) aplicando la proposición 2.3.
- Como consecuencia de la proposición 2.3. Si $V(f) \subseteq V(g)$ entonces los factores irreducibles de f dividen a g.

2.2. Cambio de referencial

Un método útil en curvas algebraicas es hacer un cambio de referencial o coordenadas tal que se preserven propiedades geométricas. Estas serán el tipo de propiedades a las que les daremos mayor prioridad en esta tesis, aquellas independientes del sistema de referencia en que se definan. Una de las aplicaciones habituales de los cambios de coordenadas es la de reducir a casos más simples el estudio de propiedades de las curvas.

Definición 2.4. Un *referencial* o *sistema de coordenadas* del plano $\mathbb{A}^2(K)$, digamos R, consiste en un punto $O \in \mathbb{A}^2(K)$, llamado el *origen del referencial*, y una base $\{v_1, v_2\}$ del espacio vectorial K^2. El referencial *canónico* es dado por

$$O = (0,0) \qquad v_1 = (1,0) \qquad v_2 = (0,1).$$

El *vector coordenadas* de um punto $P \in K^2$ en relación a un referencial

$$R = \{O, \{v_1, v_2\}\}$$

es el par ordenado $(P)_R = (x_1, x_2) \in K^2$ tal que

$$P = O + x_1 v_1 + x_2 v_2.$$

Sean $R = \{O, \{v_1, v_2\}\}$ y $R' = \{O', \{v_1', v_2'\}\}$ dos referenciales tal que $(P)_R = (x_1, x_2)$ y $(P)_{R'} = (x_1', x_2')$ con $P \in K^2$. Veamos como se relaciona el vector de coordenadas (x_1', x_2') con x_1 y x_2. Para esto, se escribe $v_1 = a_{11}v_1' + a_{21}v_2'$, $v_2 = a_{12}v_1' + a_{22}v_2'$ y $O - O' = a_1 v_1' + a_2 v_2'$. Por tanto (a_{ij}) es la matriz cambio de base de $\{v_1, v_2\}$ a $\{v_1', v_2'\}$ y, en particular, cumple que $\det(a_{ij}) \neq 0$. Luego

$$\begin{aligned} x_1'v_1' + x_2v_2 &= P - O' \\ &= O - O' + x_1v_1 + x_2v_2 \\ &= a_1v_1' + a_2v_2' + x_1(a_{11}v_1' + a_{21}v_2') + x_2(a_{12}v_1' + a_{22}v_2') \\ &= (a_1 + a_{11}x_1 + a_{12}x_2)v_1' + (a_2 + a_{21}x_1 + a_{22}x_2)v_2'. \end{aligned}$$

Entonces se tiene la relación $(P)_{R'} = (a_1 + a_{11}x_1 + a_{12}x_2, a_2 + a_{21}x_1 + a_{22}x_2)$. Con esto se puede definir la transformación de cambio de referencial.

Definición 2.5. Una *transformación afín* o *afinidad* en $\mathbb{A}^2(K)$ es una aplicación T, donde $T : K^2 \longrightarrow K^2$ es una composición de una traslación con un isomorfismo lineal.

De la definición se sigue que si T es una afinidad entonces para $P = (x_1, x_2) \in K^2$ se cumple que $T(P) = (a_{11}x_1 + a_{12}x_2 + a_1, a_{21}x_1 + a_{22}x_2 + a_2) = AP + O$ con $O = (a_1, a_2)$ y $A = (a_{i,j})$ tal que $\det(A) \neq 0$. Se puede definir el referencial $R = \{O, \{(a_{11}, a_{21}), (a_{12}, a_{22})\}\}$ que cumple la relación

$$(T(P))_R = P \qquad (\forall P \in K^2).$$

Se dice que R es el referencial *asociado* a T, o que T y R son *asociados*. Además T es biyectiva, por ser composición de dos aplicaciones biyectivas, y su inversa también es una afinidad. En efecto, si $P \in K^2$ entonces $T^{-1}(P) = A^{-1}P - A^{-1}O$ y

$$(P)_R = T^{-1}(P) \qquad (\forall P \in K^2),$$

es decir, la afinidad T^{-1} encuentra las coordenadas de un punto en el referencial R. Esto proporciona las nuevas coordenadas a partir de las previamente dadas, que generalmente están en el referencial canónico.

Proposición 2.6. *Sea T una afinidad. La aplicación $T_\bullet : K[X, Y] \longrightarrow K[X, Y]$ definida por*

$$(T_\bullet f)(x, y) = f(T^{-1}(x, y)) \qquad \forall (x, y) \in K^2,$$

es un K-automorfismo.

Demostración. Claramente $T_\bullet$ es homomorfismo K-lineal, falta probar que es biyectivo. Digamos que $T^{-1}(x, y) = (b_{11}x + b_{12}y + b_1, b_{21}x + b_{22}y + b_2)$ con $\det(b_{ij}) \neq 0$.
Para la inyectividad veamos que $\ker T_\bullet = \{0\}$. Sea $f \in K[X, Y]$ tal que $(T_\bullet f) = 0$, por tanto $(T_\bullet f)(x, y) = f(T^{-1}(x, y)) = 0$ $\forall (x, y) \in K^2$ y como la imagen de T^{-1} es K^2, entonces f se anula en K^2; Luego $f = 0$.
Utilizando que $T_\bullet$ es homomorfismo K-lineal, se sigue la sobreyectividad si existen $f, g \in K[X, Y]$ tales que $T_\bullet f = X$ y $T_\bullet g = Y$. Sea $f(X, Y) = (\det(b_{ij}))^{-1}(b_{22}X - b_{12}Y - b_{22}b_1 + b_{12}b_2)$,

luego

$$\begin{aligned} f(T^{-1}(x,y)) &= f(b_{11}x + b_{12}y + b_1, b_{21}x + b_{22}y + b_2) \\ &= (\det(b_{ij}))^{-1}[b_{22}(b_{11}x + b_{12}y + b_1) - b_{12}(b_{21}x + b_{22}y + b_2) - b_{22}b_1 + b_{12}b_2] \\ &= (\det(b_{ij}))^{-1}([b_{22}b_{11} - b_{12}b_{21}]x) \\ &= (\det(b_{ij}))^{-1}(\det(b_{ij}))x \\ &= x \end{aligned}$$

Análogamente se puede definir g. □

Si R es el referencial asociado a T entonces $(P)_R = T^{-1}(P)$, es decir, $T^{-1}(P)$ obtiene las coordenadas de P en el referencial R. Esto justifica el uso de T^{-1} en la definición de $T_\bullet$.

Corolario 2.7. *Sean $V(f)$ una curva, T una afinidad y R su referencial asociado. Entonces:*

(a) *$V(T_\bullet f) = T(V(f))$.*

(b) *La ecuación de la curva $V(f)$ con respecto al referencial R es $(T^{-1})_\bullet f$.*

Demostración.

(a)

$$\begin{aligned} P \in V(T_\bullet f) &\iff (T_\bullet f)(P) = 0 \\ &\iff f(T^{-1}(P)) = 0 \\ &\iff T^{-1}(P) \in V(f) \\ &\iff P \in T(V(f)) \end{aligned}$$

(b)

$$\begin{aligned} P \in V(f) &\iff f(P) = 0 \\ &\iff f(T(T^{-1}(P))) = 0 \\ &\iff (T^{-1})_\bullet f(T^{-1}(P)) = 0 \\ &\iff (T^{-1})_\bullet f((P)_R) = 0 \end{aligned}$$

□

Definición 2.8. Se dice que una propieded $\mathcal{P}$ es *invariante* o *independiente del referencial* si, para toda afinidad T, una curva $V(f)$ (o $\mathcal{C}$ conjunto de curvas o puntos) satisface $\mathcal{P}$ si y solo si $V(T_\bullet f)$ (respectivamente $T_\bullet(\mathcal{C})$) satisface $\mathcal{P}$.

Sea T una afinidad, es fácil ver que las siguientes propiedades son invariantes:

- Grado de una curva. Es decir, si $f \in K[X,Y]$ tiene grado n entonces $T_\bullet f$ tiene grado n.

- Reducibilidad de una curva.
- La propiedad de que un conjunto de curvas se intersectan.

En los siguientes capítulos se usaran algunas propiedades invariantes sin entrar en detalle a la demostración de la invarianza.

Ejemplo 2.9. **(a)** Sea $P = (1, 2)$ en el referencial canónico y $R = \{(1, 1), \{(1, 2), (3, 5)\}\}$. A partir del procedimiento para encontrar la forma de las afinidades se encuentre $(P)_R$ y despues se verifica que $(P)_R = T^{-1}(P)$, donde T es la afinidad asociada a R. Se tienen que

$$\begin{aligned}(1,0) &= (-5)\cdot(1,2) + 2\cdot(3.5)\\ (0,1) &= 3\cdot(1,2) + (-1)\cdot(3.5)\\ (0,0) - (1,1) &= 2\cdot(1,2) + (-1)\cdot(3.5)\end{aligned}$$

Entonces $(P)_R = (2 - 5 \cdot 1 + 3 \cdot 2, -1 + 2 \cdot 1 - 1 \cdot 2) = (3, -1)$. La afinidad asociada a R y su inversa son

$$\begin{aligned}T(X,Y) &= \begin{bmatrix}1 & 3\\ 2 & 5\end{bmatrix}\cdot\begin{pmatrix}X\\ Y\end{pmatrix} + \begin{pmatrix}1\\ 1\end{pmatrix}\\ T^{-1}(X,Y) &= \begin{bmatrix}1 & 3\\ 2 & 5\end{bmatrix}^{-1}\cdot\begin{pmatrix}X\\ Y\end{pmatrix} - \begin{bmatrix}1 & 3\\ 2 & 5\end{bmatrix}^{-1}\cdot\begin{pmatrix}1\\ 1\end{pmatrix}\\ &= \begin{bmatrix}-5 & 3\\ 2 & -1\end{bmatrix}\cdot\begin{pmatrix}X\\ Y\end{pmatrix} - \begin{pmatrix}-2\\ 1\end{pmatrix}\end{aligned}$$

por tanto se cumple que $T^{-1}(P) = (3, -1) = (P)_R$.

(b) Sean $\{P_1, P_2, P_3\}$ y $\{Q_1, Q_2, Q_3\}$ conjuntos de puntos no colineales, entonces existe una afinidad T tal que $T(P_i) = Q_i$ para $i = 1, 2, 3$. En efecto, como los $P_i = (x_i, y_i)$ no son colineales entonces los puntos $(x_i, y_i, 1)$ no son coplanares, para $i = 1, 2, 3$, por tanto la aplicación lineal en K^3 definida por la matriz que tiene como filas esos puntos es un isomorfismo. Entonces, si $Q_i = (w_i, z_i)$, existen $a, b, c, d, e, f \in K$ tales que

$$\begin{bmatrix}x_1 & y_1 & 1\\ x_2 & y_2 & 1\\ x_3 & y_3 & 1\end{bmatrix}\cdot\begin{pmatrix}a\\ b\\ c\end{pmatrix} = \begin{pmatrix}w_1\\ w_2\\ w_3\end{pmatrix}$$

$$\begin{bmatrix}x_1 & y_1 & 1\\ x_2 & y_2 & 1\\ x_3 & y_3 & 1\end{bmatrix}\cdot\begin{pmatrix}d\\ e\\ f\end{pmatrix} = \begin{pmatrix}z_1\\ z_2\\ z_3\end{pmatrix}$$

defina $T(x, y) = (ax + by + c, dx + ey + f)$.

2.3. Intersección de curvas

El problema de encontrar la solución de un sistema de ecuaciones es uno de los mas antiguos e importantes de la matemática. Los primeros que se estudian son los sistemas lineales y la existencia de soluciones, finitas o infinitas; además la forma de encontrarlas.
Considerando ecuaciones de polinomios en dos variables, lo anterior se traduce en estudiar la intersección de curvas y la manera de encontrar los puntos de intersección, en caso de existir y ser finitos.
Veamos que el conjunto de intersección de curvas, sin componentes irreducibles en común, es finito.

Lema 2.10. *Sean $f, g \in K[X,Y]\backslash K$ sin factores irreducibles en común, entonces existen $a, b, c, d \in K[X,Y]$, $r \in K[X]$ y $s \in K[Y]$ tales que*

$$af + bg = r \qquad y \qquad cf + dg = s.$$

Demostración. Vea la demostración de la proposición 2.3. □

Se sabe que para $f \in K[X]\backslash\{0\}$ la ecuación $f = 0$ tiene a lo mas $\mathrm{d}^\circ f$ soluciones diferentes. Teniendo esto en cuenta veamos la siguiente proposición.

Proposición 2.11. *El conjunto de intersección de dos curvas sin componentes irreducibles en común es finito. Es decir, si $f, g \in K[X,Y]\backslash K$ tal que $mcd(f,g) = 1$ en $K[X,Y]$ entonces $|V(f) \cap V(g)| < +\infty$.*

Demostración. Aplicando el lema 2.10 se obtienen $a, b, c, d \in K[X,Y]$, $r \in K[X]$ y $s \in K[Y]$ tales que

$$af + bg = r(X) \qquad \text{y} \qquad cf + dg = s(Y).$$

Si $P = (x, y) \in V(f) \cap V(g)$ entonces, por las anteriores igualdades, se tiene que

$$r(x) = a(P)f(P) + b(P)g(P) = 0 \qquad \text{y} \qquad s(y) = c(P)f(P) + d(P)g(P) = 0.$$

Luego y es raíz de $s(Y)$ y x de $r(X)$. Hay a lo sumo $\mathrm{d}^\circ r$ y $\mathrm{d}^\circ s$ raíces distintas de r y s, respectivamente. Entonces $|V(f) \cap V(g)| \leq \mathrm{d}^\circ r \cdot \mathrm{d}^\circ s$. □

La anterior proposición nos garantiza una cota superior para las intersecciones de dos curvas con ciertas características, pero ¿cómo las encontramos?. El método usual o natural es despejar una de la variables y después remplazarla en la otra ecuación, esto no siempre es fácil de aplicar. Veamos como podemos encontrar las intersecciones con ayuda de la resultante.

Definición 2.12. Sea A un anillo conmutativo (en particular $K[X]$) y $f, g \in A[Y]$ tal que

$$f(Y) = a_n Y^n + a_{n-1} Y^{n-1} + \cdots + a_0 \qquad (n \geq 1)$$
$$g(Y) = b_m Y^m + b_{m-1} Y^{m-1} + \cdots + b_0 \qquad (m \geq 1).$$

La *resultante* de f y g se define como

$$R_{f,g} = \begin{vmatrix} a_n & a_{n-1} & \cdots & a_0 & & & & \\ & a_n & \cdots & a_1 & a_0 & & & \\ & & \cdots & \cdots & \cdots & & & \\ & & & & & a_n & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & & & & \\ & b_m & \cdots & b_1 & b_0 & & & \\ & & \cdots & \cdots & \cdots & & & \\ & & & & & b_m & \cdots & b_0 \end{vmatrix}$$

es un determinante de una matriz de orden $n+m$, tal que las primeras m filas tienen $a's$ y las otras n filas tienen $b's$. Los espacios en blanco de cada fila son llenados con ceros.
Cuando $A = K[X_1, X_2, \ldots, X_n]$ y $f, g \in A[Y]$ entonces la resultante de f y g es un polinomio de n variables y se denota por $R_{f,g}(X_1, X_2, \ldots, X_n)$.

Ejemplo 2.13. Considere $f(X,Y) = X^2 + Y^2 - 4$ y $g(X,Y) = X + Y^2 - 3$. Luego

$$R_{f,g}(Y) = \begin{vmatrix} 1 & 0 & Y^2-4 \\ 1 & Y^2-3 & 0 \\ 0 & 1 & Y^2-3 \end{vmatrix} = (Y^2-3)^2 + Y^2 - 4$$

Note que para encontrar las coordenadas en Y de los elementos de $V(f) \cap V(g)$, el método usual seria despejar X en $g = 0$ y reemplazar en $f = 0$. Lo cual es igual a $R_{f,g}(Y) = 0$. Esta coincidencia no es accidental, además veremos que la resultante puede dar mas información que el método usual.

Proposición 2.14. *Sean $f, g \in K[X,Y]\backslash K$, suponga*

$$f(X,Y) = a_n(X)Y^n + a_{n-1}(X)Y^{n-1} + \cdots + a_0(X) \qquad (n \geq 1)$$
$$g(X,Y) = b_m(X)Y^m + b_{m-1}(X)Y^{m-1} + \cdots + b_0(X) \qquad (m \geq 1)$$

donde $a_i, b_j \in K[X]$. Si $\alpha \in K$ entonces

$$R_{f,g}(\alpha) = 0 \Longleftrightarrow \begin{cases} a_n(\alpha) = b_m(\alpha) = 0 \\ o \\ f(\alpha, Y) \text{ y } g(\alpha, Y) \text{ tienen factor común no constante.} \end{cases}$$

Demostración. Sea $\alpha \in K$. Suponga $a_n(\alpha) \neq 0$, luego $f(\alpha, Y)$ y $g(\alpha, Y)$ tienen factor no constante en $K[Y]$ si y solo si existen $p, q \in K[Y]\backslash K$ con $\mathrm{d}^\circ p = n-1$ y $\mathrm{d}^\circ q = m-1$ tales que $q(Y)f(\alpha,Y) = p(Y)g(\alpha,Y)$, ya que K es algebraicamente cerrado. Suponga

$$p(Y) = u_{n-1}Y^{n-1} + u_{n-2}Y^{n-2} + \cdots + u_0$$
$$q(Y) = v_{m-1}Y^{m-1} + v_{m-2}Y^{m-2} + \cdots + v_0$$

entonces

$$q(Y)f(\alpha,Y)=p(Y)g(\alpha,Y)$$
$$(v_{m-1}Y^{m-1}+\cdots+v_0)(a_n(\alpha)Y^n+\cdots+a_0(\alpha))=(u_{n-1}Y^{n-1}+\cdots+u_0)(b_m(\alpha)Y^m+\cdots+b_0(\alpha))$$

igualando los coeficientes de Y^{m+n-i}, se tiene que

$$\begin{aligned}
v_{m-1}a_n(\alpha) &= u_{n-1}b_m(\alpha) && (i=1)\\
v_{m-1}a_{n-1}(\alpha)+v_{m-2}a_n(\alpha) &= u_{n-1}b_{m-1}(\alpha)+u_{n-2}b_m(\alpha) && (i=2)\\
&\vdots && \vdots\\
\sum_{j=1}^{m} v_{m-j}a_{n-i+j}(\alpha) &= \sum_{j=1}^{n} u_{n-j}b_{m-i+j}(\alpha) && (i=\cdots,n+m)
\end{aligned}$$

donde $a_{n-i+j}=0$ si $n-i+j<0$ o $n-i+j>n$, y $b_{m-i+j}=0$ si $m-i+j<0$ o $m-i+j>m$. Las anteriores igualdades se pueden escribir en forma matricial como

$$\begin{bmatrix}
a_n(\alpha) & & & & -b_m(\alpha) & & & \\
a_{n-1}(\alpha) & a_n(\alpha) & & & -b_{m-1}(\alpha) & -b_m(\alpha) & & \\
a_{n-2}(\alpha) & a_{n-1}(\alpha) & a_n(\alpha) & & -b_{m-2}(\alpha) & -b_{m-1}(\alpha) & -b_m(\alpha) & \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots \\
a_0(\alpha) & a_1(\alpha) & a_2(\alpha) & \cdots & -b_0(\alpha) & -b_1(\alpha) & -b_2(\alpha) & \cdots \\
 & a_0(\alpha) & a_1(\alpha) & \cdots & & -b_0(\alpha) & -b_1(\alpha) & \cdots \\
 & \vdots & \vdots & & & \vdots & \vdots & \\
 & & & a_0(\alpha) & & & & -b_0(\alpha)
\end{bmatrix}\cdot\begin{pmatrix} v_{m-1}\\ v_{m-2}\\ \vdots\\ v_0\\ u_{n-1}\\ u_{n-2}\\ \vdots\\ u_0 \end{pmatrix}=0$$

denotemos lo anterior por $A\cdot V=0$, donde A tiene orden $n+m$, tal que las primeras m columnas tienen $a's$ y las otras n columnas tienen $b's$. Los espacios en blanco de cada fila son ceros. La existencia de p y q es equivalente a la de V. Además $A\cdot V=0$ si y solo si $\det(A)=0$. Por definición de la resultante de f y g evaluada en α y propiedades del determinante se tiene que

$$R_{f,g}(\alpha)=(-1)^n\det(A^t)=(-1)^n\det(A)=0$$

□

Sean $f,g\in K[X,Y]$, se sigue que las raćes de $R_{f,g}(X)$ (resp. $R_{f,g}(Y)$), sin tener en cuenta los valores que anulan el polinomio que acompañan la mayor potencia de Y (resp. X), son las proyecciones de los elementos de $V(f)\cap V(g)$ en el eje X (resp. Y). Por tanto $R_{f,g}(X)$ o $R_{f,g}(Y)$ es idénticamente nulo si y solo si f y g tienen componentes en común. En este caso $|V(f)\cap V(g)|$ no es finito.

Ejemplo 2.15. Sea $f(x) = ax^3 + bx^2 + cx + d$, con $a \neq 0$, entonces $f'(x) = 3ax^2 + 2bx + c$.

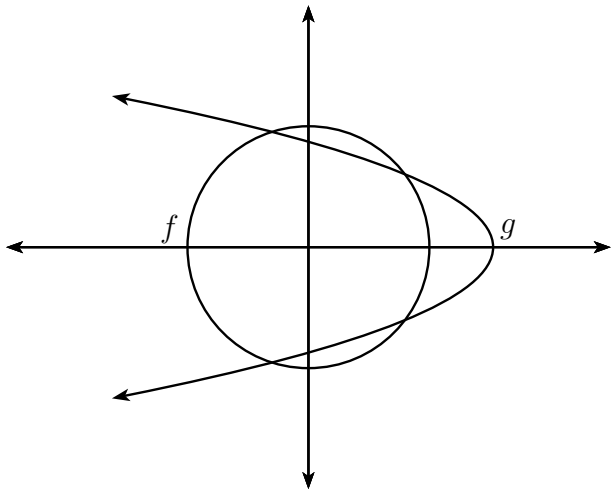
$$R_{f,f'} = \begin{vmatrix} a & b & c & d & 0 \\ 0 & a & b & c & d \\ 3a & 2b & c & 0 & 0 \\ 0 & 3a & 2b & c & 0 \\ 0 & 0 & 3a & 2b & c \end{vmatrix} = a(-18abcd + 27a^2d^2 + 4ac^3 + 4b^3d - b^2c^2).$$

Si $-18abcd + 27a^2d^2 + 4ac^3 + 4b^3d - b^2c^2 = 0$ entonces f tiene raíz múltiple.

Continuando con el ejemplo 2.13. Aplicando el método usual para encontrar las coordenadas en el eje X de los elementos de $V(f) \cap V(g)$, despejando Y de $g = 0$ y reemplazando en $f = 0$ se tiene la ecuación

$$X^2 - X - 1 = 0,$$

la cual tiene dos soluciones reales distintas, con ellas se pueden encontrar los cuatro elementos de $V(f) \cap V(g)$ que se ven en la siguiente figura:



Ahora considere la resultante de f y g en X, se obtiene

$$R_{f,g}(X) = \begin{vmatrix} 1 & 0 & X^2 - 4 & 0 \\ 0 & 1 & 0 & X^2 - 4 \\ 1 & 0 & X - 3 & 0 \\ 0 & 1 & 0 & X - 3 \end{vmatrix} = X^4 - 2X^3 - X^2 + 2X + 1 = (X^2 - X - 1)^2$$

Note que aunque encontramos las mismas soluciones que con el método usual, en la resultante tienen multiplicidad dos. Puede significar que hay dos pares de puntos en $V(f) \cap V(g)$ con la misma abscisa, como se puede ver en la figura. Al decir que "puede significar" es porque

la multiplicidad en la resultante también se puede interpretar como el *grado de intersección* de f y g en el punto con esa abscisa. Esto se estudiará mas adelante para la demostración del teorema de Bézout.
Por lo anterior y la proposición 2.14 es importante conocer el grado de la resultante entre f y g, para tener idea de la cantidad de puntos en $V(f) \cap V(g)$. Es posible conocer el grado de la resultante para unos polinomios con ciertas condiciones, como veremos enseguida. Pero antes necesitamos una definición.
Recuerde que un polinomio *homogéneo* de grado n es aquel que todos sus monomios tienen grado n. Por tanto, si $f \in K[X,Y]$ es homogeneo de grado n entonces la forma de f es

$$f(X,Y) = \sum_{i=0}^{n} a_i X^{n-i} Y^i.$$

Además cumple la relación $f(TX,TY) = T^n f(X,Y)$ en $K[X,Y,T]$, donde T es una nueva variable independiente. Otra propiedad importante, la que da sentido a la siguiente definición, es que f se puede expresar como

$$f(X,Y) = \prod_{i=1}^{n} (b_i X - c_i Y)$$

para esto es esencial la hipótesis de que K es algebraicamente cerrado.

Definición 2.16. Sea $f \in K[X,Y]$, digamos $\mathrm{d}^\circ f = n$, se puede escribir como

$$f(X,Y) = f_0 + f_1(X,Y) + \cdots + f_n(X,Y)$$

donde f_i es homogéneo de grado i y $f_n \neq 0$. Cada componente $aX + bY$ de f_n se llama *dirección asintótica* de f (o de $V(f)$).

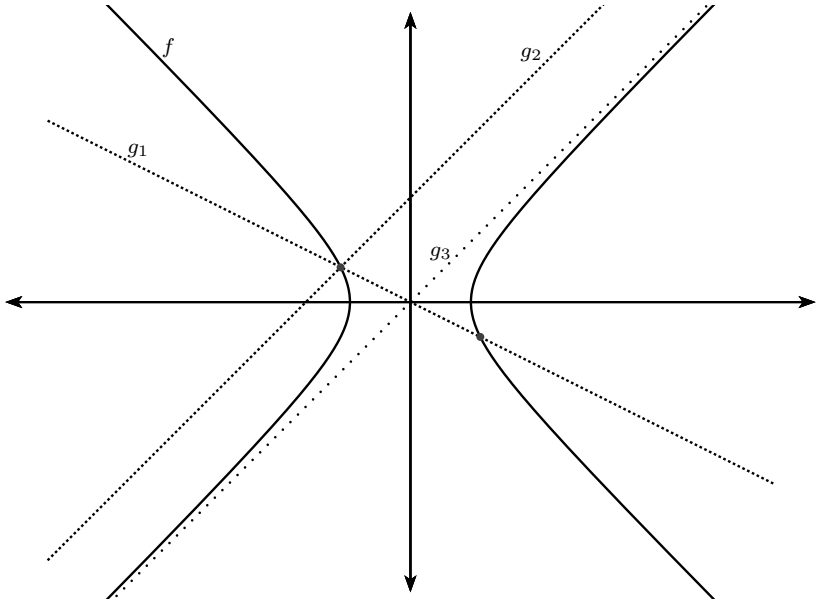
Geométricamente las direcciones asintóticas de una curva $V(f)$ son una dirección limite de recta OP, donde $P \in V(f)$ y se aleja indefinidamente del origen O.
En estos momentos estas definiciones e interpretaciones pueden no tener mucho sentido o razón de ser. En el próximo capitulo cuando se estudie el plano proyectivo y las propiedades de curvas proyectivas, se entenderá mejor esta sección. Como por ejemplo, la demostración de la siguiente proposición como consecuencia inmediata del teorema de Bézout. O si el lector prefiere la puede encontrar en [13], pag. 27.

Proposición 2.17. *Sean $f, g \in K[X,Y] \backslash K$ sin dirección asintótica en común, entonces $d^\circ R_{f,g} = d^\circ f \cdot d^\circ g$.*

Ejemplo 2.18. $f(X,Y) = X^2 - Y^2 - 1$ tiene las direcciones asintóticas $X - Y$ y $X + Y$. Considere $g(X,Y) = Y + aX - b$, luego

$$R_{f,g}(X) = \begin{vmatrix} -1 & 0 & X^2 - 1 \\ 1 & aX - b & 0 \\ 0 & 1 & aX - b \end{vmatrix} = (X^2 - 1) - (aX - b)^2 = (1 - a^2)X^2 + 2abX - (1 + b^2).$$

Note que $\mathrm{d}^\circ R_{f,g}(X) = 2$ para $a \neq \pm 1$. Cuando $a = \pm 1$ pasa que f,g tienen dirección asintótica en común y $\mathrm{d}^\circ R_{f,g}(X) = 1$ si $b \neq 0$. Observe que



$g_1 = Y + \frac{X}{2}$ intersecta a f en dos puntos y $\mathrm{d}^\circ R_{f,g_1}(X) = 2$, $g_2 = Y - X - \frac{5}{3}$ intersecta a f en un punto y $\mathrm{d}^\circ R_{f,g_2}(X) = 1$, $g_3 = Y - X$ no intersecta a f y $R_{f,g_1}(X) = -1$.

2.4. Multiplicidades

Para polinomios de una variable es fácil definir la multiplicidad en un punto o raíz, dado que cada elemento α de un cuerpo define un polinomio minimal, digamos $p_\alpha(X)$, tal que si $f(\alpha) = 0$ entonces p_α divide a f. En este caso la multiplicidad de α en f se define como el mayor exponente de p_α que divide a f. Cuando el cuerpo es algebraicamente cerrado se tiene que $p_\alpha(X) = X - \alpha$.
En polinomios de dos o mas variables no se tiene la existencia del p_α, descrito anteriormente. Por tal motivo se necesita otro método para definir la multiplicidad de puntos en una curva, que explique el porqué una curva pasa "mas veces" por un mismo punto. Para esto se utilizan las curvas mas simples, las rectas, que permiten definir de manera natural el grado de intersección con otras curvas.

Sean $f, l \in K[X,Y]\backslash K$, donde l es una recta con ecuación $Y - aX - b = 0$. Se puede encontrar las coordenadas en X de los punto de $V(f) \cap V(l)$ resolviendo la ecuación

$$f_l(X) := f(X, aX + b) = 0.$$

Posibles situaciones:

- $f_l(X)$ es nulo, esto pasa cuando l es componente de f, es decir, $l|f$.

- $f_l(X)$ es una constante no nula. Significa que $V(f) \cap V(l) = \phi$.
- $f_l(X)$ es un polinomio no constante. Como K es algebraicamente cerrado, pasa que

$$f_l(X) = c \prod_{i=1}^{d} (X - x_i)^{m_i} \tag{2-1}$$

donde d es el número de raíces distintas de $f_l(X)$, c es una constante y $x_i \neq x_j$ si $i \neq j$.

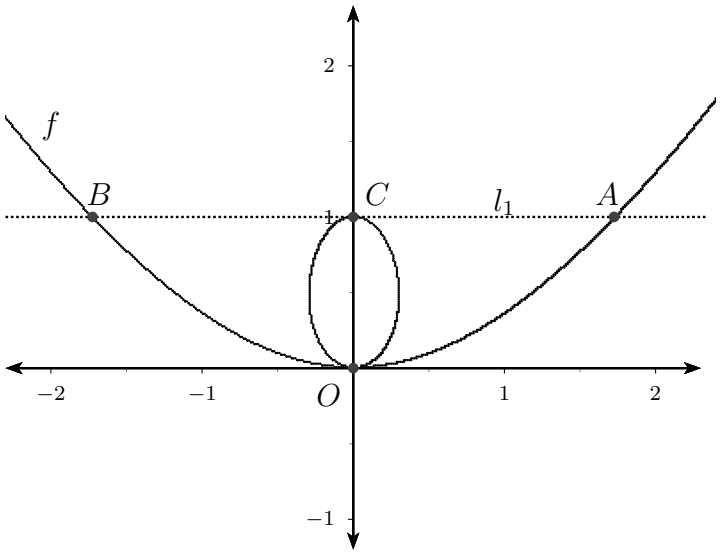
Análogamente se define $f_l(Y)$, para encontrar las coordenadas en Y.

Definición 2.19. La *multiplicidad* o *índice de intersección* de f y l en un punto P, con $l(X,Y) = Y - aX - b$, se define como

$$(f,l)_P = \begin{cases} 0 & \text{si} \quad P \notin V(f) \cap V(l) \\ \infty & \text{si} \quad P \in V(l) \subseteq V(f) \\ m_i & \text{si} \quad P = (x_i, ax_i + b), \text{ definidos en (2-1).} \end{cases}$$

Ejemplo 2.20. Sean $f(X,Y) = Y^2 - 3X^2Y - Y^3 + X^4$, $l_1 = Y - 1$, $l_2 = Y$ y $l_3 = X$.

$$f_{l_1}(X) = f(X,1) = (X + \sqrt{3}) \cdot (X - \sqrt{3}) \cdot X^2$$
$$f_{l_2}(X) = f(X,0) = X^4$$
$$f_{l_3}(Y) = f(0,Y) = (Y-1) \cdot Y^2$$



Entonces $(f,l_1)_A = (f,l_1)_B = 1$ y $(f,l_1)_C = 2$, $(f,l_2)_O = 4$, $(f,l_3)_C = 1$ y $(f,l_3)_O = 2$. Note que $\mathrm{d}^\circ f_{l_1}(X) = \mathrm{d}^\circ f_{l_2}(X) = 4$, $\mathrm{d}^\circ f_{l_3}(Y) = 3$ y l_3 es la única dirección asintótica de f.

Es de esperar, por la naturaleza de las afinidades, que los enteros m_i son independientes del referencial. Esto es de gran utilidad para demostraciones de propiedades puntuales.

Proposición 2.21. *Sean $f, l \in K[X,Y]\backslash K$ con $l(X,Y) = Y - aX - b$. Los enteros m_i definidos en (2-1) son independientes del referencial.*

Demostración. Considere el K-homomorfismo sobreyectivo $\varphi_l : K[X,Y] \longrightarrow K[X]$ tal que $\varphi_l(g) = g_l = g(X, aX+b)$, el cual tiene como kernel al ideal $\langle l\rangle = \langle Y - aX - b\rangle$. Se sigue que

$$K[X,Y]/\langle l\rangle \simeq_{\varphi_l} K[X],$$

por tanto la clase $\overline{f}$ modulo $\langle l\rangle$ corresponde a f_l. Si $f_l(X)$ se factoriza como $c\prod_{i=1}^{d}(X-x_i)^{m_i}$ entonces la factorización de $\overline{f}$ es $c\prod_{i=1}^{d}\overline{(X-x_i)}^{m_i}$, con el mismo número d de factores irreducibles y los mismos m_i, dado que $K[X]$ es un dominio de factorización única.
Veamos que los m_i son independientes del referencial. Sea T una afinidad y $T_\bullet$ el K-automorfismo en $K[X,Y]$, entonces

$$K[X,Y]/\langle l\rangle \simeq_{T_\bullet} K[X,Y]/\langle T_\bullet l\rangle$$
$$f + \langle l\rangle \longrightarrow T_\bullet f + \langle T_\bullet l\rangle$$

se sigue $T_\bullet f + \langle T_\bullet l\rangle$ tiene la misma cantidad d de factores irreducibles, con sus respectivas multiplicidades, que $f + \langle l\rangle$ y por tanto $T_\bullet f$ también, como se quería demostrar. □

Como se ve en el ejemplo 2.20, es posible que para rectas distintas, y una misma curva, el índice de intersección en un punto sea distinto. Sin embargo para casi todas las rectas l que intersectan a una curva $V(f)$ en el punto P, el índice de intersección $(f,l)_P$ es el mismo. Esto lleva a pensar que ese valor es intrínseco de la curva en el punto.

Proposición 2.22. *Sea $f \in K[X,Y]\backslash K$ y $P \in V(f)$. Existe un entero $m \geq 1$ tal que para toda recta l que pasa por P se cumple*

$$(f,l)_P \geq m,$$

además ocurre la desigualdad estricta para mínimo una y máximo m rectas.

Demostración. Sea $f \in K[X,Y]\backslash K$ y $P \in V(f)$. Sin perdida de generalidad, aplicando la proposición 2.21, se supone $P = (0,0)$. Entonces

$$f = f_m + f_{m+1} + \cdots + f_n$$

con f_i homogéneo de grado i y $m \geq 1$. También se puede suponer que $X \nmid f_m$. Por tanto

$$f_X(Y) = f(0,Y) = f_m(0,Y) + \cdots + f_n(0,Y) = Y^m(f_m(0,1) + \cdots + f_n(0,1)Y^{n-m})$$

donde $f(0,1) \neq 0$, entonces $(f,X)_P = m$. Las demás rectas que pasan por P son $l_t = Y - tX$ con $t \in K$, luego

$$f_{l_t}(X) = f(X,tX) = f_m(X,tX) + \cdots + f_n(X,tX) = X^m(f_m(1,t) + \cdots + f_n(1,t)X^{n-m}).$$

Se sigue que $(f,l_t)_P \geq m$, ocurre la igualdad cuando $f_m(1,t) \neq 0$. Como $X \nmid f_m$, entonces $f_m(1,t)$ es un polinomio de grado m en $K[t]$, por tanto se anula en mínimo uno y máximo m valores distintos. □

Definición 2.23. Sea $f \in K[X,Y]\backslash K$. Si $P \in V(f)$ el entero definido en la proposición 2.22 se llama la multiplicidad de P en $V(f)$ y se denota por $m_P(f)$. Si $P \notin V(f)$ se define $m_P(f) = 0$.

Como consecuencia de la demostración de la proposición 2.22 se tiene una manera de encontrar la multiplicidad de un punto $P = (x_0, y_0) \in V(f)$. Para esto se aplica la traslación $T(X,Y) = (X - x_0, Y - y_0)$ tal que $T(P) = O$, por tanto $O \in V(T_\bullet f)$. luego

$$T_\bullet f(X,Y) = f(T^{-1}(X,Y)) = f(X + x_0, Y + y_0) = f_m(X,Y) + \cdots + f_n(X,Y)$$

con f_i homogéneo de grado i, donde $m_P(f) = m \geq 1$. Además se conocen las rectas l tales que $(f,l)_P > m$. Son las imágenes de las componentes de f_m bajo $T_\bullet^{-1}$, para convertirlas al referencial inicial. Como f_m es homogeneo entonces

$$f_m(X,Y) = \prod_{j=1}^{d} (a_j X + b_j Y)^{r_j} \qquad (d \text{ componentes distintas}),$$

después de aplicar $T_\bullet^{-1}$, las rectas $l_j = a_j(X - x_0) + b_j(Y - y_0)$ se llaman *rectas tangentes* a f en P, el exponente r_j se define como la *multiplicidad de la recta tangente* l_j.

Se dice que un punto $P \in V(f)$ es *no singular* o *simple* en f y que f es *no singular* o *simple* en P si $m_P(f) = 1$; en otro caso se dice *singular*. Si $m_P(f) = 2, 3, \ldots, m$ se dice que P es un punto *duplo*, *tripo*,..., *m-uplo*. La curva $V(f)$ es *no singular* o *simple* si $m_P(f) = 1$ para todo $P \in V(f)$. Si f tiene algún punto singular entonces se dice que f es *singular*.

Observación. Si un punto P es no singular en f, entonces existe solo una recta tangente a f en P. No obstante, el reciproco es falso. Por ejemplo $f(X,Y) = (Y - X)^2 + X^3 + Y^4$ tiene solo la recta tangente $l = Y - X$ en $P = (0,0)$ y $m_P(f) = 2$.

Se describió un método para saber si un punto es no singular y encontrar la recta tangente en él, pero esto no es muy eficiente cuando aumenta el grado de la curva. Un mejor método es dado por la siguiente proposición.

Proposición 2.24. *Sean $f \in K[X,Y]\backslash K$ y $P = (x_0, y_0) \in V(f)$.*

(a) *P es no singular si y solo si una de las derivadas parciales f_x, f_y no se anulan en P*

(b) *Si P es no singular entonces la recta tangente a f en P es dada por la ecuación*

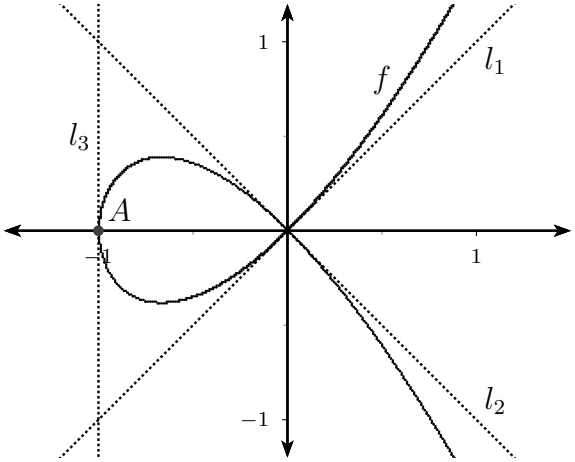
$$f_x(P) \cdot (X - x_0) + f_y(P) \cdot (Y - y_0) = 0.$$

Demostración. Dado que $f \in K[X,Y]\backslash K$ es infinitamente diferenciable, se puede encontrar el polinomio de Taylor en torno a P para cualquier grado, en particular con un residuo de grado mayor o igual a dos. Por tanto

$$\begin{aligned} f(X + x_0, Y + y_0) &= f(x_0, y_0) + f_x(x_0, y_0) \cdot X + f_y(x_0, y_0) \cdot Y + r(X,Y) \\ &= f_x(x_0, y_0) \cdot X + f_y(x_0, y_0) \cdot Y + r(X,Y) \end{aligned}$$

donde todos los términos de $r(X,Y)$ tienen grado mayor o igual a dos. Esto demuestra la proposición. □

Ejemplo 2.25. Sea $f(X,Y) = Y^2 - X^2(X+1)$, por tanto $f_x(X,Y) = -X(3X+2)$ y $f_y(X,Y) = 2Y$. Se sigue que su único punto singular es $O = (0,0)$ con $m_O(f) = 2$ y tiene dos rectas tangentes en O, a saber, $l_1 = Y - X$ y $l_2 = Y + X$. Además $(f, l_1)_O = (f, l_2)_O = 3$.



Considere el punto $A = (-1,0) \in V(f)$, el cual es no singular, la recta tangente a f en A es

$$l_3 = f_x(A) \cdot (X+1) + f_y(A) \cdot Y = -(X+1).$$

Note que l_3 tiene dirección asintótica en común con f y $(f, l_3)_O = 2$.

Proposición 2.26. *Si $f \in K[X,Y] \backslash K$ no tiene componentes múltiples, entonces el conjunto de puntos singulares de f es finito.*

Demostración. Por la proposición 2.24, los puntos P singulares de f cumplen que

$$f(P) = f_x(P) = f_y(P) = 0.$$

Como $f \notin K$, sin perdida de generalidad, suponemos que $f_x \neq 0$. Además $|V(f) \cap V(f_x)|$ es finito, por la proposición 2.11, dado que f no tiene componentes múltiples. □

Como consecuencia de la anterior proposición, toda curva irreducible tiene un numero finito de puntos singulares.

2.5. Índice de intersección

Por la simplicidad de encontrar las intersecciones de una curva con un recta, se logro definir, en ese caso, un índice de intersección. No es tan simple para dos curvas en general. Lo que se va hacer es definir unas propiedades, con sentido geométrico y algebraico, que el índice de intersección de dos curvas en un punto debe cumplir. Además, a partir de esas propiedades se garantiza su unicidad. Antes se deben hacer varias definiciones y lemas.
Se inicia con la generalización de curva para un conjunto algebraico. Sea $S \subseteq K[X_1, \ldots, X_n]$, un subconjunto cualesquier de polinomios, se define

$$V(S) = \{P \in \mathbb{A}^n / \ f(P) = 0, \ \ \forall f \in S\}.$$

Sea $A \subseteq \mathbb{A}^n$, es un *conjunto algebraico afín* o *conjunto algebraico* si existe $S \subseteq K[X_1, \ldots, X_n]$ tal que $A = V(S)$. En el caso de una curva es lo que se llamarán *hiperfícies*, esto es, las generadas por un solo polinomio. Una curva es una hiperfície en el plano $\mathbb{A}^2$. Un conjunto algebraico V se dice *reducible* si $V = V_1 \cup V_2$, con $V_1, \ V_2$ subconjuntos algebraicos distintos de vacío; en otro caso V es *irreducible*.
Para $W \subseteq \mathbb{A}^n$ se define el ideal de los polinomios que se anulan en W,

$$\mathcal{I}(W) = \{f \in K[X_1, \ldots, X_n] / \ f(P) = 0, \ \ \forall P \in W\}.$$

Sean $f, g \in K[X_1, \ldots, X_n]$, I un ideal de $K[X_1, \ldots, X_n]$ y $A \subseteq \mathbb{A}^n$ algebraico. Entones las siguientes propiedades son satisfechas:

- $V(\langle f, g\rangle) = V(f) \cap V(g)$.
- A es irreducible si y solo si $\mathcal{I}(A)$ es primo.
- Si f es irreducible entonces $\mathcal{I}(V(f)) = \langle f\rangle$.
- $\mathcal{I}(V(I)) = \sqrt{I}$ (teorema de los ceros de Hilbert).

Sea $A \subseteq \mathbb{A}^n$ un conjunto algebraico irreducible, se define el *anillo coordenado* de A como $\Gamma(A) = K[X_1, \ldots, X_n]/\mathcal{I}(A)$. Dado que $\mathcal{I}(A)$ es primo, entonces $\Gamma(A)$ es dominio. El cuerpo de fracciones de $\Gamma(A)$ se denota por $K(A)$ y sus elementos se llaman *funciones racionales* en A. Sea $\phi = fg^{-1} \in K(A)$, se dice que ϕ esta definida en $P \in A$ si $g(P) \neq 0$. El conjunto de las funciones racionales de A que están definidas en un punto $P \in A$, define un subanillo de $K(A)$ que se denota por $\mathcal{O}_P(A)$.
Si $A \subseteq \mathbb{A}^n$ conjunto algebraico irreducible y $P \in A$, entonces

- Se cumple que $K \subseteq \Gamma(A) \subseteq \mathcal{O}_P(A) \subseteq K(A)$, como anillos.
- $\Gamma(A) = \cap_{P \in A} \mathcal{O}_P(A)$.
- $\phi \in \mathcal{O}_P(A)$ es unidad si y solo si $\phi(P) \neq 0$.

Observación. Los anillos definidos anteriormente tienen estructura natural de K-espacio vectorial.

Lema 2.27. *Sea I un ideal de $K[X,Y]$, entonces $V(I)$ es finito si y solo si $K[X,Y]/I$ es un K-espacio vectorial finito dimensional.*

Demostración. ($\Rightarrow$) Suponga $V(I) = \{P_1, P_2, \ldots, P_r\}$ con $r \in \mathbb{N}$ y $P_i = (a_i, b_i)$. Defina $f = \prod_{i=1}^{r}(X - a_i)$ y $g = \prod_{i=1}^{r}(Y - b_i)$. Como $f, g \in \mathcal{I}(V(I)) = \sqrt{I}$, entonces existe $N \in \mathbb{N}$ tal que $f^N, g^N \in I$. luego $\overline{f}^N = \overline{g}^N = \overline{0}$ en $K[X,Y]/I$, por tanto $\overline{X}^{rN}$ y $\overline{Y}^{rN}$ se escriben como combinación lineal de $\overline{1}$, $\overline{X}$, $\ldots$, $\overline{X}^{rN-1}$ y $\overline{1}$, $\overline{Y}$, $\ldots$, $\overline{Y}^{rN-1}$ respectivamente. Se sigue que el conjunto $\{\overline{1}, \overline{X}, \overline{Y}, \ldots, \overline{X}^{rN-1}, \overline{Y}^{rN-1}\}$ genera a $K[X,Y]/I$ como K-espacio vectorial.

($\Leftarrow$) Suponga $\dim_K(K[X,Y]/I) < \infty$. Sean $P_1, P_2, \ldots, P_r \in V(I)$ y $f_1, f_2, \ldots, f_r \in K[X,Y]$ tales que $f_j(P_i) = 0$ si $i \neq j$ y $f_i(P_i) = 1$. Para $\lambda_i \in K$ suponga $\sum_{i=1}^{r} \lambda_i \overline{f_i} = \overline{0}$, entonces $\sum_{i=1}^{r} \lambda_i f_i \in I$, por tanto $0 = (\sum_{i=1}^{r} \lambda_i f_i)(P_j) = \lambda_j$ para $j = 1, 2, \ldots, r$. Se sigue que los $\overline{f_i}$ son linealmente independientes, entonces $r \leq \dim_K(K[X,Y]/I) < \infty$. □

Lema 2.28. *Sea I un ideal de $K[X,Y]$, suponga $V(I) = \{P_1, P_2, \ldots, P_n\}$ finito. Entonces existe un isomorfismo natural de $K[X,Y]/I$ con $\prod_{i=1}^{n}(\mathcal{O}_{P_i}(\mathbb{A}^2)/I\mathcal{O}_{P_i}(\mathbb{A}^2))$. En particular $dim_K(K[X,Y]/I) = \sum_{i=1}^{n} dim_K(\mathcal{O}_{P_i}(\mathbb{A}^2)/I\mathcal{O}_{P_i}(\mathbb{A}^2))$.*

Lema 2.29. *Sea $h \in K[X,Y]\backslash K$ irreducible y $P \in V(h)$, entonces*

$$\mathcal{O}_P(\mathbb{A}^2)/\langle h\rangle\mathcal{O}_P(\mathbb{A}^2) \simeq_K \mathcal{O}_P(V(h))$$

Demostración. Aplicando el primer teorema de isomorfismos a

$$\begin{aligned} \varphi : \mathcal{O}_P(\mathbb{A}^2) &\longrightarrow \mathcal{O}_P(V(h)) \\ \frac{f}{g} &\longmapsto \frac{f + \langle h\rangle}{g + \langle h\rangle}, \end{aligned}$$

dado que $\mathrm{Ker}(\varphi) = \langle h\rangle\mathcal{O}_P(\mathbb{A}^2)$, se demuestra el corolario. □

Definición 2.30. Sean $q, f, g \in K[X,Y]\backslash K$ tal que $q|f$ y $P \in V(f)$, se dice que q *atraviesa* por P si $P \in V(q)$ y que f, g se *intersectan propiamente* en P si f y g no tienen componentes en común que atraviesen por P.

Sean $f, g \in K[X,Y]\backslash K$ y $P \in \mathbb{A}^2$, el *índice de intersección* o *multiplicidad* de f y g en P, denotado por $(f,g)_P$, satisface las siguientes propiedades:

1. Si f, g se intersectan propiamente en P entonces $(f,g)_P$ es un entero no negativo. Si f, g no se intersectan propiamente en P entonces $(f,g)_P = \infty$. Además $(f,g)_P = 0$ si y solo si $P \notin V(f) \cap V(g)$.

2. El índice $(f,g)_P$ solo depende de las componentes de f y g que atraviesan por P.

3. Si T es una afinidad y $T(P) = Q$ entones $(f, g)_P = (T_\bullet f, T_\bullet g)_Q$.
4. $(f, g)_P = (g, f)_P$.
5. Si $f = \prod_i^d f_i^{r_i}$ y $g = \prod_j^e s_j^{s_j}$ entonces $(f, g)_P = \sum_{i=1}^d \sum_{j=1}^e r_i s_j (f_i, g_j)_P$.
6. $(f, g)_P = (f, g + hf)_P$ para todo $h \in K[X, Y]$.
7. $(f, g)_P \geq m_P(f) m_P(g)$, ocurre la igualdad si y solo si f y g no tienen rectas tangentes en P en común.

Teorema 2.31. *Sean $f, g \in K[X, Y]$ y $P \in \mathbb{A}^2$. Existe un único entero $(f, g)_P$ que satisface las propiedades $1 - 7$, el cual es dado por*

$$(f, g)_P = dim_K(\mathcal{O}_P(\mathbb{A}^2)/\langle f, g\rangle \mathcal{O}_P(\mathbb{A}^2)). \tag{2-2}$$

Demostración. **Existencia**: defina $(f, g)_P$ como en (2-2). Las propiedades 4 y 6 se cumplen porque $\langle f, g\rangle \mathcal{O}_P(\mathbb{A}^2) = \langle g, f\rangle \mathcal{O}_P(\mathbb{A}^2)$ y $\langle f, g\rangle \mathcal{O}_P(\mathbb{A}^2) = \langle f, g + hf\rangle \mathcal{O}_P(\mathbb{A}^2)$, respectivamente.

Suponga que $f = v_P v$ y $g = u_P u$, donde v_P y u_P son el producto de las componentes que atraviesan por P de f y g, respectivamente. Como $v(P) \cdot u(P) \neq 0$ entonces v y u son unidades en $\mathcal{O}_P(\mathbb{A}^2)$, por tanto $\langle f\rangle = \langle v_P\rangle$ y $\langle g\rangle = \langle u_P\rangle$. luego $\langle f, g\rangle = \langle v_P, u_P\rangle$. Esto demuestra la propiedad 2.

Sea T una afinidad con $T(P) = Q$, entonces $\widetilde{T} : \mathcal{O}_P(\mathbb{A}^2) \longrightarrow \mathcal{O}_Q(\mathbb{A}^2)$ tal que $\widetilde{T}(\phi) = \phi \circ T^{-1}$ es un K-homomorfismo de espacios vectoriales, además $\widetilde{T^{-1}} : \mathcal{O}_Q(\mathbb{A}^2) \longrightarrow \mathcal{O}_P(\mathbb{A}^2)$ definido de manera análoga a $\widetilde{T}$, es inversa a izquierda y derecha de $\widetilde{T}$. Por tanto $\widetilde{T}$ es K-isomorfismo, luego

$$\mathcal{O}_P(\mathbb{A}^2)/\langle f, g\rangle \mathcal{O}_P(\mathbb{A}^2) \simeq_K \mathcal{O}_Q(\mathbb{A}^2)/\langle f \circ T^{-1}, g \circ T^{-1}\rangle \mathcal{O}_Q(\mathbb{A}^2),$$

entonces $(f, g)_P = (T_\bullet f, T_\bullet g)_Q$ (propiedad 3).
Aplicando las propiedades 2 y 3 se puede suponer que $P = (0, 0)$ y que todas las componentes de f y g atraviesan por P. Veamos que se cumple la propiedad 1.

Suponga que f, g se intersectan propiamente en P. Como todas las componentes de f y g atraviesan a P entonces no tienen componentes en común y por la proposición 2.11 se sigue que $V(\langle f, g\rangle) = |V(f) \cap V(g)|$ es finito. Luego, por los lemas 2.27 y 2.28 se tiene que $(f, g)_P$ es finito. Ahora, suponga que f y g tienen componente irreducible común h, entonces $\langle f, g\rangle \subseteq \langle h\rangle$, por tanto existe un K-homomorfismo sobreyectivo de $\mathcal{O}_P(\mathbb{A}^2)/\langle f, g\rangle \mathcal{O}_P(\mathbb{A}^2)$ a $\mathcal{O}_P(\mathbb{A}^2)/\langle h\rangle \mathcal{O}_P(\mathbb{A}^2)$. Entonces $\dim_K(\mathcal{O}_P(\mathbb{A}^2)/\langle h\rangle \mathcal{O}_P(\mathbb{A}^2)) \leq (f, g)_P$. Por definición se tiene que $\Gamma(V(h)) \subseteq \mathcal{O}_P(V(h))$, además $\Gamma(V(h))$ es K-espacio de dimensión infinita, por el lema 2.29 se sigue que $(f, g)_P = \infty$. Por último $P \notin V(f) \cap V(g)$ si y solo si alguno, f o g, es unidad en $\mathcal{O}_P(\mathbb{A}^2)$, lo cual equivale a $\langle f, g\rangle = \mathcal{O}_P(\mathbb{A}^2)$ y $(f, g)_P = 0$.

Para la propiedad 6 es suficiente demostrar que $(f, gh)_P = (f, g)_P + (f, h)_P$ para cualquier $f, g, h \in K[X, Y]$. Sin perdida de generalidad suponga que f y gh no tienen componentes en

común. Como $\langle f, gh\rangle \subseteq \langle f, g\rangle$, sea $\varphi : \mathcal{O}_P(\mathbb{A}^2)/\langle f, gh\rangle\mathcal{O}_P(\mathbb{A}^2) \longrightarrow \mathcal{O}_P(\mathbb{A}^2)/\langle f, g\rangle\mathcal{O}_P(\mathbb{A}^2)$ el K-homomorfismo natural sobreyectivo.
Defina el K-homomorfismo $\psi : \mathcal{O}_P(\mathbb{A}^2)/\langle f, h\rangle\mathcal{O}_P(\mathbb{A}^2) \longrightarrow \mathcal{O}_P(\mathbb{A}^2)/\langle f, gh\rangle\mathcal{O}_P(\mathbb{A}^2)$ tal que $\psi(\overline{\phi}) = \overline{g\phi}$ para $\phi \in \mathcal{O}_P(\mathbb{A}^2)$. Veamos la siguiente secuencia es exacta

$$0 \to \mathcal{O}_P(\mathbb{A}^2)/\langle f, h\rangle\mathcal{O}_P(\mathbb{A}^2) \xrightarrow{\psi} \mathcal{O}_P(\mathbb{A}^2)/\langle f, gh\rangle\mathcal{O}_P(\mathbb{A}^2) \xrightarrow{\varphi} \mathcal{O}_P(\mathbb{A}^2)/\langle f, g\rangle\mathcal{O}_P(\mathbb{A}^2) \to 0$$

ψ es inyectiva: sea $\phi \in \mathcal{O}_P(\mathbb{A}^2)$ tal que $\psi(\overline{\phi}) = 0$, entones $g\phi = uf + vgh$ con $u, v \in \mathcal{O}_P(\mathbb{A}^2)$. Considere $s \in K[X, Y]$ tal que $s(P) \neq 0,\ su = a,\ sv = b$ y $s\phi = c$ con $a, b, c \in K[X, Y]$, luego $g(c - bh) = gs\phi - gsvh = s(g\phi - vgh) = s(g\phi + uf - g\phi) = suf = af \in K[X, Y]$. Como f y g no tienen factores en común, existe $d \in K[X, Y]$ tal que $c - bh = df$, entonces al dividir por s^{-1} se tiene que $s^{-1}bh + s^{-1}df = s^{-1}c = \phi$, por tanto $\overline{\phi} = 0$ en $\mathcal{O}_P(\mathbb{A}^2)/\langle f, h\rangle\mathcal{O}_P(\mathbb{A}^2)$. Solo falta probar que Im(ψ) =Ker(φ), lo cual es inmediato de las definiciones de ψ y φ. Por la exactitud de la secuencia se tiene que

$$\dim_K(\mathcal{O}_P(\mathbb{A}^2)/\langle f, gh\rangle\mathcal{O}_P(\mathbb{A}^2)) = \dim_K(\mathcal{O}_P(\mathbb{A}^2)/\langle f, g\rangle\mathcal{O}_P(\mathbb{A}^2)) + \dim_K(\mathcal{O}_P(\mathbb{A}^2)/\langle f, h\rangle\mathcal{O}_P(\mathbb{A}^2))$$
$$(f, gh)_P = (f, g)_P + (f, h)_P$$

Unicidad: se utiliza inducción y se describe un procedimiento que a partir de las propiedades implica la unicidad.
Por las propiedades 3 y 1 se supone $P = (0, 0)$ y $(f, g)_P$ finito. El paso base $(f, g)_P = 0$ es demostrado por la propiedad 1. Por inducción, suponga $(f, g)_P = n > 0$ y que $(a, b)_P$, con $a, b \in K[X, Y]$, puede ser calculado cuando $(a, b)_P < n$.
Sean $f(X, 0), g(X, 0) \in K[X]$ de grados $r,\ s$, respectivamente, con $r \leq s$.
Caso 1: si $r = 0$, entonces f=Yh para algún $h \in K[X, Y]$. Aplicando la propiedad 5,

$$(f, g)_P = (Y, g)_P + (h, g)_P.$$

Como $Y \nmid g$, propiedad 1, entonces $g(X, 0) = X^m(a_0 + a_1X + \cdots + aX^{r-m})$ con $a_0 \neq 0$ y $m > 0$. Note que $\langle Y, g\rangle = \langle Y, g(X, 0)\rangle$, por tanto $(Y, g)_P = (Y, g(X, 0))_P$. Luego, por las propiedades 2, 5 y se 7, respectivamente, $(Y, g(X, 0))_P = (Y, X^m)_P = m(Y, X)_P = m$. Dado que $m > 0$, entones $(h, g)_P < n$ y se obtiene por la hipótesis de inducción.
Caso 2: $r > 0$. Se supone $f(X, 0)$ y $g(X, 0)$ mónicos. Sea $h = g - X^{s-r}f$, por la propiedad 6, se tiene que $(f, g)_p = (f, h)_P$. Note que $\mathrm{d}^\circ h(X, 0) = t < s$. Repitiendo este proceso un número finito de veces, intercambiando f y h cuando $t < r$, se tendrá dos polinomios $a, b \in K[X, Y]$ tal que $(f, g)_P = (a, b)_p$ con $\mathrm{d}^\circ a(X, 0) \cdot \mathrm{d}^\circ b(X, 0) = 0$, que corresponde al caso 1. □

Note que los valores de $(f, l)_P$, cuando l es una recta, según la definición del teorema 2.31 coinciden con la definición 2.19.

Ejemplo 2.32. Sean $f(X, Y) = X^2Y + X^3 + Y^3 + Y$, $g(X, Y) = X^2Y + Y^3 + X$ y considere el punto $P = (0, 0) \in V(f) \cap V(g)$. Utilizando las propiedades del índice de intersección

y el procedimiento descrito en la parte de unicidad del teorema anterior se calcula $(f,g)_P$. Como $f(X,0) = X^3$ y $g(X,0) = X$, se define $h(X,Y) = f(X,Y) - X^2 g(X,Y)$ donde $h(X,0) = X^3 - X^2 \cdot X = 0$. Luego $h(X,Y) = Y(Y^2X - Y^2X^2 - X^2 + X^2 + 1)$, entonces

$$\begin{aligned}(f,g)_P = (h,g)_P &= (Y, X^2Y + Y^3 + X)_P + (Y^2X - Y^2X^2 - X^2 + X^2 + 1, X^2Y + Y^3 + X)_P \\ &= (Y,X)_P + 0 \\ &= 1\end{aligned}$$

3. Curvas algebraicas proyectivas

En varios ejemplos sobre intersección de curvas, cuando se tenía dirección asintótica en común, el grado de la resultante era menor que el producto de sus grados. Esto se puede interpretar, como si algunas intersecciones se "perdían" en el infinito. Entonces si cambiamos el plano afín por un conjunto que también contenga estos en el infinito, veremos que esas intersecciones aparecerán naturalmente.

3.1. Introducción

Considere el espacio afín $\mathbb{A}^3(K)$ sin el punto $(0,0,0)$, lo denotamos por $\mathbb{A}^3(K)^*$. Se define la relación $\sim$ en $\mathbb{A}^3(K)^*$ como

$$(x,y,z) \sim (x',y',z') \Longleftrightarrow \exists_{t\in K}(\ (x,y,z) = (tx',ty',tz')\ ),$$

claramente $\sim$ es una relación de equivalencia, esto da sentido a la siguiente definición.

Definición 3.1. El *plano proyectivo* $\mathbb{P}^2(K)$, o simplemente $\mathbb{P}^2$, es el conjunto de clases de equivalencia en $\mathbb{A}^3(K)$ módulo $\sim$. La clase de equivalencia de un punto $(x,y,z) \in \mathbb{A}^3(K)^*$ se denota por $(x:y:z)$.

Se dice que a, b, c son unas *coordenadas homogéneas* del punto $(x:y:z) \in \mathbb{P}^2$, relativas a la base $\mathcal{B} = \{w_1, w_2, w_3\}$ de K^3, si existe $t \in K$ tal que $(x,y,z) = (ta, tb, tc)$ en la base $\mathcal{B}$. Note que un punto $(x:y:z)$ de $\mathbb{P}^2(K)$, visto en K^3 es la recta que pasa por el origen, sin contenerlo, y por (x,y,z).
Los puntos $(x:y:z)$ con $z \neq 0$ están en correspondencia biunívoca con el plano π de ecuación $Z = 1$ en K^3, ver figura 2.1. En efecto, pues tienen un representante en el plano π, ya que

$$(x:y:z) = \left(\frac{x}{z} : \frac{y}{z} : 1\right) \Longleftrightarrow \exists_{t\in K}\left(\ (x,y,z) = \left(t\frac{x}{z}, t\frac{y}{z}, t\right)\ \right),$$

y claramente $t = z$ cumple la condición. El plano afín $\mathbb{A}^2$ se puede identificar con el plano π, bajo la biyección

$$\begin{aligned} \mathbb{A}^2 &\longrightarrow \pi \subseteq \mathbb{P}^2 \\ (x,y) &\longmapsto (x:y:1), \end{aligned}$$

por esta correspondencia se dice que $\mathbb{A}^2 \subseteq \mathbb{P}^2$. Los elementos de π se dicen que están a *distancia finita* y los de $\mathbb{P}^2 \backslash \pi$ se llaman *puntos en el infinito* o que están a *distancia infinita*, son de la forma $(x:y:0)$ con x o y no nulo.

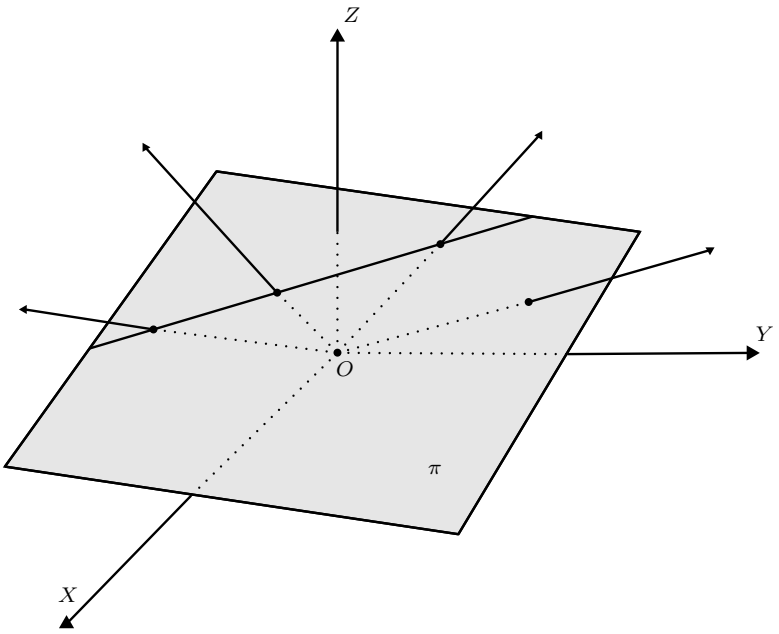


Figura 2.1

Veamos para cuales polinomios f el conjunto solución de $f = 0$, esta contenido en el plano proyectivo. Se debe considerar polinomio de tres variables, entonces $f \in K[X, Y, Z]$. Además, para que un punto $(x : y : z) \in \mathbb{P}^2$ se pueda interpretar como solución de $f = 0$, se debe cumplir que todos los representantes de $(x : y : z)$ son solución. Esto se cumple si f es homogéneo, de grado n, ya que

$$f(tx, ty, yz) = t^n f(x, y, z) \qquad \forall_{t \in K},$$

se tiene entonces a la siguiente definición.

Definición 3.2. Sea F un polinomio homegéneo en $K[X, Y, Z]\backslash K$. La *curva proyectiva* $V_K(F)$, o simplemente $V(F)$, se define como

$$V_K(F) = \left\{(x : y : z) \in \mathbb{P}^2(K)/F(x, y, z) = 0\right\}.$$

Como en el caso de curvas afines, se tiene definiciones similares para *curva proyectiva irreducible*, *grado de una curva proyectiva*, *componente irreducible* y *multiplicidad de componente*.

Observación. Se puede hablar de componente irreducible en curvas proyectivas, dado que todos los factores de un polinomio homogéneo son homogéneos.

Ejemplo 3.3. Las *rectas proyectivas*, polinomios homogéneos de grado 1, son de la forma $aX + bY + cZ$. Vistas en K^3, son planos que pasan por el origen. En $\mathbb{P}^2(K)$ están compuestas por una recta de la forma $aX + bY + c$ en el plano π (ver figura 2.1) y un punto en el infinito dado por $(b : -a : 0)$. Además, como dos planos diferentes en K^3 que pasan por el origen siempre se intersectan en una recta que pasa por el origen, esto se traduce en que dos rectas proyectivas diferentes siempre se intersectan en un punto.

Dado que $\mathbb{A}^2 \subset \mathbb{P}^2$, veamos como se relacionan las curvas afines con las curvas proyectivas. Sea $f \in K[X,Y]\backslash K$ de grado n tal que $f = f_0 + f_1 + \cdots + f_n$, donde f_i es homogéneo de grado i. Se define la homogenización de f con respecto a Z, como

$$f^*(X,Y,Z) = Z^n f_0(X,Y) + Z^{n-1} f_1(X,Y) + \cdots + Z f_{n-1}(X,Y) + f_n(X,Y),$$

f^* es un polinomio homogéneo de grado n, entonces $V(f^*)$ es una curva proyectiva. Además, existe una biyección natural entre $V(f)$ y los puntos a una distancia finita de $V(f^*)$

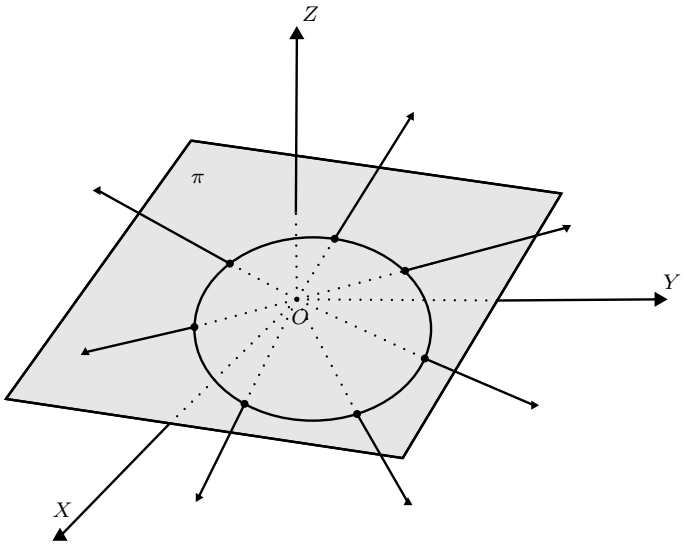
$$\begin{aligned} V(f) &\longrightarrow \pi \cap V(f^*) \\ (x,y) &\longmapsto (x:y:1). \end{aligned}$$

De ahora en adelante se considera $V(f)$ como la parte que está a una distancia finita de la curva proyectiva $V(f^*)$.

Ejemplo 3.4. Sea $K = \mathbb{R}$. Si $f(X,Y) = 5(X-2)^2 + 3(X-2)^2 - 15$, entonces $V(f)$ se considera como la parte a una distancia finita de la curva proyectiva

$$f^*(X,Y,Z) = 5(X-2Z)^2 + 3(X-2Z)^2 - 15Z^2$$

y su gráfico es



Por facilidad, se seguirá graficando en $\mathbb{R}^2$.

Note que los puntos de $V(f^*)\backslash V(f)$, es decir, los puntos en el infinito de $V(f^*)$, están es correspondencia con las direcciones asintóticas de f. En efecto, ya que

$$f^*(X,Y,0) = f_n(X,Y) = \prod_{i=1}^{d} (b_i X - a_i Y)^{r_i}$$

donde d es el número de direcciones asintóticas diferentes de f. Esto muestra que si dos curvas no tienen direcciones asintóticas en común si y solo si no se intersectan en el infinito, por tanto todas sus intersecciones están en $\mathbb{A}^2$. Como garantiza la proposición 2.17.

Se define el proceso inverso a la homogenización. Sea $F \in K[X,Y,Z]\backslash K$ homogéneo, entonces la deshomogenización de F respecto a Z es

$$F_*(X,Y) = F(X,Y,1),$$

es decir, $V(F_*)$ son los puntos a una distancia finita de $V(F)$. Se cumplen las propiedades:

- $(fg)^* = f^*g^*$.
- $(FG)_* = F_*G_*$.
- $(f^*)_* = f$.
- Si $r = \mathrm{d}^\circ F - \mathrm{d}^\circ F_*$ entones $Z^r(F_*)^* = F$.

Observación. Haber escogido el plano $Z = 1$ en K^3 para definir los puntos a una distancia finita e infinita, no es una elección relevante. Lo visto en esta sección se puede definir de manera análoga con los planos $X = 1$ o $Y = 1$, lo cual a veces resulta mas conveniente. Además, realizando un procedimiento similar en K^2 y K^{n+1}, al que se hizo para definir $\mathbb{P}^2$ a partir de K^3, se puede definir la recta proyectiva $\mathbb{P}$ y el espacio proyectivo $\mathbb{P}^n$.

Proposición 3.5. *Sean $V(F)$, $V(G)$ curvas proyectivas. Si F, G no tiene componentes en común entonces $|V(F) \cap V(G)|$ es finito.*

Demostración. Si F, G no tienen factor común en $K[X,Y,Z]$ entonces F_*, G_* no tienen factor común en $K[X,Y]$. Por tanto $V(F), V(G)$ tienen intersecciones finitas a una distancia finita. Como Z no puede dividir a F y G a la vez, entonces $|V(Z) \cap V(F)|$ o $|V(Z) \cap V(G)|$ es finito. Por tanto $|V(F) \cap V(G)|$ es finito. □

Note que la anterior proposición nos garantiza la finitud de la intersección de dos curva con unas condiciones, pero no afirma que tal intersección es no vacia. Esto es consecuencia inmediata del teorema de Bézout.

3.2. Cambio de coordenadas proyectivas

Los puntos de $\mathbb{P}^2(K)$ se pueden ver como rectas en K^3 que pasan por el origen o subespacios de dimensión uno, para definir un cambio de coordenadas en el plano proyectivo, es necesario una aplicación que envíe subespacios de dimensión uno en subespacios de dimensión uno. Las aplicaciones con esa propiedad, en espacios de dimensión finita, son equivalentes a isomorfismos lineales. Recuerde que los isomorfismos lineales efectúan un cambio de base o

coordenadas, si se define previamente una base para el dominio. Cuando no se especifique la base, se toma la base canónica.
Sea $T_1 : K^3 \to K^3$ un isomorfismo K-lineal. Luego, T_1 induce una biyección $T_2 : \mathbb{P}^2 \to \mathbb{P}^2$ tal que si $P = (x : y : z) \in \mathbb{P}^2$ entonces

$$T_2(P) = (a : b : c), \text{ donde } T_1(x, y, z) = (a, b, c).$$

La biyección T_2 esta bien definida como consecuencia de la linealidad de T_1.
Por conveniencia las dos aplicaciones definidas anteriormente las vamos a denotar por T, para la siguiente definición.

Definición 3.6. Sea $T : K^3 \to K^3$ un isomorfismo lineal. La biyección $T : \mathbb{P}^2 \to \mathbb{P}^2$, definida anteriormente, se llama *proyectividad* o *cambio de coordenadas proyectivas* en $\mathbb{P}^2$.

A todo isomorfismo K-lineal $T : K^3 \to K^3$ le corresponde un matriz de orden tres $A = (a_{ij})$ con $\det(A) \neq 0$ tal que $T(v) = Av^t$ para todo $v \in K^3$. Por tanto, si $v = (x, y, z)$ entonces

$$T(v) = (a_{11}x + a_{12}y + a_{13}z, a_{21}x + a_{22}y + a_{23}z, a_{31}x + a_{32}y + a_{33}z).$$

Si x, y, z fueran variables, las coordenadas de $T(v)$ serian polinomios homogéneos de grado uno. Entonces se puede definir un K-isomorfismo

$$\begin{aligned} T_\bullet : K[X, Y, Z] &\longrightarrow K[X, Y, Z] \\ F(X, Y, Z) &\longrightarrow F(T^{-1}(X, Y, Z)) \end{aligned}$$

inducido por T, tal que deja invariante el conjunto de polinomios homogéneo, es decir, envía curvas proyectivas en curvas proyectivas. Mas específicamente, si (b_{ij}) es la matriz asociada a T^{-1} entonces

$$(T_\bullet F)(X, Y, Z) = F(b_{11}X + b_{12}Y + b_{13}Z, b_{21}X + b_{22}Y + b_{23}Z, b_{31}X + b_{32}Y + b_{33}Z).$$

Observación. Cuando se considera el polinomio $T_\bullet F$, T representa la aplicación K-lineal definida en K^3. Pero cuando se considera la curva proyectiva $V(T_\bullet F)$, T representa la biyección definida en $\mathbb{P}^2$.

Definición 3.7. Dos curvas $V(F), V(G)$ se dicen *congruentes* si existe una proyectividad T tal que $T_\bullet F = G$. Una propiedad $\mathcal{P}$ es *invariante* o *independiente de coordenadas* si, para toda proyectividad T, una curva $V(F)$ (o $\mathcal{C}$ conjunto de curvas o puntos) satisface $\mathcal{P}$ si y solo si $V(T_\bullet F)$ (respectivamente $T_\bullet(\mathcal{C})$) satisface $\mathcal{P}$.

Las siguientes propiedades son invariantes:

- Grado de una curva. Es decir, si F tiene grado n entonces $T_\bullet F$ tiene grado n.
- Reducibilidad de una curva.
- La propiedad de que un conjunto de curvas se intersectan.
- Colinealidad de puntos.

3.3. Multiplicidad

Sea $V(F)$ curva proyectiva de grado n y una recta $V(L)$. Supongamos en principio que $L = X$, entonces $P = (x : y : z) \in V(X) \cap V(F)$ si y solo si $x = 0$ y $F(0, y, z) = 0$. El polinomio $F(0, Y, Z)$ es idénticamente nulo, si $X|F$, o es un polinomio homogéneo de grado n, en ese caso se tiene que

$$F(0, Y, Z) = \prod_{i=1}^{d} (c_i Y - b_i Z)^{m_i}$$

donde los puntos $P_i = (0 : b_i : c_i)$ son distintos dos a dos y $\sum_{i=1}^{d} m_i = n$. Este caso particular será la base para el caso general, con ayuda de las proyectividades. Ahora, se puede definir, como en el plano afín, el indice de intersección entre una curva y una recta.

Proposición 3.8. *Sea $V(L)$ un recta y $V(F)$ una curva de grado n. Si $L \nmid F$ entonces*

$$V(L) \cap V(F) = \{P_1, \ldots, P_d\}$$

donde los P_i son distintos y existen enteros m_i tal que para toda proyectividad T donde $T_\bullet L = X$, se cumple que

$$(T_\bullet F)(0, Y, Z) = \prod_{i=1}^{d} (c_i Y - b_i Z)^{m_i}$$

con $T(P_i) = (0 : b_i : c_i)$ para $i = 1, \ldots, d$. En particular $\sum_{i=1}^{d} m_i = n$.

Demostración. Sea T una proyectividad tal que $T_\bullet L = X$. El K-isomorfismo $T_\bullet$ induce un isomorfismo de $K[X, Y, Z]/\langle L\rangle$ a $K[Y, Z]$, ya que $K[X, Y, Z]/\langle X\rangle \simeq K[Y, Z]$, y lo denotamos por $\overline{T_\bullet}$. Entonces el siguiente diagrama conmuta

$$\begin{array}{ccc} K[X,Y,Z] & \xrightarrow{T_\bullet} & K[X,Y,Z] \\ \varphi \downarrow & & \downarrow \psi \\ K[X,Y,Z]/\langle L\rangle & \xrightarrow{\overline{T_\bullet}} & K[Y,Z] \end{array}$$

donde φ es el homomorfismo canónico y $\psi(G) = G(0, Y, Z)$ para todo $G \in K[X, Y, Z]$. Se sigue que $K[X, Y, Z]/\langle L\rangle$ es un dominio de factorización única, por tanto $\varphi(F) = \overline{F}$ se escribe como

$$\overline{F} = \overline{H_1}^{m_1} \cdots \overline{H_d}^{m_d}$$

donde los H_i son irreducibles distintos dos a dos. Por la conmutatividad del diagrama se tiene que

$$\overline{F}(\overline{0}, \overline{Y}, \overline{Z}) = \overline{T_\bullet}\varphi(F) = \psi(T_\bullet F) = (T_\bullet F)(0, Y, Z)$$

como $L \nmid F$ entonces $X \nmid T_\bullet F$, por tanto $(T_\bullet F)(0, Y, Z)$ es homogéneo de grado n. Luego

$$(T_\bullet F)(0, Y, Z) = \prod_{j=1}^{r} (c_j Y - b_j Z)^{n_j},$$

con $c_jY - b_jZ$ distintos dos a dos y $\sum_{j=1}^{r} n_i = n$. Comparando las factorizaciones de $\overline{F}(\overline{0}, \overline{Y}, \overline{Z})$ y $(T_\bullet F)(0, Y, Z)$, se tiene que $r = d$ y $n_i = m_i$, en algún orden, como se querá demostrar. Los resultados sobre los puntos de $V(L) \cap V(F)$ son inmediatos como consecuencia de la prueba de lo anterior. □

De manera análoga al caso afín se tiene la siguiente definición.

Definición 3.9. La *multiplicidad* o *índice de intersección* de F y con una recta L en un punto P, se define como

$$(F, L)_P = \begin{cases} 0 & \text{si} \quad P \notin V(F) \cap V(L) \\ \infty & \text{si} \quad P \in V(L) \subseteq V(F) \\ m_i & \text{si} \quad P = P_i, \text{ definidos en la proposición 3.8.} \end{cases}$$

Por esta definición y la proposición 3.8 se considera que una recta y una curva de grado n se intersectan, contando sus multiplicidades, es n puntos. Esto es un caso particular del teorema de Bézout. Otra consecuencia de la proposición 3.8, es que se puede suponer que un punto $P \in V(F) \cap V(L)$, bajo una proyetividad, esta a una distancia finita y por tanto

$$(F, L)_P = (F_*, L_*)_P, \tag{3-1}$$

tal que si $P = (x : y : z)$ en el primer miembro de la igualdad, entonces $P = (x, y)$ en el segundo. Con ayuda de esta relación se define la multiplicidad de un punto en una curva proyectiva.

Proposición 3.10. *Sean $V(F)$ curva proyectiva y $P \in V(F)$. Existe un entero $m \geq 1$ tal que para toda recta $V(L)$ que pasa por P se cumple*

$$(F, L)_P \geq m,$$

además ocurre la desigualdad estricta para mínimo una y máximo m rectas.

Demostración. Sin perdida de generalidad se supone que P esta a una distancia finita. Por la igualdad 3-1 y la proposición 2.22, la análoga para el caso afín, se sigue el resultado. □

Definición 3.11. Sea $V(F)$ curva proyectiva. Si $P \in V(F)$ el entero definido en la proposición 3.10 se llama la multiplicidad de P en F y se denota por $m_P(F)$. Si $P \notin V(F)$ se define $m_P(F) = 0$.

Como en el caso de curvas afines, se tiene definiciones similares para punto *no singular o simple*, *singular* y *m-uplo* dependiendo del valor de $m_P(F)$. También definiciones para *curvas proyectivas no singulares o simples*, *rectas tangentes*, etc.

Ejemplo 3.12. Sea $F = YZ^2 - X^3$. Al deshomogenizar respecto a Z se tiene $f_* = Y - X^3$, luego $V(f_*)$ es una curva no singular, ya que $(f_*)_y = 1$. Por tanto $m(F)_p = 1$ para todo $P = (a : b : 1) \in V(F)$. Como f_* solo tiene una dirección asintótica, entonces $V(F)$ solo tiene el punto $P = (0 : 1 : 0)$ en el infinito. Para calcular la multiplicidad de P en F se deshomogeniza respecto a Y, la coordenada de P no nula, entonces $f_* = Z^2 - X^3$. Se sigue que $m(F)_P = 2$ y además la recta $V(Z)$ es su única recta tangente, por tanto $(F, L)_P = 2$ para toda recta $L \neq Z$ y $(F, Z)_P = 3$.

Observación. Dado un polinomio $F \in K[X, Y, Z]$ homogéneo de grado n, las derivadas parciales F_x, F_y y F_z son polinomios homogéneos de grado $n-1$. Ya que, por ejemplo, al derivar con respecto a X, los términos que no contienen a X se anulan y los otros disminuyen el grado en uno. Por tanto, las derivadas de curvas proyectivas también definen curvas proyectivas.

Veamos como se encuentran los puntos singulares de una curva y cual es la recta tangente a la curva en un punto simple.

Proposición 3.13. *Sean $F \in K[X, Y, Z]\backslash K$ homogéneo de grado n y $P \in \mathbb{P}^2$. Entonces*

(a) $n \cdot F = X \cdot F_x + Y \cdot F_y + Z \cdot F_z$.

(b) *P es un punto singular de F si y solo si $F_x(P) = F_y(P) = F_z(P) = 0$.*

(c) *Si P es un punto simple de F, entonces la recta tangente F en P es*

$$F_x(P) \cdot X + F_y(P) \cdot Y + F_z(P) \cdot Z.$$

Demostración.

(a) Por la linealidad de las derivadas, es suficiente demostrar la igualdad para los términos de F. Sin contar los coeficientes constantes, los términos de F son de la forma $X^iY^jZ^k$ con $i + j + k = n$. Luego

$$\begin{aligned} X(X^iY^jZ^k)_x + Y(X^iY^jZ^k)_y + Z(X^iY^jZ^k)_z &= iX^iY^jZ^k + jX^iY^jZ^k + kX^iY^jZ^k \\ &= (i + j + k)X^iY^jZ^k \\ &= nX^iY^jZ^k. \end{aligned}$$

(b) Note que las derivadas parciales se comportan bien con la deshomogeneización respecto a variables diferentes, es decir, si se deshomogeniza respecto a Z, entonces

$$\begin{aligned} (F_*)_x &= (F_x)_* \\ (F_*)_y &= (F_y)_*. \end{aligned} \tag{3-2}$$

Supongamos $P = (a : b : 1)$. Por la proposición 2.24, P es punto singular de F si y solo si $(F_*)_x = (F_*)_y = F_* = 0$ en (a, b). Luego, al deshomogeneizar la ecuación del ítem ***(a)*** y aplicar las ecuaciones 3-2 se obtiene que $(F_x)_* = (F_y)_* = (F_z)_* = 0$ en (a, b). Se sigue que $F_x(P) = F_y(P) = F_z(P) = 0$. Análogamente cuando P es de la forma $(a : 1 : c)$ o $(1 : b : c)$.

(c) Suponga $P = (a : b : 1)$. Si se deshomogeniza la recta tangente a F en P, se obtiene la recta l tangente a F_* en (a, b). La proposición 2.24 dice cual es la recta l, luego al homogenizarla se obtiene la recta tangente

$$(F_*)_x(a, b) \cdot (X - aZ) + (F_*)_y(a, b) \cdot (Y - bZ),$$

utilizando las ecuaciones 3-2, el ítem ***(a)*** y el hecho de que $(H)_*(x, y) = H(x, y, 1)$ para todo polinomio homogéneo en $K[X, Y, Z]$, la recta tangente a F en P es

$$F_x(P) \cdot X + F_y(P) \cdot Y + F_z(P) \cdot Z.$$

□

Ejemplo 3.14. Sea $F = Y^2Z - X^3 + X^2Z$. Si $P = (x : y : z) \in \mathbb{P}^2$ es un punto singular, debe cumplir que

$$\begin{aligned} F(P) &= y^2z - x^3 + x^2z = 0 \\ F_x(P) &= 2xz - 3x^2 = 0 \\ F_y(P) &= 2yz = 0 \\ F_z(P) &= y^2 + x^2 = 0. \end{aligned}$$

Entonces el único punto singular de F es $P = (0 : 0 : 1)$. Al deshomogenizar respecto a Z se sigue que $m(F)_P = 2$. Considere $Q = (0 : 1 : 0) \in V(F)$, la recta tangente a F en Q es $F_x(Q) \cdot X + F_y(Q) \cdot Y + F_z(Q) \cdot Z = Z$ la recta infinito y $(F, Z)_Q = 3$.

Se tiene un resultado análogo a la proposición 2.26 y como es de esperar la demostración se reduce al caso afín.

Proposición 3.15. *Si $F \in K[X, Y, Z]$ homogéneo no tiene componentes múltiples, entonces el conjunto de puntos singulares de F es finito.*

3.4. Intersección de curvas

Como vio en el plano proyectivo todo par de rectas se intersectan (ver ejemplo 3.3), algo que no sucede con las rectas paralelas en el plano afín. Ademas, por la proposición 3.8 y la definición, no solo se garantiza que una curva siempre se intersecta con una recta, también se conoce su número de intersecciones. Siguiendo este proceso, veamos lo que pasa para dos curvas en general, con el teorema de Bézout. Pero antes de eso, veamos que la interpretación del conjunto de polinomios homogéneos de un mismo grado, como K-espacio vectorial es de gran utilidad para resultados sobre existencia de curvas que pasan por algunos puntos y para la demostración del teorema de Bézout.

Sea $K_d[X,Y]$ el conjunto de polinomios homogéneos de dos variables de grado d. Claramente $K_d[X,Y]$ tiene estructura de K-espacio vectorial, con la suma usual de polinomios y además el polinomio constante cero es homogéneo de cualquier grado. Sus elementos son de la forma

$$f(X,Y) = \sum_{i=0}^{d} a_i X^{d-i} Y^i$$

entonces $X^d, X^{d-1}Y, \ldots, XY^{d-1}, Y^d$ son base, ya que son linealmente independientes. Por tanto $\dim_K K_d[X,Y] = d+1$.
Veamos ahora que pasa si se agrega otra variable. Claramente $\mathcal{B} = \{X^i Y^j Z^l\}_{i+j+l=d}$ es una base para $K_d[X,Y,Z]$. Para calcular su dimensión se cuentan los elementos de $\mathcal{B}$ con $l = 0, 1, \ldots, d$. Note que los polinomios que acompañan a los elementos de $\mathcal{B}$ con $l = r$ y $0 \leq r \leq d$ son base para $K_{d-r}[X,Y]$, por tanto hay $d-r+1$ elementos de $\mathcal{B}$ con $l = r$. Se sigue que

$$\begin{aligned}
\dim_K K_d[X,Y,Z] &= \sum_{r=0}^{d} (d-r+1) \\
&= d(d+1) - \frac{d(d+1)}{2} + d + 1 \\
&= \frac{(d+1)(d+2)}{2}
\end{aligned}$$

entonces a cada $V(F)$ con $F \in K_d[X,Y,Z]$ le corresponde un punto $(a_1, a_2, \ldots, a_{\frac{(d+1)(d+2)}{2}})$, donde los a's son los coeficientes de la combinación lineal de la base $\mathcal{B}$, ordenados de alguna manera. Además, como $V(tF) = V(F)$ para todo $t \in K$, entonces las curvas proyectivas de grado d están en correspondencia con los puntos $(a_1 : a_2 : \cdots : a_{\frac{(d+1)(d+2)}{2}})$ de $\mathbb{P}^{\frac{d(d+3)}{2}}$.
En el siguiente ejemplo se utiliza lo anterior para probar existencia de curvas que pasan por puntos fijos.

Ejemplo 3.16. Dados $P_1, \ldots, P_5 \in \mathbb{P}^2$ existe al menos una cónica que pasa por ellos. En efecto, las cónicas son los elementos de $K_2[X,Y,Z]$ y una base es dada por $\{X^2, Y^2, Z^2, XY, XZ, YZ\}$, con ese orden al i-esimo elemento lo denotamos por M_i. Luego una cónica representada por $(a_1 : a_2 : \cdots : a_6)$ para por un punto $P \in \mathbb{P}^2$ si

$$\sum_{i=1}^{6} a_i M(P)_i = 0.$$

Por tanto la cónica $(a_1 : a_2 : \cdots : a_6)$ pasa por los cinco puntos si

$$\begin{pmatrix} M_1(P_1) & M_2(P_1) & \cdots & M_6(P_1) \\ M_1(P_2) & M_2(P_2) & \cdots & M_6(P_2) \\ \vdots & & \ddots & \\ M_1(P_5) & M_2(P_5) & \cdots & M_6(P_5) \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_6 \end{pmatrix} = 0$$

La existencia de la cónica se sigue porque la aplicación K-lineal definida por la anterior matriz de 5×6, digamos $A : K^6 \to K^5$, tiene kernel distinto de cero.

Otra consecuencia interesante es que el conjunto de polinomios homogéneos de grado d que pasan por un punto $P \in K^3$, el cual tiene estructura natural de subespacio de $K_d[X, Y, Z]$, forman un hiperplano en $K^{\frac{(d+1)(d+2)}{2}}$. En efecto, siguiendo con la notación del ejemplo anterior, sea M_i con $1 \leq i \leq \frac{(d+1)(d+2)}{2} = N$ los elementos de la base de $K_d[X, Y, Z]$, entonces un polinomio homogéneo, digamos $(x_1, x_2, \ldots, x_N)$, pasan por P si

$$\sum_{i=1}^{N} x_i M_i(P) = 0$$

y esto es la ecuación, con variables los x's, de un hiperplano. Entonces tal subespacio tiene dimensión $N - 1 = \frac{d(d+3)}{2}$.
Generalizando lo anterior, si consideramos r puntos de K^3, el subespacio de $K_d[X, Y, Z]$ de los polinomios que pasan por ellos tiene dimensión mayor o igual a $N - r$. Dado que su representación en K^N, es la intersección de r hiperplanos distintos.

Ejemplo 3.17. Una curva proyectiva de grado d, esta determinada por $d(d-3)/2$ puntos que contiene. En otras palabras, existen $d(d-3)/2$ puntos por los cuales pasa exactamente un curva proyectiva de grado d.

Proposición 3.18. *La condición para que un punto $P \in \mathbb{A}^2$ sea m-uplo de una curva $V(f)$ con $d^\circ f = d$, se expresa por un sistema de $m(m+1)/2$ ecuaciones lineales en los coeficientes de f.*

Demostración. Sea $P = (a, b) \in \mathbb{A}^2$ con $m(f)_P = m$. Entonces $f(X+a, Y+b) = f_m(X, Y) + f_{m+1}(X, Y) + \cdots + f_d(X, Y)$ con f_i homogéneo de grado i, para $m \leq i \leq d$. Por tanto, los coeficientes de los monomios con grado menor que m de $f(X + a, Y + b)$ son iguales a cero. Además esos coeficientes son de la forma

$$p_0(a, b)c_0 + p_1(a, b)c_1 + \cdots + p_{\frac{(d+1)(d+2)}{2}}(a, b)c_{\frac{(d+1)(d+2)}{2}}$$

donde $p_i \in K[X, Y]$ y los c_i son los coeficientes de los términos de f. Note que hay $m(m+1)/2$ monomios de grado menor o igual a $m - 1$. □

Observación. Aunque solo una parte de lo descrito anteriormente, se utiliza en la demostración del siguiente teorema. Lo demás va ser necesario en el próximo capitulo cuando se estudie el genero virtual de una curva.

Retomando con el tema de intersecciones de curvas. Note que no se ha hablado nada sobre el índice de intersección $(F, G)_P$ en el caso de curvas proyectivas. Lo que se va hacer, en realidad se ha hecho a lo largo de todo este capítulo, es pasar al caso afín.

Teorema 3.19 (Bézout)**.** *Sean $V(F)$ y $V(G)$ curvas proyectivas tal que $d^\circ F = m$, $d^\circ G = n$ y no tienen componentes en común. Entonces*

$$\sum_{P\in\mathbb{P}^2} (F,G)_P = m\cdot n$$

Demostración. Como $V(F)\cap V(G)$ es finito, haciendo un cambio de coordenadas, si es necesario, se puede asumir que ninguno de sus puntos está en la recta infinito. Se sigue que $(F,G)_P = (F_*,G_*)_P$. Además, si $P\notin V(F)\cap V(G)$ entonces $(F,G)_P = 0$. Luego

$$\sum_{P\in\mathbb{P}^2} (F,G)_P = \sum_{P\in V(F_*)\cap V(G_*)} (F_*,G_*)_P = \dim_K(K[X,Y]/\langle F_*,G_*\rangle).$$

Se define

$$\Gamma_* = K[X,Y]/\langle F_*,G_*\rangle, \qquad \Gamma = K[X,Y,Z]/\langle F,G\rangle, \qquad R = K[X,Y,Z]$$

y Γ_d (resp. R_d) el K-espacio vectorial de polinomios homogéneos con grado d de Γ (resp. R). Para demostrar el teorema veamos que $\dim_K\Gamma_d = m\cdot n$ y $\dim_K\Gamma_* = \dim_K\Gamma_d$ para algún d.

Paso 1: $\dim_K\Gamma_d = m\cdot n$. Suponga $d\geq m+n$. Defina $\phi: R\to\Gamma$ el homomorfismo natural, $\varphi: R\times R\to R$ tal que $\varphi(A,B) = AF+BG$ y $\psi: R\to R\times R$ donde $\psi(C) = (CG,-CF)$. Dado que F y G no tienen factores en común, es inmediato que la siguiente secuencia es exacta

$$0\to R\xrightarrow{\psi} R\times R\xrightarrow{\varphi} R\xrightarrow{\phi}\Gamma\to 0.$$

Se restringen los homomorfismos a polinomios homogéneos de varios grados y se obtiene la siguiente secuencia exacta

$$0\to R_{d-m-n}\xrightarrow{\psi} R_{d-m}\times R_{d-n}\xrightarrow{\varphi} R_d\xrightarrow{\phi}\Gamma_d\to 0.$$

Entonces

$$\begin{aligned}\dim_K\Gamma_d = &\ \dim_K R_d - \dim_K(R_{d-m}\times R_{d-n}) + \dim_K R_{d-m-n}\\ = &\ \tfrac{(d+1)(d+2)}{2} - \tfrac{(d-m+1)(d-m+2)}{2} - \tfrac{(d-n+1)(d-n+2)}{2} + \tfrac{(d-m-n+1)(d-m-n+2)}{2}\\ = &\ m\cdot n\end{aligned}$$

Paso 2: Si denotemos por H_0 a $H(X,Y,0)$, para $H\in R$. Note que F_0 y G_0 son homogéneos sin factor común en $K[X,Y]$, ya que $V(F)\cap V(G)\cap V(Z) = \phi$.
Veamos que la aplicación K-lineal $\alpha:\Gamma\to\Gamma$ definida por $\alpha(\overline{H}) = \overline{ZH}$, donde $\overline{H} = H+\langle F,G\rangle$ y $H\in R$, es inyectiva. Sea $\overline{H}\in\mathrm{Ker}(\alpha)$, por tanto $ZH = AF+BG$ con $A,B\in R$. Luego $A_0F_0 = -B_0G_0$ y como F_0 y G_0 no tienen factor común en $K[X,Y]$, entonces $B_0 = F_0C$ y $A_0 = -G_0C$ con $C\in K[X,Y]$. Defina $A_1 = A+CG$ y $B_1 = B-CF$, como $(A_1)_0 = (B_1)_0 = 0$ entonces $A_1 = ZA'$ y $B_1 = ZB'$ con $A',B'\in R$. Luego

$$A_1F+B_1G = AF+CGF+BG-CFG = AF+BG = ZH,$$

entonces $A'F + B'G = H$. Por tanto $\overline{H} = \overline{0}$ y $\mathrm{Ker}(\alpha) = \langle\overline{0}\rangle$, es decir, α es inyectiva.

Paso 3: Sea $d \geq m + n$. En el paso 1 se probó que $\dim_K \Gamma_e = m \cdot n$ para todo $e \geq m + n$, entonces se pueden escoger $A_1, A_2, \ldots, A_{mn} \in R_d$ cuyos residuos en Γ_d formen una base. Además, por el paso 2, $\alpha|_{\Gamma_d} : \Gamma_d \to \Gamma_{d+1}$ es un isomorfismo K-lineal de espacios vectoriales. Se sigue que los residuos de $Z^r A_1, Z^r A_2, \ldots, Z^r A_{mn}$ en Γ_{d+r} forman un base, para todo $r \geq 0$.
Defina a_i como el residuo de $(A_i)_* = A(X, Y, 1) \in K[X, Y]$ en Γ_* con $i = 1, 2, \ldots, mn$. Veamos que $\{a_1, \ldots, a_{mn}\}$ es una base para Γ_*. Sea $\overline{H} \in \Gamma_*$ con $H \in K[X, Y]$, existe $N \in \mathbb{N}$ tal que $Z^N H^*$ es homogéneo de grado $d + r$ con $r \geq 0$, dado que los residuos de $Z^r A_1, Z^r A_2, \ldots, Z^r A_{mn}$ en Γ_{d+r} son base, se tienen que $Z^N H^* = \sum_{i=1}^{mn} \alpha_i Z^r A_i + AF + BG$ con $\alpha_i \in K$ y $A, B \in K[X, Y, Z]$, entonces $H = (Z^N H^*)_* = \sum_{i=1}^{mn} \alpha_i (A_i)_* + A_* F_* + B_* G_*$. Se sigue que $\overline{H} = \sum_{i=1}^{mn} \alpha_i a_i$. Por tanto $\{a_1, \ldots, a_{mn}\}$ genera a Γ_*.
Para mostrar que $\{a_1, \ldots, a_{mn}\}$ son linealmente independientes, tome $\lambda_1, \ldots, \lambda_{mn} \in K$ tal que $\sum_{i=1}^{mn} \lambda_i a_i = \overline{0}$ y veamos que $\lambda_i = 0$. Luego, por definición, $\sum_{i=1}^{mn} \lambda_i (A_i)_* = AF_* + BG_*$ con A, B en $K[X, Y]$. Además, si homogenizamos la anterior igualdad, existen $r, s, t \in \mathbb{N}$ tal que $Z^r \sum_{i=1}^{mn} \lambda_i A_i = Z^s A^* F + Z^t B^* G \in R_{d+r}$, entonces $\sum_{i=1}^{mn} \lambda_i \overline{Z^r A_i} = \overline{0}$ en Γ_{d+r} y como $\{\overline{Z^r A_i}\}_{i=1}^{mn}$ es base de Γ_{d+r}, se sigue $\lambda_i = 0$ para $i = 1, \ldots, mn$. □

Así como el teorema fundamental del álgebra nos permite realizar operaciones o propiedades sobre las raíces de un polinomio de una variable, sin conocerlas explícitamente, ya que nos garantiza su existencia y también la cantidad. Con ayuda del teorema de Bézout, en realidad es la base, se puede definir una estructura de grupo sobre el conjunto de ceros de un polinomio de grado tres no singular, que lo llamaremos *curva elíptica*.

Ejemplo 3.20. Si una curva proyectiva $V(F)$, con $\mathrm{d}^\circ F = d$, no tienen componentes múltiples entonces

$$d(d-1) \geq \sum_{P \in V(F)} m_P(F)(m_P(F) - 1).$$

En efecto, aplicando el teorema de Bézout y por una propiedad del índice de intersección se sigue que

$$d(d-1) = \sum_P (F, F_x)_P \geq \sum_P m_P(F) m_P(F_x),$$

veamos que $m_P(F_x) \geq m_P(F) - 1$. Sin perdida de generalidad suponga $P = (0 : 0 : 1)$. Sea $m = m_P(F) = m_P(F_*)$ entonces

$$F_* = f_m + f_{m+1} + \cdots + f_d \qquad \text{con } f_i \text{ homogéneo de grado } i,$$

luego

$$(F_*)_x = (f_m)_x + (f_{m+1})_x + \cdots + (f_d)_x \qquad \text{con } (f_i)_x \text{ homogéneo de grado } i - 1,$$

y como $(F_x)_* = (F_*)_x$ entonces $m_P(F_x) = m_P((F_x)_*) \geq m - 1 = m_P(F) - 1$.

4. Curvas racionales

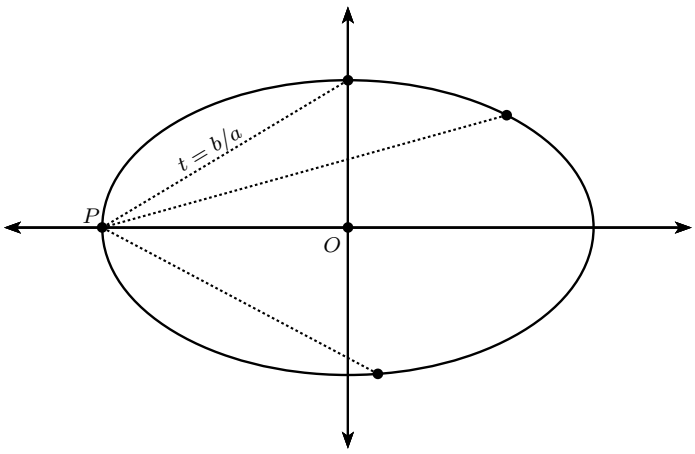
Una curva afín $V(f)$ pueden ser considerada un objeto de dimensión uno, en el sentido que la ecuación $f(X,Y)=0$ hace depender una variable de la otra, por tanto se podría conseguir una función de un parámetro que recorra el gráfico de f. Por ejemplo, $r(t)=(\cos(t),\text{sen}(t))$ es una función que recorre el circulo unidad. En este capítulo, vamos a estudiar las propiedades de las curvas que se pueden recorrer por medio de expresiones racionales polinomiales.

4.1. Curvas racionales afines

Definición 4.1. Una curva afín irreducible $V(f)$ es *racional* si existe un par de funciones racionales $x(T)$, $y(T)$ no ambas constantes, tal que $f(x(T),y(T))=0$ en $K(T)$. El par $x(T)$, $y(T)$ se llama *parametrización racional* o simplemente *parametrización*.

La definición se restringe a curva irreducibles por que si una es racional, cualquier mÃºltiplo de ella también es racional con la misma parametrización. Sea $f\in K[X,Y]\backslash K$, si es posible despejar de la ecuación $f(X,Y)=0$ una de las variables, digamos X, de tal manera que sea igual a una fracción polinomial no constante $x(Y)$ entonces f es racional. En efecto, una parametrización es dada por $x(T)$ y $y(T)=T$. Se sigue que las rectas y parábolas son racionales. Veamos un ejemplo menos trivial.

Ejemplo 4.2. Considere la elipse $f(X,Y)=b^2X^2+a^2Y^2-a^2b^2\in\mathbb{R}[X,Y]$. Sea $P=(-a,0)$, con $P\in V(f)$, para encontrar una parametrización de f, se encuentra el otro punto de intersección de las rectas que pasan por P con f variando su pendiente, como se ve en la figura.



Sea $t \in \mathbb{R}$, la recta que pasa por P y tiene pendiente t es $l_t := Y - t(X+a)$. Luego

$$\begin{aligned} f_{l_t} = f(X, t(X+a)) &= b^2X^2 + a^2t^2(X+a)^2 - a^2b^2 \\ &= (b^2 + a^2t^2)X^2 + 2a^3t^2X + a^4t^2 - a^2b^2 \end{aligned}$$

resolviendo la ecuación $f_{l_t} = 0$

$$\begin{aligned} X &= \frac{-2a^3t^2 \pm \sqrt{4a^6t^4 - 4(b^2 + a^2t^2)(a^4t^2 - a^2b^2)}}{2(b^2 + a^2t^2)} \\ &= -a\,\frac{a^2t^2 \mp b^2}{b^2 + a^2t^2} \end{aligned}$$

La solución del + resulta en el punto P. Entonces una parametrización para la elipse es

$$\begin{aligned} x(T) &= \frac{ab^2 - a^3T^2}{b^2 + a^2T^2} \\ y(T) &= \frac{2ab^2T}{b^2 + a^2T^2} \end{aligned}$$

Note que el ejemplo anterior no hay ninguna restricciń para T y no existe un valor para T tal que $(x(T), y(T)) = P$.
Cuando una curva es racional, cada valor del parámetro de una parametrización, excepto los que anulan sus denominadores, le corresponde un único punto de la curva. Puede pasar que la correspondencia valor $\to$ punto no sea inyectiva o sobreyectiva. Por ejemplo en $\mathbb{R}^2$, la parametrización $x = T^2, y = 1/T^2$ de la hipérbole $XY = 1$ esta recorriendo dos veces la parte de la hipérbole que esta en el primer cuadrante y no define ningún punto de la hipérbole del tercer cuadrante.
Vamos a ver que para toda curva racional existe una *buena parametrización* tal que la correspondencia valor $\to$ punto es inyectiva, excepto para un número finito de valores. Pero antes se necesitan unas definiciones y proposiciones.

Definición 4.3. Sea $C = V(f)$ una curva afín irreducible. Una función $\varphi : C \to \mathbb{A}$ se dice *regular* o *polinomial* si es igual a la restricción en C a una función polinomial $\mathbb{A}^2 \to \mathbb{A}$, es decir, si existe $p \in K[X, Y]$ tal que $\varphi(x, y) = p(x, y)$ para todo $(x, y) \in C$.

Denotamos por $A(C)$ en conjunto de las funciones regulares de una curva afín $C = V(f)$ irreducible, el cual tiene estructura natural de anillo con la suma y producto usual de funciones. Por definición existe un epimorfismo natural $\psi : K[X, Y] \to A(C)$ que hace corresponder a cada polinomio p la función polinomial p restricta a C. Como C es irreducible, aplicando la proposición 2.3 se sigue que $\operatorname{Ker}\psi = \langle f \rangle$, luego

$$A(C) \simeq K[X, Y]/\langle f \rangle$$

por tanto $A(C)$ es dominio y se puede definir su cuerpo de fracciones, se denota por $K(C)$ y lo llamamos el cuerpo de *funciones racionales* de la curva afín irreducible C.
Cada elemento de $K(C)$ puede ser expresado como $\overline{p}/\overline{q}$, con $\overline{q} \neq \overline{0}$, donde $\overline{p}, \overline{q}$ denota las funciones polinomiales $p, q : \mathbb{A}^2 \to \mathbb{A}$ restrictas a C o las clases de equivalencia de los polinomios $p, q \in K[X,Y]$ en $K[X,Y]/\langle f\rangle$. Dos expresiones $\overline{p}/\overline{q}$, $\overline{r}/\overline{s}$ representan la misma función racional en $K(C)$ si y solo si la función polinomial $\overline{ps} - \overline{qr} = \overline{0}$ es nula, o equivalentemente, el polinomio $ps - qr$ es múltiplo de f.
Diremos que una función racional $\varphi \in K(C)$ es *regular* o esta *definida* en el punto $P \in C$, si admite una representación p/q con $p, q \in A(C)$ tal que $q(P) \neq 0$. Denotamos por C_φ al subconjunto de C donde φ esta definida.

Observación. Para una función racional $\varphi \in K(C)$ el conjunto C_φ es el complemento de un subconjunto finito de C. En efecto, si $\varphi = \overline{p}/\overline{q}$ con $\overline{q} \neq 0$ entonces el polinomio q no es múltiplo de f, donde $C = V(f)$, y por la proposición 2.11 se sigue que, el conjunto donde φ puede no estar definida, $V(p) \cap C$ es finito.

Claramente toda función regular $\varphi \in A(C)$, es una función racional que esta definida en todos los puntos de C, es decir, $C_\varphi = C$. El reciproco de la anterior afirmación esta dado por la siguiente proposición.

Proposición 4.4. *Sea $C = V(f)$ curva afín irreducible. Si una función racional φ esta definida en todo los puntos de C, entonces φ es regular, es decir, $\varphi \in A(c)$.*

Demostración. Suponga $\varphi = \overline{p}/\overline{q}$ con $\overline{p}$, $\overline{q} \in K[X,Y]/\langle f\rangle \simeq A(C)$ y $C_\varphi = C$. Se define

$$I = \{s \in K[X,Y]/\langle f\rangle \,/\, s\varphi \in K[X,Y]/\langle f\rangle\},$$

claramente es un ideal de $K[X,Y]/\langle f\rangle$, la proposición se sigue si $\overline{1} \in I$. Supongamos que $\overline{1} \notin I$, entonces I esta contenido en algún ideal maximal de $K[X,Y]/\langle f\rangle$. Luego, existe $P = (a,b) \in C$ tal que $I \subseteq \langle X - a, Y - b\rangle/\langle f\rangle$, por tanto $s(P) = 0$ para todo $s \in I$. En particular $\overline{q}$ y todos los denominadores de las distintas expresiones de φ pertenecen a I, esto contradice la regularidad de φ en P. □

Ejemplo 4.5. Sea $C = V(X^2 + Y^2 - 1)$ y $\varphi = (\overline{Y} - \overline{1})/\overline{X} \in K(C)$. Claramente φ es regular en todos los puntos $(x,y) \in C$ con $x \neq 0$. Solo falta saber la regularidad de φ en $P_1 = (0,1)$ y $P_2 = (0,-1)$. Note que

$$\varphi = \frac{\overline{Y} - \overline{1}}{\overline{X}} = \frac{-\overline{X}}{\overline{Y} + \overline{1}},$$

por tanto φ es regular en P_1. Supongamos que φ es regular en P_2, entonces $C_\varphi = C$ y por la proposición 4.4 $\varphi \in A(C)$. Luego, existe $\overline{p} \in K[X,Y]/\langle f\rangle$ tal que $\frac{\overline{Y}-\overline{1}}{\overline{X}} = \overline{p}$, por tanto existe $q \in K[X,Y]$ tal que

$$Y - 1 - Xp(X,Y) = q(X,Y)(X^2 + Y^2 - 1)$$

y evaluando P_2 en la anterior ecuación se tiene que $-2 = 0$, contradicción. Entonces φ no es regular en P_2 y por tanto $C_\varphi = C \backslash P_2$.

Ahora veamos un resultado algebraico para saber cuando una curva racional a partir de su cuerpo de funciones racionales.

Proposición 4.6. *La curva $C = V(f)$ es racional si y solo si su cuerpo de funciones racionales $K(C)$ es K-isomorfo a un subcuerpo de $K(T)$, cuerpo de funciones racionales en la variable T.*

Demostración. ($\Leftarrow$) Supongamos que $K(C)$ es K-isomorfo, por $\Phi : K(C) \to K(T)$, a un subcuerpo de $K(T)$. Sean $x(T) = \Phi(\overline{X})$ y $y(T) = \Phi(\overline{Y})$. Si $x(T)$ es constante entonces $\overline{X}$ también lo es, por tanto existe $a \in K$ tal que $X - a \in \langle f \rangle$. Ya que f es irreducible, entonces existe $b \in K$ no nulo tal que $f = b(X - a)$. Se sigue que $\overline{Y}$ no es constante. Como $\overline{f} = \overline{0}$, por tanto

$$0 = \Phi(f) = f(\Phi(\overline{X}), \Phi(\overline{Y})) = f(x(T), y(T)),$$

entonces $x(T)$, $y(T)$ es una parametrización de C.
($\Rightarrow$) Sea $x(T)$, $y(T) \in K(T)$ una parametrización de C. Se define el K-homomorfismo

$$\begin{aligned} \Phi : K[X,Y] &\longrightarrow K(T) \\ h(X,Y) &\longmapsto h(x(T), y(T)), \end{aligned} \tag{4-1}$$

veamos que $\operatorname{Ker}\Phi = \langle f \rangle$. Claramente $\langle f \rangle \subseteq \operatorname{Ker}\Phi$. Suponga que $\operatorname{Ker}\Phi \nsubseteq \langle f \rangle$, por tanto existe $g \in \operatorname{Ker}\Phi$ tal que $f \nmid g$. Como f es irreducible entonces, aplicando el lema 2.10, existen $r(X)$, $s(Y) \in \operatorname{Ker}\Phi$ no nulos. Ya que $\langle r(X), s(Y) \rangle \subseteq \operatorname{Ker}\Phi$, existe un K-epimorfismo natural de $K[X,Y]/\langle r(X), s(Y) \rangle$ a $K[X,Y]/\operatorname{Ker}\Phi$.
Por el lema 2.27, como $V(\langle r(X), s(Y) \rangle)$ es finito, entonces $\dim_K K[X,Y]/\langle r(X), s(Y) \rangle < \infty$ y por tanto $\dim_K K[X,Y]/\operatorname{Ker}\Phi = N < \infty$. Luego

$$K[x(T), y(T)] \simeq K[X,Y]/\operatorname{Ker}\Phi$$

es la K-subalgebra de $K(T)$ generada por $x(T)$, $y(T)$ y además es K-espacio vectorial de dimensión N. En particular, las funciones $1, x(T), x^2(T), \ldots, x^N(T)$ son linealmente dependientes sobre K, entonces $x(T)$ es algebraico sobre K y por tanto $x(T) \in K$, análogamente $y(T) \in K$. Contradicción, ya que $x(T), y(T)$ es para metrización de C.
Se sigue que

$$A(C) \simeq K[X,Y]/\langle f \rangle \simeq K[x(T), y(T)],$$

entonces

$$K(C) \simeq K(x(T), y(T)) \leq K(T).$$

□

Como consecuencia de la anterior proposición, si $C = V(f)$ es racional, se puede consideran a $K(C)$ como subcuerpo de $K(T)$ bajo la inclución dada por la extensión de (4-1)

$$\begin{aligned} K(C) &\hookrightarrow K(T) \\ \varphi(X,Y) &\longmapsto \varphi(x(T), y(T)) \end{aligned} \tag{4-2}$$

donde $x(T), y(T)$ es una parametrización de C. Otro resultado es la siguiente definición.

Definición 4.7. De dice que la parametrización $x(T)$, $y(T)$ de una curva C es *buena* si la inclución definida por (4-2) es sobreyectiva.

Como se habia dicho, una buena parametrización es cuando la correspondencia

$$\text{(valor de parametro)} \longrightarrow \text{(punto de curva)} \tag{4-3}$$

es inyectiva, excepto para un número finito de valores. La definición anterior implica esta interpretación. En efecto, si la inclución (4-2) es sobreyectiva entonces existe $\varphi \in K(C)$ tal que $\varphi(x(T), y(T)) = T$.

Ejemplo 4.8. Por construcción, la parametrización

$$x(T) = \frac{1-T^2}{1+T^2} \qquad\qquad y(T) = \frac{2T^2}{1+T^2}$$

de la circunferencia $X^2 + Y^2 - 1$, dada por el ejemplo 4.2, debería ser buena. En efecto, considere $\varphi(X, Y) = \frac{Y}{X+1}$ entonces

$$\varphi(x(T), y(T)) = \frac{\frac{2T}{1+T^2}}{\frac{1-T^2}{1+T^2} + 1} = \frac{2T}{1 - T^2 + 1 + T^2} = T$$

Teorema 4.9 (Lüroth)**.** *Sea L un subcuerpo de $K(T)$ que contiene propiamente a K, entonces existe $\alpha \in K(T)$ tal que $L = K(\alpha)$.*

Demostración. Considere $g = a(T)/b(T) \in L$ no constante con $a, b \in K[T]$, entonces T es raíz del polinomio $a(X) - gb(X) \in L[X]$. Se sigue que T es algebraico sobre L y en consecuencia $K(T)$ es una extensión algebraica sobre L. Sea $p \in L[X]$ el polinomio mínimo de T sobre L tal que

$$p(X, T) = a_0(T)X^m + a_1(T)X^{m-1} + \cdots + a_m(T)$$

donde $a_j \in K[T]$, $a_0(T) \neq 0$, $a_j/a_0 \in L$ y se puede suponer que $\text{mcd}(a_0, a_1, \ldots, a_m) = 1$. Tome $0 \leq i_0, j_0 \leq m$ tal que

$$n = \text{d}^\circ a_{i_0}(T) \geq \text{d}^\circ a_j(T) \qquad \text{para} \quad 0 \leq j \leq m$$

y $a_{i_0}/a_{j_0} \notin K$, esto se puede porque los a's son primos relativos. Defina $\alpha = a_{i_0}/a_{j_0}$ que pertenece a L, ya que a_{i_0}/a_0 y a_{j_0}/a_0 estan en L. Como el polinomio $\alpha a_{j_0}(X) - a_{i_0}(X) \in L[X]$ se anula en T y es de grado n, el grado de a_{i_0}, entonces

$$[K(T) : K(\alpha)] \leq n. \tag{4-4}$$

Sea $q(X, T) = a_{j_0}(X)a_{i_0}(T) - a_{j_0}(T)a_{i_0}(X)$. Como $q(T, T) = 0$ entonces $p(X, T)$ divide a $q(X, T)$ en $K[X, T]$, porque $\text{mcd}(a_0, a_1, \ldots, a_m) = 1$. Por tanto existe $r(X, T) \in K[X, Y]$ tal que

$$p(X, T)r(X, T) = q(X, T) \tag{4-5}$$

comparando los grados respecto a la variable T se tiene que

$$n = \mathrm{d}^\circ_T p \leq \mathrm{d}^\circ_T p + \mathrm{d}^\circ_T r = \mathrm{d}^\circ_T q \leq n,$$

luego $\mathrm{d}^\circ_T r = 0$. Como $r(X,Y) = r(X)$ divide a $q(X,T)$, por simetría de q, $r(T)$ también divide a $q(X,Y)$. Por tanto $r(T)$ divide a $p(X,T)$ en $K[X,Y]$, pero como $\mathrm{mcd}(a_0, a_1, \ldots, a_m) = 1$ entonces $r(T)$ es constante. De la ecuación 4-5 se sigue que $m = \mathrm{d}^\circ_X p = \mathrm{d}^\circ_X q = n$. Luego, por la desigualdad 4-4

$$n \geq [K(T) : K(\alpha)] = [K(T) : L] \cdot [L : K(\alpha)] \geq [K(T) : L] = m = n,$$

por tanto $[L : K(\alpha)] = 1$, esto implica que $L = K(\alpha)$. □

Sean $x(T), y(T) \in K(T)$. Suponga $x(T)$ no constante. Por la primera parte de la demostración del teorema de Lüroth, se sigue que la extensión $K(T)|K(x(T))$ es algebraica. Luego, existe $p \in K(x(T))[X]$, digamos

$$p(X) = \frac{a_n}{b_n} X^n + \frac{a_{n-1}}{b_{n-1}} X^{n-1} + \cdots + \frac{a_0}{b_0}$$

con $a_i, b_i \in K[x(T)]$ tal que $p(y(T)) = 0$. Entonces, a partir de p, se puede encontrar un polinomio $f \in K[X,Y]$ con $f(x(T), y(T)) = 0$, sin perdida de generalidad se puede suponer f irreducible. En conclusión, todo par de funciones racionales $x(T), y(T)$, no ambas constantes, parametrizan alguna curva afín irreducible $C = V(f)$.

Corolario 4.10. *Toda curva afín racional admite una buena parametrización.*

Demostración. Sea $C = V(f)$ curva afín racional, por tanto existe una parametrización $x(T), y(T) \in K(T)$ tal que $K(C) \simeq K(x(T), y(T))$. Por teorema de Lüroth existe $\alpha \in K(T)$ tal que $K(x(T), y(T)) \simeq K(\alpha)$, por tanto existe $\psi \in K(C)$ tal que $\psi(x(T), y(T)) = \alpha$. Además existen $r, s \in K(T)$ tal que $x(T) = r(\alpha)$ y $y(T) = s(\alpha)$. Si se cambia T por α como parámetro, entonces la aplicación

$$\begin{aligned} K(C) &\longrightarrow K(\alpha) \\ \varphi(X,Y) &\longmapsto \varphi(r(\alpha), s(\alpha)) \end{aligned}$$

es sobreyectiva. Por tanto $r(\alpha)$, $s(\alpha)$ es una buena parametrización de C. □

Ejemplo 4.11. Veamos cual es la curva irreducible C que definen las funciones racionales

$$x := x(T) = T^6 - T^2 + 1 \qquad\qquad y := y(T) = \frac{T^2}{1 + T^2}$$

Se tiene que

$$\begin{aligned} y + yT^2 &= T^2 \\ T^2 &= \frac{y}{1 - y} \end{aligned}$$

reemplazando en x

$$\begin{aligned} x &= \frac{y^3}{(1-y)^3} - \frac{y}{1-y} + 1 \\ (x-1)(1-y)^3 &= y^3 - y(1-y)^2 \\ (x-1)(1-y)^3 &= -y(1-2y) \end{aligned}$$

Entonces $C = V((X-1)(1-Y)^3 + Y(1-2Y))$. Note que $K(x(T), y(T)) = K(T^2)$, por tanto haciendo $\alpha = T^2$ se tiene la una buena parametrización de C dada por $x(\alpha) = \alpha^3 - \alpha + 1$ y $y(\alpha) = \frac{\alpha}{1+\alpha}$.

4.2. Curvas racionales proyectivas

En el ejemplo 4.2 se encontró una parametrización $x(T), y(T)$ para la elipse de la forma $f(X,Y) = b^2X^2 + a^2Y^2 - a^2b^2$ tal que el punto $(-a, 0) \in V(f)$ no pertenece a la imagen de la aplicación $\psi : \mathbb{A} \to \mathbb{A}^2$ con $\psi(t) = (x(t), y(t))$. Si se considera $K = \mathbb{R}$ o $\mathbb{C}$

$$\lim_{t\to\infty} \psi(t) = \lim_{t\to\infty} \left(\frac{ab^2 - a^3t^2}{b^2 + a^2t^2}, \frac{2ab^2t}{b^2 + a^2t^2} \right) = (-a, 0),$$

entonces si pudiéramos considerar al infinito como un valor del parámetro, se completaría la curva. El procedimiento, como es de esperar, es considerar a $\mathbb{A}$ y $\mathbb{A}^2$ como subconjunto de $\mathbb{P}$ y $\mathbb{P}^2$, respectivamente. Se define

$$\begin{aligned} \widetilde{\psi} : \mathbb{P} &\longrightarrow \mathbb{P}^2 \\ (t, u) &\longmapsto (ab^2u^2 - a^3t^2 : 2ab^2tu : b^2u^2 + a^2t^2) \end{aligned}$$

tal que $\psi(t) = \widetilde{\psi}(t : 1)$ y además $\widetilde{\psi}(1 : 0) = (-a : 0 : 1)$. Otra ventaja de la definición de $\widetilde{\psi}$ es que esta definida en $t = \pm\sqrt{-1}$. Note que $\widetilde{\psi}(\mathbb{P}) = V(f^*)$.
Veamos como se formaliza el procedimiento anterior.

Definición 4.12. Una aplicación $\Psi : \mathbb{P} \to \mathbb{P}^2$ se dice *regular* o *polinomial*, si existen polinomios homogéneos del mismo grado $F_0, F_1, F_2 \in K[X, Y]$ tales que

$$\Psi(P) = (F_0(P) : F_1(P) : F_2(P)) \qquad \forall P \in \mathbb{P}$$

y los polinomios F_0, F_1, F_2 no tienen un cero $P \in \mathbb{P}$ en común, es decir, se debe cumplir que $V(F_0) \cap V(F_1) \cap V(F_n) = \emptyset$. A los polinomios F_0, F_1, F_2 se les llama coordenadas de Ψ.

La condición de que F_0, F_1, F_2 tengan el mismo grado, digamos d, es para garantizar que Ψ esta bien definida. En efecto, sean $(a, b) \in \mathbb{A}^2$ y $t \in K$ no nulo, entonces

$$\begin{aligned} \Psi(a : b) &= ((F_0(a, b) : F_1(a, b) : F_2(a, b))) \\ &= (t^d(F_0(a, b) : t^dF_1(a, b) : t^dF_2(a, b))) \\ &= ((F_0(at, bt) : F_1(at, bt) : F_2(at, bt))) \end{aligned}$$

Proposición 4.13. *Sean $x(T), y(T)$ funciones racionales y $B \subseteq \mathbb{A}$ el mayor conjunto donde están definidas. Entonces existe una única aplicación polinomial $\Psi : \mathbb{P} \to \mathbb{P}^2$ tal que*

$$\Psi(t:1) = (x(t) : y(t) : 1) \qquad \forall t \in B$$

Demostración. Suponga $x(T) = \frac{p(T)}{q(T)}$ y $y(T) = \frac{r(T)}{s(T)}$ con $p, q, r, s \in K[T]$. Al homogeneizar respecto a una variable U se define

$$x^*(T,U) = \frac{p^*(T,U)}{q^*(T,U)} \qquad y^*(T,U) = \frac{r^*(T,U)}{s^*(T,U)}$$

de tal manera que $\mathrm{d}^\circ p^* = \mathrm{d}^\circ q^*$ y $\mathrm{d}^\circ r^* = \mathrm{d}^\circ s^*$, esto es para garantizar la buena definición en un punto de la recta proyectiva $\mathbb{P}$. Ademas se define $f = qs \in K[T]$ y se homogeneiza como $f^*(T,U) = q^*(T,U)s^*(T,U)$. Entonces, por las definiciones anteriores, la aplicación $\psi : \mathbb{P} \to \mathbb{P}^2$ definida por

$$\psi(t:u) = (f^*(t,u)x^*(t,u) : f^*(t,u)y^*(t,u) : f^*(t,u)) \qquad \forall (t:u) \in \mathbb{P}$$

es polinomial y para $t \in B$ se cumple que $f(t) \neq 0$ y por tanto

$$\begin{aligned}\psi(t:1) &= (f^*(t,1)x^*(t,1) : f^*(t,1)y^*(t,1) : f^*(t,1)) \\ &= (f(t)x(t) : f(t)y(t) : f(t)) \\ &= (x(t) : y(t) : 1)\end{aligned}$$

La unicidad de la aplicación se sigue por el procedimiento para su definición. □

Esta proposición, garantiza que una parametrización puede ser reemplazada por una aplicación polinomial. Este cambio es favorable, no solo porque se pierden las restricciones del parámetro, los valores que anulaban los denominadores, ademaás la curva se completa por la siguiente proposición.

Proposición 4.14. *La imagen de una aplicación polinomial $\Psi : \mathbb{P} \to \mathbb{P}^2$ no constante es una curva proyectiva irreducible.*

Demostración. Sean $F_0, F_1, F_2 \in K[X,Y]$ coordenadas de Ψ, tal que sus grados son iguales a n. Si $F_2 = 0$, veamos que $\Psi(\mathbb{P})$ es la recta infinito $V(Z)$. En efecto, claramente $\Psi(\mathbb{P}) \subseteq V(Z)$, sea $Q = (a : b : 0) \in V(Z)$ y sin perdida de generalidad suponga $b \neq 0$. El polinomio $bF_0(X,Y) - aF_1(X,Y)$ es no nulo, ya que Ψ no es constante, por tanto tiene una raíz $P \in \mathbb{P}$. Luego, $bF_0(P) = aF_1(P)$ y entonces

$$\begin{aligned}\Psi(P) &= (F_0(P) : F_1(P) : 0) \\ &= \left(\frac{a}{b}F_1(P) : F_1(P) : 0\right) \\ &= (a : b : 0) = Q,\end{aligned}$$

se sigue que $\Psi(\mathbb{P}) = V(Z)$. Ahora, suponga $F_2 \neq 0$ y sean

$$x(T) := \frac{(F_0)_*(T)}{(F_2)_*(T)} = \frac{F_0(T,1)}{F_2(T,1)}$$
$$y(T) := \frac{(F_1)_*(T)}{(F_2)_*(T)} = \frac{F_1(T,1)}{F_2(T,1)}$$

al menos una esas funciones racionales es no constante, de no ser así F_0, F_1, F_2 tendrían un cero en común. Sea $V(f)$ la curva afín irreducible racional, parametrizada por $x(T), y(T)$ y $F = f^*$ irreducible con $\mathrm{d}^\circ F = \mathrm{d}^\circ f = d$. Veamos que $\Psi(\mathbb{P}) = V(F)$. Se define el polinomio homogéneo

$$\widetilde{F}(T,U) = F(F_0(T,U), F_1(T,U), F_2(T,U))$$

tal que $\mathrm{d}^\circ \widetilde{F} = \mathrm{d}^\circ F \cdot \mathrm{d}^\circ F_i$. Luego

$$\begin{aligned}
\widetilde{F}(T,1) &= F(F_0(T,1), F_1(T,1), F_2(T,1)) \\
&= (F_2(T,1))^d \, F\left(\frac{F_0(T,1)}{F_2(T,1)}, \frac{F_1(T,1)}{F_2(T,1)}, 1\right) \\
&= (F_2(T,1))^d \, F(x(T), y(T), 1) \\
&= (F_2(T,1))^d \, f(x(T), y(T)) = 0
\end{aligned}$$

entonces $\widetilde{F}$ es un polinomio homogéneo tal que $\widetilde{F}_* = 0$ y por tanto $\widetilde{F} = 0$, esto implica que $\Psi(\mathbb{P}) \subseteq V(F)$.
Sea $(a : b : c) \in \mathbb{P}^2$ con $c \neq 0$. El punto $(a : b : c)$ esta en $\Psi(\mathbb{P})$ si y solo si existe $(t : u) \in \mathbb{P}$ con $(a : b : c) = (F_0(t,u) : F_1(t,u) : F_2(t,u))$, por tanto existe $\alpha \in K$ no nulo tal que

$$\begin{aligned}
a &= \alpha F_0(t,u) \\
b &= \alpha F_1(t,u) \\
c &= \alpha F_2(t,u).
\end{aligned}$$

Coma c y α son no nulos, haga $\alpha = c/F_2(t,u)$, entonces

$$\begin{aligned}
aF_2(t,u) - cF_0(t,u) &= 0 \\
bF_2(t,u) - cF_1(t,u) &= 0.
\end{aligned} \tag{4-6}$$

Defina $G_i = X_i F_2(T,U) - X_2 F_i(T,U) \in K[X_0, X_1, X_2, T, U]$ homogenéo con $i = 0, 1$. Note que por el sistema (4-6), se sigue que $(a : b : c) \in \Psi(\mathbb{P})$ si y solo si existe solución al sistema de ecuaciones $G_0(a,b,c,T,U) = 0$, $G_1(a,b,c,T,U) = 0$.
Los G_i son homogéneos, además también son homogéneos en las variables T, U, por tanto

$$\begin{aligned}
G_0 &= r_0 T^n + r_1 T^{n-1} U + \cdots + r_{n-1} T U^{n-1} + r_n U^n \\
G_1 &= s_0 T^n + s_1 T^{n-1} U + \cdots + s_{n-1} T U^{n-1} + s_n U^n
\end{aligned}$$

donde r_j, s_j son polinomios homogéneos de grado 1 en las variables X_0, X_1, X_2. Considere la resultante $R(X_0, X_1, X_2)$ de $G_0(X_0, X_1, X_2, T, 1)$ y $G_1(X_0, X_1, X_2, T, 1)$, entonces

$$R(a,b,c) = 0 \Leftrightarrow \begin{cases} r_0(a,b,c) = s_0(a,b,c) = 0 \\ \text{o} \\ G_0(a,b,c,T,1) \text{ y } G_1(a,b,c,T,1) \text{ tienen raíz común.} \end{cases}$$

Si $r_0(a,b,c) = s_0(a,b,c) = 0$ por tanto $G_0(a,b,c,1,0) = G_1(a,b,c,1,0) = 0$, se concluye que

$$R(a,b,c) = 0 \Longleftrightarrow \exists (t:u) \in \mathbb{P} \text{ tal que } G_0(a,b,c,t,u) = G_1(a,b,c,t,u) = 0.$$

En resumen, por equivalencias, se tiene que

$$(a:b:c) \in \Psi(\mathbb{P}) \text{ con } c \neq 0 \Longleftrightarrow R(a,b,c) = 0$$

entonces $V(R(X_0, X_1, 1)) \subseteq \Psi(\mathbb{P}) \subseteq V(F)$ y como $V(f)$ es irreducible, se sigue que $f(X_0, X_1)$ divide a $R(X_0, X_1, 1)$, por tanto

$$(a:b:1) \in V(F) \Longrightarrow R(a,b,1) = 0 \Longrightarrow (a:b:1) \in \Psi(\mathbb{P}).$$

Repitiendo el procedimiento para a y b no nulos, en lugar de c, se deduce que $V(F) \subseteq \Psi(\mathbb{P})$ y por tanto $\Psi(\mathbb{P}) = V(F)$. Como se quería demostrar. □

Definición 4.15. Una curva proyectiva se dice *racional* si es igual a la imagen de una aplicación polinomial no constante.

Cuando se define algo en el espacio afín y luego se hace un procedimiento para una definición semejante en es espacio proyectivo, ya que con eso se obtiene alguna ventaja, es de esperar que las definiciones sean consistente. Y esta no es la excepción.

Proposición 4.16. *Sean $V(f)$ una curva afín y $V(F)$ una curva proyectiva, entonces*

(a) *$V(f)$ es racional si y solo si $V(f^*)$ es racional.*

(b) *$V(F)$ es racional si y solo si $V(F_*)$ es racional o vacío.*

Veamos las definiciones semejantes a $A(C)$ y $K(C)$ para el caso proyectivo, que son necesarias para el siguiente capitulo.

Definición 4.17. Sea $V(F)$ curva proyectiva irreducible, se define el *dominio homogéneo* de F como

$$A(F)_h = K[X,Y,Z]/\langle F \rangle.$$

Denotamos por $\overline{G}$ la clase de equivalencia de $G \in K[X,Y,Z]$ modulo $\langle F \rangle$ y por $K(F)_h$ a su cuerpo de fracciones.

El subconjunto de $K(F)_h$ formado por las fracciones $\overline{G}/\overline{H}$ con G, H homogéneos del mismo grado forma un subcuerpo, lo denotamos por $K(F)$ y lo llamamos *cuerpo de las funciones racionales* de F. Esta definición se justifica por la siguiente proposición.

Proposición 4.18. *Sea $C = V(f)$ una curva afín irreducible y $F = f^*$ entonces $K(F)$ es isomorfo a $K(C)$.*

Demostración. Considere el K-homomorfismo

$$\begin{aligned} \psi : K[X,Y] &\longrightarrow K(F)_h \\ g(X,Y) &\longmapsto g(\overline{X}/\overline{Z}, \overline{Y}/\overline{Z}). \end{aligned}$$

Note que $g^*(X,Y,Z) = Z^{\mathrm{d}^\circ g} g(X/Z, Y/Z)$, entonces

$$\psi(g) = g(\overline{X}/\overline{Z}, \overline{Y}/\overline{Z}) = \frac{g^*(\overline{X}, \overline{Y}, \overline{Z})}{\overline{Z}^{\mathrm{d}^\circ g}} \in K(F).$$

Se sigue que la imagen de ψ esta contenida en $K(F)$. Veamos que $\operatorname{Ker}\psi = \langle f \rangle$. Sea $g \in \langle f \rangle$, luego $g^* = FH$ con $H \in K[X,Y,Z]$ homogéneo, por tanto

$$\psi(g) = \frac{g^*(\overline{X}, \overline{Y}, \overline{Z})}{\overline{Z}^{\mathrm{d}^\circ g}} = \frac{F(\overline{X}, \overline{Y}, \overline{Z}) H(\overline{X}, \overline{Y}, \overline{Z})}{\overline{Z}^{\mathrm{d}^\circ g}} = \overline{0}.$$

Suponga $g \in \operatorname{Ker}\psi$, entonces $\frac{g^*(\overline{X}, \overline{Y}, \overline{Z})}{\overline{Z}^{\mathrm{d}^\circ g}} = \overline{0} \in K(F)_h$.Se sigue que $g^*(X,Y,Z) \in \langle F \rangle$ y por tanto $g(X,Y) \in \langle f \rangle$.
Luego, como $A(C) \simeq K[X,Y]/\langle f \rangle \simeq \operatorname{Im}\psi \subseteq K(F)$ entonces $K(C) \simeq L$ un subcuerpo de $K(F)$. Dado que todo elemento de $K(F)$ tiene una representación como cociente de polinomios generados por $\overline{X}/\overline{Z}$, $\overline{Y}/\overline{Z} \in \operatorname{Im}\psi$, entonces $L = K(F)$. □

4.3. Genero virtual

Saber que una curva es racional no es un problema sencillo, como vimos en las secciones pasadas. Una forma es encontrando una parametrización y la otra es aplicando la proposición 4.6, pero ninguna de ellas es fácil de hacer. En esta sección, a cada curva se le va asociar un número que depende del grado y de sus punto singulares, tal que hay una relación entre el valor del número y la racionalidad de la curva.

Definición 4.19. El *genero virtual* de una curva proyectiva $V(F)$ sin componentes múltiples, con $\mathrm{d}^\circ F = d$, es en número entero

$$g_v(F) = \frac{(d-1)(d-2)}{2} - \sum_P \frac{m_P(F)(m_P(F)-1)}{2}.$$

Se define para curvar sin componentes múltiples para que solo una cantidad finita de terminos de la sumatoria sea no nula, aplicando la proposición 3.15.
Claramente el genero virtual es una propiedad invariante, ya que el grado de una curva y la multiplicidad de sus puntos son propiedades invariantes.

Ejemplo 4.20. Como las rectas no tiene puntos singulares entonces $g_v(L) = 0$ para toda recta. Ahora, veamos que las cónicas irreducibles tienen genero virtual cero. Considere $K = \mathbb{C}$. Toda cónica es congruente a una de la forma

$$X^2 + aY^2 + bZ^2 + cYZ,$$

esto se comprueba completando cuadrados en la forma general de las cónicas. Reduciendo las equivalentes, solo quedan tres cónicas

$$X^2 + Y^2 - Z^2, \quad X^2 - Y^2, \quad X^2$$

donde solo la primera es irreducible y también no singular, por tanto su genero virtual es cero.

Antes de mencionar y demostrar el resultado central de esta sección, veamos unos lemas necesarios.

Lema 4.21. *Sea $C = V(f)$ curva afín irreducible y $\varphi \in K(C)$ no constante. El homomorfismo*

$$\begin{aligned} \Psi : K[T] &\longrightarrow K(C) \\ p(T) &\longmapsto p(\varphi) \end{aligned}$$

es inyectivo. En particular, se puede extender a un isomorfismo de cuerpos, de las funciones racionales $K(T)$ sobre un subcuerpo de $K(C)$ que denotamos por $K(\varphi)$.

Demostración. Como K es algebraicamente cerrado y φ es no constante, se sigue fácilmente que $\operatorname{Ker}\Psi = \{0\}$. □

Lema 4.22. *Sea $C = V(f)$ curva afín irreducible y $\varphi \in K(C)$ función racional no constante. Si $[K(C) : K(\varphi)] = m$ entonces la ecuación $\varphi(P) = t$ admite exactamente m soluciones distintas, excepto para un número finito de valores $t \in K$. En particular, si C admite una función racional inyectiva entonces C es racional.*

La demostración del lema 4.22 se encuentra en [13], pag. 111. Ahora veamos el teorema principal de esta sección. En su demostración se describe un método para encontrar la parametrización de una curva racional.

Teorema 4.23. *Sea $V(F)$ irreducible de grado d. Entonces*

(a) $g_v(F) \geq 0$.

(b) *Si* $g_v(F) = 0$ *entonces* $V(F)$ *es racional.*

Demostración.

(a) Los casos cuando $d = 1, 2$ estan resuelto por el ejemplo 4.20, entonces suponga $d \geq 3$. Sean $P_1, P_2, \ldots, P_r$ los distintos puntos singulares de F, defina $m_i = m_{P_i}(F) \geq 2$.
Si consideramos que el polinomio nulo tiene cualquier multiplicidad en todo punto, entonces el siguiente subconjunto de $K_n[X, Y, Z]$ tiene estructura natural de K-subespacio vectorial

$$S_n = \{G \in K_n[X, Y, Z] \ / \ m_{P_i}(G) \geq m_i - 1 \text{ para } i = 1, 2, \ldots, r\}.$$

Por la proposición 3.18 para cada P_i se tiene al menos $\frac{m_i(m_i-1)}{2}$ ecuaciones lineales que cumplen los coeficientes de los elementos de S_n. Cada ecuación linealmente independiente baja la dimensión de S_n en uno, dado que se puede encontrar un coeficiente como combinación lineal de los otros. Entonces

$$\begin{aligned} \dim_K S_n &\geq \dim_K K_n[X, Y, Z] - \sum_{i=1}^{r} \frac{m_i(m_i - 1)}{2} \\ &= \frac{(n+1)(n+2)}{2} - \sum_{i=1}^{r} \frac{m_i(m_i - 1)}{2} =: N_n \end{aligned}$$

donde $\dim_K S_n = N_n$ cuando todas las ecuaciones lineales dadas por los P_i son linealmente independientes. Suponga $n = d - 1$, entonces

$$\begin{aligned} 2N_{d-1} &= d(d+1) - \sum_{i=1}^{r} m_i(m_i - 1) \\ &= d(d-1) - \sum_{i=1}^{r} m_i(m_i - 1) \ + 2d \qquad (4\text{-}7) \\ &\geq 2d > 0 \qquad \text{(ver ejemplo 3.20)} \end{aligned}$$

por tanto $S_{d-1} \neq \emptyset$. Además, existe $G \in S_{d-1}$ que pasa por $N_{d-1} - 1$ puntos de $V(f)$ distintos a los P_i, por la imposición de $N_{d-1} - 1$ nuevas ecuaciones lineales. Aplicando el teorema de Bézout

$$d(d-1) \geq \sum_P (F, G)_P \geq \sum_P m_P(F) m_P(G) \geq \sum_{i=1}^{r} m_i(m_i - 1) \ + N_{d-1} - 1 \qquad (4\text{-}8)$$

luego por la ecuación (4-7) y la desigualdad anterior se tiene que

$$\begin{aligned} g_v(F) &= N_{d-1} - 2d + 1 \\ &\leq d(d-1) - \sum_{i=1}^{r} m_i(m_i-1) \ - 2d + 2 \\ &= (d-1)(d-2) - \sum_{i=1}^{r} m_i(m_i-1) \\ &= 2g_v(F) \end{aligned}$$

entonces $g_v(F) \geq 0$.

(b) Continuando con la notación y definiciones del ítem ***(a)***. Suponga $g_v(F) = 0$, luego

$$\begin{aligned} \dim_K S_{d-2} &\geq N_{d-2} \\ &= \frac{(d-1)d}{2} - \sum_{i=1}^{r} \frac{m_i(m_i-1)}{2} \\ &= \frac{(d-1)(d-2)}{2} - \sum_{i=1}^{r} \frac{m_i(m_i-1)}{2} + d - 1 \\ &= g_v(F) + d - 1 \\ &= d - 1. \end{aligned}$$

A partir de la imposición de $d-3$ nuevas ecuaciones lineales, se escogen distintos puntos $Q_j \in V(F)$ con $j = 1, 2, \ldots, d-3$, $Q_j \notin \{P_1, \ldots, P_r\}$ y se define el K-subespacio vectorial de S_{d-2}

$$S' = \{H \in S_{d-2} \ / \ Q_j \in V(H) \text{ para } j = 1, 2, \ldots, d-3\}$$

claramente $\dim_K S' \geq (d-1) - (d-3) = 2$. Supongamos $\dim_K S' \geq 3$, entonces existe $H \in S'$ tal que pasa por otros dos puntos de $V(F)$ distintos de los P_i y Q_j. Por un procedimiento análogo a (4-8) se tiene que

$$\begin{aligned} \sum_{i=1}^{r} m_i(m_i-1) \ + d - 3 + 2 &\leq d(d-2) \\ 1 &\leq d(d-2) - (d-2) - \sum_{i=1}^{r} m_i(m_i-1) \\ &= (d-2)(d-1) - \sum_{i=1}^{r} m_i(m_i-1) \\ &= 2g_v(F) = 0, \end{aligned}$$

contradicción. Por tanto $\dim_K S' = 2$, entonces existen $H_0, H_1 \in S'$ tal que todo elemento de S' es de la forma $x_0H_0 + x_1H_1$ con $x_0, x_1 \in K$.
Veamos que es posible parametrizar a $C = V(F_*)$ utilizando a S'. Sea $C' = V((H_0)_*)$,

$$\begin{aligned} \varphi : V(F)\backslash V(H_0) &\longrightarrow \mathbb{A} & \qquad \varphi_* : C\backslash C' &\longrightarrow \mathbb{A} \\ P &\longmapsto -\frac{H_1(P)}{H_0(P)} & P &\longmapsto -\frac{(H_1)_*(P)}{(H_0)_*(P)} \end{aligned}$$

Por construcción $V(\varphi(P)H_0 + H_1)$ es la única curva, a menos de factor constante, de grado $d-2$ que pasa por P, los Q_j y los P_i con una multiplicidad mayor o igual a $m_i - 1$. Por tanto φ es inyectiva, y en consecuencia φ_* también. En particular φ_* es no constante, aplicando el lema 4.21 el subcuerpo $K(\varphi_*)$ de $K(C)$ es isomorfo al cuerpo de funciones racionales de una variable, y por el lema 4.22 $K(\varphi_*) = K(C)$. Luego, por la proposición 4.6 C es racional y por tanto $V(F)$ también.

□

Veamos como se utiliza el teorema anterior para demostrar que una curva es racional y encontrar una parametrización

Ejemplo 4.24. Sea $K = \mathbb{C}$ y $F = (X^2+Y^2)^2-(X^2-Y^2)Z^2$. El punto $(x : y : z)$ es singular de F si cumplen las ecuaciones

1) $F(x, y, z) = (x^2 + y^2)^2 - (x^2 - y^2)z^2 = 0$
2) $F_x(x, y, z) = 4x(x^2 + y^2) - 2xz^2 = 0$
3) $F_y(x, y, z) = 4y(x^2 + y^2) + 2yz^2 = 0$
4) $F_z(x, y, z) = -2z(x^2 - y^2) = 0$

De 4) se sigue que $z = 0$ o $x = \pm y$. Suponga $z = 0$, luego de 1) se tiene que $(x^2 + y^2)^2 = 0$ y por tanto $x = \pm yi$, entonces los puntos $P_1 = (i : 1 : 0)$ y $P_2 = (-i : 1 : 0)$ son singulares. Con $x = \pm y$ se obtiene el punto $P_3 = (0 : 0 : 1)$. Ahora se encuentran sus multiplicidades. Al deshomogeneizar respecto a Z se tiene que $m_{P_3}(F) = 2$ y respecto a Y se sigue que

$$\begin{aligned} F_*(X \pm i, Z) &= ((X \pm i)^2 + 1)^2 - ((X \pm i)^2 - 1)Z^2 \\ &= (X^2 \pm 2iX)^2 - (X^2 \pm 2iX - 2)Z^2 \\ &= X^4 \pm 4iX^3 - X^2Z^2 \mp 2iXZ^2 - 4X^2 - 2Z^2 \end{aligned}$$

por tanto $m_{P_1}(F) = m_{P_2}(F) = 2$. Entonces $V(F)$ es racional por que $g_v(F) = 0$.
Considere $P_4 = (1 : 0 : 1) \in V(F)$ y veamos cuales son las dos cónicas que generan a todas las cónicas que pasan por P_1, P_2, P_3 y P_4. Note que solo es necesario que pasen por P_j ya que $m_{P_j}(F) - 1 \leq 1$ con $j = 1, 2, 3$. La forma general de las cónicas es

$$a_1X^2 + a_2Y^2 + a_3Z^2 + a_4XY + a_5XZ + a_6YZ$$

y al imponer las condiciones de que pasen por los puntos, se reducen a

$$a_1(X^2 + Y^2 - XZ) + a_6YZ.$$

Luego, defina $H_0 = YZ$ y $H_1 = X^2 + Y^2 - XZ$. Una parametrización de $V(F_*)$ se obtiene encontrando la función inversa de

$$\begin{aligned} \varphi_* : V(F_*)\backslash V((H_0)_*) &\longrightarrow \mathbb{A} \\ (x, y) &\longmapsto -\frac{(H_1)_*(x, y)}{(H_0)_*(x, y)} = \frac{x - x^2 - y^2}{y} \end{aligned}$$

Sea $t = \varphi_*(x, y)$, entonces $x^2 + y^2 = x - ty$ y al sustituir en F_* se tiene que

$$\begin{aligned} (x - ty)^2 - (x - ty - 2y^2) &= 0 \\ t^2y^2 + y^2 - 2txy &= 0 \\ y &= \frac{2tx}{t^2 + 1} \end{aligned}$$

y para terminar reemplace y en $t = \varphi_*(x, y)$, se obtiene la parametrización

$$\begin{aligned} x(T) &= \frac{T^4 - 1}{(T^2 + 1)^2 + 4T^2} \\ y(T) &= \frac{2Tx(T)}{T^2 + 1} \end{aligned}$$

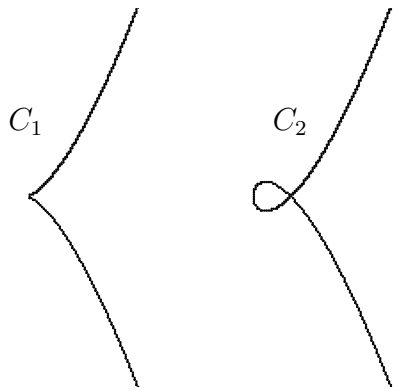
5. Curvas elípticas

A las curvas, afines o proyectivas, que se definen mediante polinomio de grado tres no singular son las que se conocen como *curvas elípticas*. Como se menciono en el ejemplo 4.20 las cónicas no singulares solo se reducen, bajo proyectividad, a una. En el caso de curvas elípticas no se pueden reducir a un número finito de curvas, pero si se conoce que forma tienen.
Si en $V(F)$ es una curva elíptica, entonces F es proyectivamente congruente a una curva elptica de la forma

$$Y^2Z - X(X-Z)(X-\lambda Z) \text{ con } \lambda \in K,\ \lambda \neq 0,1 \tag{5-1}$$

y se conoce como su *forma normal* o de *Legendre*. Cuando $\lambda = -1$, el gráfico en $\mathbb{A}^2(\mathbb{R})$ es el ejemplo 1.2 (c). Note que (5-1) solo tiene en el infinito al punto $P = (0:1:0)$, entonces como consecuencia del teorema de Bézout la recta infinto intersecta a (5-1) tres veces en P, por tanto es la recta tangente a F en P.
Los puntos no singulares tal que su recta tangente tiene índice de intersección con la curva, en el punto de tangencia, mayor o igual a tres; se les llama puntos de *inflexión*. Luego, el punto P es un punto de inflexión.

Observación. Solo hay dos tipos de cubicas irreducibles singulares, la que llamamos *cuspudal* $C_1 = V(Y^2Z - X^3)$ con punto singular $Q = (0:0:1)$ de multiplicidad 2 el cual solo tiene una recta tangente de multiplicidad dos, y la *nodal* $C_2 = V(Y^2Z - X^2(X+Z))$ con punto singular Q de multiplicidad 2 el cual tiene dos rectas tangentes distintas.



Note que las cubicas irreducibles singulares solo tienen un punto de singular de multiplicidad dos. En efecto, supongamos que $V(G)$ es una cubica con dos puntos singulares, digamos P y Q, considere la recta L que pasa por ellos. Luego

$$(G,L)_P + (G,L)_Q \geq m_P(G)m_P(L) + m_Q(G)m_Q(L) = m_P(G) + m_Q(G) \geq 4$$

lo que contradice el teorema de Bézout. Análogamente se prueba que una cubica irreducible no tiene punto de multiplicidad mayor que dos.

Proposición 5.1. *Si $V(F)$ es una curva elíptica entonces no es racional.*

Demostración. Sin perdida de generalidad, suponga $\lambda \in K\backslash$ diferente de 0 y 1 tal que $F_* = Y^2 - X(X-1)(X-\lambda)$. Por Absurdo, suponga que F_* es racional, por tanto existen $a, b, c, d \in K[T]$, no todos constantes y con $\text{mcd}(a, c) = \text{mcd}(b, d) = 1$, tales que $x = a/c$, $y = b/d$ es una buena parametrización de F_*. Luego

$$F_*(x,y) = \frac{b^2}{d^2} - \frac{a}{c}\left(\frac{a}{c} - 1\right)\left(\frac{a}{c} - \lambda\right) = 0$$
$$d^2 a(a-c)(a-\lambda c) = b^2 c^3,$$

dado que $\text{mcd}(a, c) = \text{mcd}(a-c, c) = \text{mcd}(a-\lambda c, c) = \text{mcd}(b, d) = 1$ y $K[T]$ es un dominio de factorización única, entonces c^3 y d^2 son asociados, es decir, $c^3/d^2 \in K$. Sin perdida de generalidad se puede suponer $c^3/d^2 = 1$, entonces

$$b^2 = a(a-c)(a-\lambda c). \tag{5-2}$$

Veamos que $\text{d}^\circ b = 3$ y $\text{d}^\circ a = 2 \geq \text{d}^\circ c$. Las rectas $Y - \gamma Z$ no intersectan a F en el infinito, entonces casi todas las rectas horizontales $Y = \gamma$ intersectan a F_* en tres puntos distintos. En efecto, ya que las rectas $Y = \gamma$ que no intersectan a F_* en tres puntos distintos, son las que $g = \gamma^2 - X(X-1)(X-\lambda)$ y $g_x(X)$ tienen raíces en común, note que $g_x(X)$ es independiente de γ. Como la parametrización es buena, esos tres puntos son de la forma $(x(t), \gamma)$. Los tres valores distintos de t son dados por la ecuación

$$y(t) = b(t)/d(t) = \gamma$$

por tanto el polinomio $b(T) - \gamma d(T)$ admite exactamente tres raíces distintas, para casi todo γ, luego $\text{d}^\circ b \leq 3$.
Supongamos $\text{d}^\circ b < 3$, entonces $\text{d}^\circ d = 3$ y $\text{d}^\circ c = 2$, ya que $c^3 = d^2$. Por al igualdad (5-2) $\text{d}^\circ b = 2$ y $\text{d}^\circ a = 0$ o $\text{d}^\circ a = 2$. Sea $b = b_1 b_2$, por la igualdad (5-2) b^2 tiene factores primos relativos, ya que $\text{mcd}(a-c, c) = \text{mcd}(a-\lambda c, c) = 1$, entonces $\text{mcd}(b_1, b_2) = 1$ y

$$b_1^2 b_2^2 = a(a-c)(a-\lambda c).$$

Supongamos $\text{d}^\circ a = 0$, entonces

$$b_1^2 = \alpha(a-c), \qquad b_2^2 = \beta(a-\lambda c) \qquad \text{con } \alpha \neq \beta$$

$$\lambda\beta b_1^2 - \alpha b_2^2 = \lambda\beta\alpha a - \lambda\beta\alpha c - \alpha\beta a + \alpha\beta\lambda c$$
$$(\lambda - 1)\alpha\beta a = (\sqrt{\lambda\beta} b_1 + \sqrt{\alpha} b_2)(\sqrt{\lambda\beta} b_1 - \sqrt{\alpha} b_2) \in K$$

por tanto

$$\sqrt{\lambda\beta}b_1 + \sqrt{\alpha}b_2 = u$$
$$\sqrt{\lambda\beta}b_1 - \sqrt{\alpha}b_2 = v$$

con $u, v \in K\backslash\{0\}$ y $u \neq \pm v$, los casos $u = \pm v$ conllevan a $b_1 b_2 = 0$, luego

$$v\sqrt{\lambda\beta}b_1 + v\sqrt{\alpha}b_2 = u\sqrt{\lambda\beta}b_1 - u\sqrt{\alpha}b_2$$
$$(v-u)\sqrt{\lambda\beta}b_1 = -(v+u)\sqrt{\alpha}b_2$$

por tanto b_1 y b_2 son asociados, contradicción. Con un procedimiento similar se llega a una contradicción si se supone $\mathrm{d}^\circ a = 2$.
Se sigue que $\mathrm{d}^\circ b = 3$, entonces $\mathrm{d}^\circ d \leq 3$, ya que el polinomio $b(T) - \gamma d(T)$ admite tres raíces distintas para casi todo γ, y como c^3/d^2 es constante, se sigue que $\mathrm{d}^\circ c \leq 2$. Aplicando la igualdad (5-2), implica que $\mathrm{d}^\circ a = 2$.
Se demostró que $\mathrm{d}^\circ b = 3$ y $\mathrm{d}^\circ a = 2 \geq \mathrm{d}^\circ c$. Supongamos $b = b_1 b_2 b_3$ con $\mathrm{d}^\circ b_i = 1$, por la igualdad (5-2) se sigue que b_1, b_2, b_3 son primos relativos, $b_1^2 = a$, $b_2^2 = a - c$ y $b_3^2 = a - \lambda c$ a menos de reordenamiento y factor constante. Luego

$$(b_1 - b_2)(b_1 + b_2) = b_1^2 - b_2^2 = a - (a - c) = c$$
$$(b_3 - b_2)(b_3 + b_2) = b_3^2 - b_2^2 = a - \lambda c - (a - c) = c(1 - \lambda),$$

por tanto $(b_1 - b_2)(b_1 + b_2)$ y $(b_3 - b_2)(b_3 + b_2)$ son asociados. Sin perdida de generalidad se tienen las ecuaciones

$$b_1 - b_2 = \alpha(b_3 - b_2), \qquad b_1 + b_2 = \beta(b_3 + b_2) \qquad \text{con } \alpha \neq \beta,$$

luego

$$2b_2 = \beta(b_3 + b_2) - \alpha(b_3 - b_2) = (\beta - \alpha)b_3 + (\beta + \alpha)b_2$$
$$(2 - \beta - \alpha)b_2 = (\beta - \alpha)b_3$$

entonces b_2 y b_3 son asociados, contradicción. □

Esta proposición junto con la siguiente sección nos van ha servir para la buena definición del grupo en una curva elíptica.

Nota. Otra forma equivalente de las curvas elípticas afines es $Y^2 = f(X)$, donde $f(X)$ es de grado tres y todas sus raíces son distintas. Esta forma de representar se conoce como *forma de Weierstrass*.

5.1. Ciclos y equivalencia racional

Definición 5.2.

- Un *ciclo* de una curva proyectiva $V(F)$ es una expresión del tipo

$$n_1P_1 + n_2P_2 + \cdots + n_rP_r$$

donde los n_i son enteros y $P_i \in V(F)$.

- el grado de un ciclo se define por

$$\mathrm{d}^\circ \sum n_iP_i = \sum n_i.$$

- Sea $V(G)$ curva proyectiva con $\mathrm{mcd}(G,F) = 1$. Se define el *ciclo de intersección* de $V(G)$ con $V(F)$ por la formula

$$(G)_F = \sum (F,G)_P P$$

Mas específicamente, un ciclo es un elemento de un grupo abeliano libre generado por los punto de $V(F)$. Esta definición se hace solamente para el manejo de puntos de $V(F)$ contando sus multiplicidad e índices de intersección con otra curvas.
Por el teorema de Bézout se tiene que

$$\mathrm{d}^\circ(G)_F = (\mathrm{d}^\circ G)(\mathrm{d}^\circ F).$$

Veamos como podemos extender la definición de ciclo de intersección para funciones racionales. Sea $\varphi \in K(F)$ no nulo, suponga

$$\varphi = \frac{\overline{G_0}}{\overline{H_0}} = \frac{\overline{G_1}}{\overline{H_1}}$$

con G_i, H_i homogéneos del mismo grado y $\overline{H_i} \neq 0$. Entonces $G_0H_1 = G_1H_0 + AF$ para algún $A \in K[X,Y,Z]$. Luego

$$\begin{aligned}(G_0H_1)_F &= \sum_P (G_0H_1, F)_P P = \sum_P (G_1H_0 + AF, F)_P P \\ &= \sum_P (G_1H_0, F)_P P = (G_1H_0)_F\end{aligned}$$

además

$$(G_0H_1) = \sum_P (G_0H_1, F)_P P = \sum_P (G_0, F)_P P + \sum_P (H_1, F)_P P = (G_0)_F + (H_1)_F$$
$$(G_1H_0) = \sum_P (G_1H_0, F)_P P = \sum_P (G_1, F)_P P + \sum_P (H_0, F)_P P = (G_1)_F + (H_0)_F$$

entonces $(G_0)_F - (H_0)_F = (G_1)_F - (H_1)_F$. Por lo anterior, se puede definir el ciclo para una función racional $\varphi \neq 0$ como

$$(\varphi)_F = (G)_F - (H)_F$$

donde $\varphi = \overline{G}/\overline{H}$ es una representación de φ como cociente de clases de polinomios homogéneos del mismo grado.

Ejemplo 5.3. Sea $F = Y^2Z - X(X-Z)(X-\lambda Z)$. Se tienen que $V(F) \cap V(Z) = \{(0:1:0)\}$, $V(F) \cap V(Y) = \{(0:0:1), (1:0:1), (\lambda:0:1)\}$ y $V(F) \cap V(X) = \{(0:1:0), (0:0:1)\}$. Luego

$$\begin{aligned}(Z)_F &= 3(0:1:0)\\ (Y/X)_F &= (0:0:1) + (1:0:1) + (\lambda:0:1) - (0:1:0) - 2(0:0:1)\\ &= (1:0:1) + (\lambda:0:1) - (0:1:0) - (0:0:1)\end{aligned}$$

Definición 5.4. Sean D, D' ciclos de una curva irreducible $V(F)$. Diremos que D es *racionalmente equivalente* a D', se denota por $D \equiv D'$, si existe una función racional $\varphi \in K(F)$ tal que $(\varphi)_F = D - D'$.

Observación. La equivalencia racional es una relación de equivalencia compatible con la adición de ciclos, es decir, para todo ciclos D, D', D'' se cumple:

- $D \equiv D$.
- $D \equiv D \Leftrightarrow D' \equiv D$.
- $D \equiv D'$ y $D' \equiv D'' \Rightarrow D \equiv D''$.
- $D \equiv D' \Rightarrow D + D'' \equiv D' + D''$.

Proposición 5.5. *Sea $V(F)$ curva proyectiva no singular. Si existen diferentes $P, Q \in V(F)$ racionalmente equivalentes, entonces $V(F)$ es racional.*

Demostración. Sean G_0, G_1 curvas proyectivas del mismo grado tales que

$$(G_1)_F - (G_0)_F = P - Q$$

entonces

$$(G_1)_F = P + \sum_{i=1}^{r} m_i P_i$$

$$(G_0)_F = Q + \sum_{i=1}^{r} m_i P_i$$

con $m_i = (F, G_1)_{P_i} = (F, G_0)_{P_i} \geq 1$ y $P_i \neq P_j$ si $i \neq j$. Como cada $P_i \in V(F)$ es no singular, entonces para cada $(a, b) \in \mathbb{A}^2$ se cumple que $(aG_0 + bG_1)_{P_i} \geq m_i$. Luego cada elemento del conjunto $S = \{aG_0 + bG_1 \setminus (a, b) \in \mathbb{A}^2\}$ intersecta a P_i por lo menos m_i veces y como $1 + \sum_{i=1}^{r} m_i = (\mathrm{d}^\circ F)(\mathrm{d}^\circ G_0)$, entonces por cada punto de $V(F)$ distinto de los P_i pasa un único elemento de S. Por la demostración del teorema 4.23 item ***(b)*** la función racional G_1/G_0 es inyectiva y por el lema 4.22 se sigue que $V(F)$ es racional. □

Ejemplo 5.6. Si $F = YZ - X^2$, entonces $V(F)$ es no singular. Luego

$$(Y)_F = 2(0:0:1)$$
$$(X - Y)_F = (0:0:1) + (1:1:1)$$

por tanto $(0:0:1)$ y $(1:1:1)$ son racionalmente equivalentes, ya que

$$\left(\frac{Y}{X-Y}\right)_F = (0:0:1) - (1:1:1).$$

Por la proposición, se sigue que $V(F)$ es racional.

Como consecuencia inmediata de las proposiciones 5.1 y 5.5 se tiene el siguiente corolario, con el cual ya podemos definir la estructura de grupo en las curvas elípticas.

Corolario 5.7. *Si $V(F)$ es una curva elíptica y $P, Q \in V(F)$, entonces P es racionalmente equivalente a Q si y solo si $P = Q$.*

5.2. Estructura de grupo

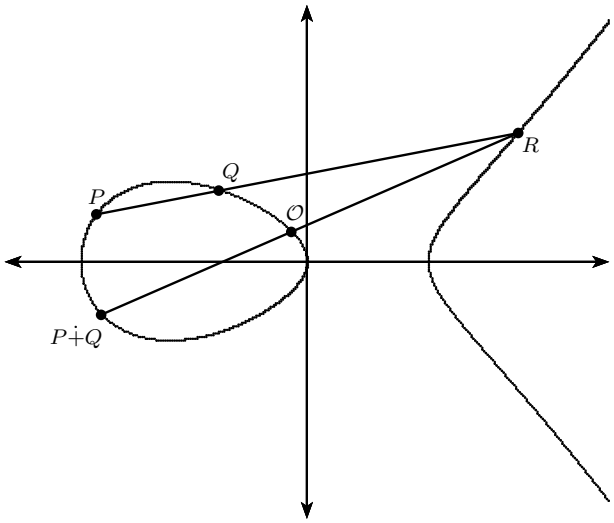
Sea F una curva eíptica, Se fija un punto $\mathcal{O} \in V(F)$. Para cada par de puntos $P, Q \in V(F)$, considere la recta L que pasa por ellos. Si $P = Q$ se toma a L como la recta tangente a F en P. Por el teorema de Bézout L debe intersectar a F en otro punto, es decir, se cumple que

$$(L)_F = P + Q + R$$

para algún $R \in V(F)$ bien determinado por P y Q. Ahora, sea L' la recta que pasa por R y $\mathcal{O}$. Se define $P \dot{+} Q$ como el tercer punto de intersección de L' con F, es decir

$$(L')_F = \mathcal{O} + R + (P \dot{+} Q)$$

Veamos una representación gráfica de la operación en $\mathbb{A}^2$.



Note que si $\varphi = L/L' \in K(F)$, entonces

$$(\varphi)_F = P + Q + R - (\mathcal{O} + R + (P\dot{+}Q)) = P + Q - \mathcal{O} - (P\dot{+}Q)$$

y por tanto

$$P\dot{+}Q \equiv P + Q - \mathcal{O}. \tag{5-3}$$

Se tiene entonces una definición mas formal de $P\dot{+}Q$, como el único punto de $V(F)$ que es racionalmente equivalente al ciclo $P + Q - \mathcal{O}$, por el corolario 5.7.

Proposición 5.8. *Sea $V(F)$ una curva elíptica y $\mathcal{O} \in V(F)$ un punto de inflexión. La aplicación que a $P, Q \in V(F)$ le asocia $P\dot{+}Q$, establece una estructura de grupo abeliano en $V(F)$. El elemento neutro es $\mathcal{O}$ y el inverso aditivo de un punto $P \in V(F)$ es el tercer punto de intersección de la recta que pasa por $\mathcal{O}$ y P con la curva $V(F)$, lo denotamos por $\dot{-}P$.*

Demostración. La buena definición se sigue del teorema de Bézout y el corolario 5.7. La conmutatividad y que $\mathcal{O}$ es el elemento neutro son consecuencia de (5-3). La definición de $\dot{-}P$ resulta por la construcción de la operación $\dot{+}$ y por la hipótesis de que $\mathcal{O}$ es un punto de inflexión. Para terminar, veamos que $\dot{+}$ es asociativa. Sean $P, Q, R \in V(F)$, por las propiedades de $\equiv$, se tiene que

$$\begin{aligned}
(P\dot{+}Q)\dot{+}R &\equiv (P\dot{+}Q) + R - \mathcal{O} \\
&\equiv P + Q - \mathcal{O} + R - \mathcal{O} \\
&\equiv P + (Q + R - \mathcal{O}) - \mathcal{O} \\
&\equiv P + (Q\dot{+}R) - \mathcal{O} \\
&\equiv P\dot{+}(Q\dot{+}R)
\end{aligned}$$

de nuevo por el coralario 5.7 se demuestra que $(P\dot{+}Q)\dot{+}R = P\dot{+}(Q\dot{+}R)$. □

Observación. Haber escogido a $\mathcal{O}$ como punto de inflexión, fue útil para definir de forma sencilla el inverso aditivo, además de otra ventaja que se vera en el siguiente párrafo. Sin embargo, no es necesario para que la operación defina un grupo abeliano. Cuando $\mathcal{O}$ es cualquier punto de $V(F)$, para definir el inverso de $P \in V(F)$ considere la recta L tangente a F en $\mathcal{O}$, L intersecta a F en otro punto, digamos R. Entonces $\dot{-}P$ se define como el otro punto de intersección con F de la recta que pasa por R y P.

Sea $V(F)$ una curva elíptica, considerando su forma normal, F solo tiene un punto en el infinito y además es punto de inflexión. De ahora en adelante se considera $\mathcal{O} = (0 : 1 : 0)$. Las rectas que pasan por $\mathcal{O}$, sin contar la recta infinito, son de la forma $X + \alpha Z$, veamos como podemos utilizar esto para encontrar las coordenadas de $\dot{-}P$ y $P\dot{+}Q$. Como todos los puntos distintos de $\mathcal{O}$ están a una distancia finita, se considera la operación en

$$F_* = Y^2 - X(X-1)(X-\lambda)$$

con la identificación $(x : y : 1) := (x, y)$. Sea $P = (x_0, y_0) \in V(F_*)$, la recta deshomogenizada que pasa por P y $\mathcal{O}$ es $l = X - x_0$. El otro punto de intersección de l y F_* es $(x_0, -y_0)$. Se sigue que $\dot{-}P = (x_0, -y_0) := (x_0 : -y_0 : 1)$.
Sean $P = (x_p, y_p)$ y $Q = (x_Q, y_Q)$ en $V(F_*)$, con $Q \neq \dot{-}P$ y $Q \neq P$, por tanto $x_P \neq x_Q$. Luego, la recta L que pasa por esos puntos es

$$Y - \alpha X - \beta \quad \text{con} \quad \alpha = \frac{y_Q - y_P}{x_Q - x_P} \quad \text{y} \quad \beta = y_P - \alpha x_P = y_Q - \alpha x_Q \tag{5-4}$$

remplazando en F_* se tiene que

$$\begin{aligned} 0 &= X(X-1)(X-\lambda) - (\alpha X + \beta)^2 \\ &= X^3 - (1 + \lambda + \alpha^2)X^2 + (\lambda - 2\alpha\beta)X - \beta^2 \end{aligned}$$

suponiendo que $R = (x, y)$ es el otro punto de la intersección de F_* con L, entonces

$$\begin{aligned} 0 &= X^3 - (1 + \lambda + \alpha^2)X^2 + (\lambda - 2\alpha\beta)X - \beta^2 \\ &= (X - x_P)(X - x_Q)(X - x) \\ &= X^3 - (x_P + x_Q + x)X^2 + (x_P x_Q + x_P x + x_Q x)X - x_P x_Q x \end{aligned}$$

igualando los coeficientes de X^2, se sigue que

$$x = \alpha^2 + \lambda + 1 - x_P - x_Q$$

entonces $y = \alpha x + \beta$. Por definición, $P\dot{+}Q$ es el inverso aditivo de R, por tanto

$$P\dot{+}Q = (\alpha^2 + \lambda + 1 - x_P - x_Q,\ -\alpha(\alpha^2 + \lambda + 1 - x_P - x_Q) - \beta). \tag{5-5}$$

Por último, encontremos las coordenadas cuando $P = Q = (x_1, y_1)$. En este caso se considera la recta tangente a F_* en P, para encontrar la pendiente se deriva F_* considerando a Y como función de X, luego

$$2YY' = 3X^2 - 2(\lambda + 1)X + \lambda.$$

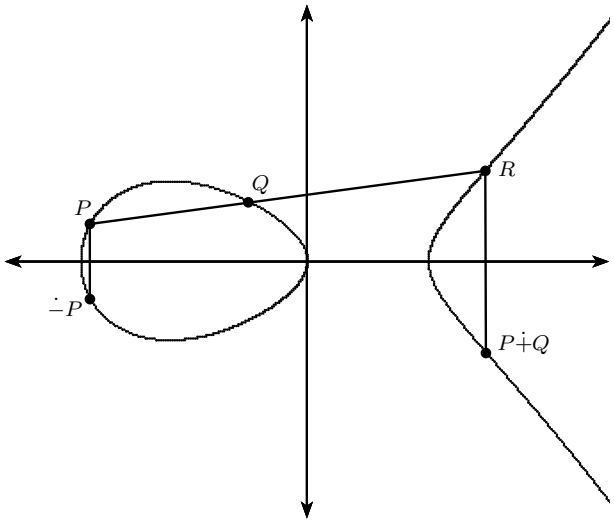
Entonces la recta tangente es $Y - \alpha X - \beta$, con

$$\alpha = \frac{3x_1^2 - 2(\lambda+1)x_1 + \lambda}{2y_1} \qquad \beta = y_1 - \alpha x_1. \tag{5-6}$$

Utilizando la igualdad (5-5) se encuentran las coordenadas

$$P\dot{+}P = (\alpha^2 + \lambda + 1 - 2x_1,\ -\alpha(\alpha^2 + \lambda + 1 - 2x_1) - \beta).$$

Como consecuencia de lo visto anteriormente, la operación tiene otra interpretación gráfica en $\mathbb{A}^2$ mas sencilla



ya que las rectas que intersectan a $\mathcal{O}$ son las verticales.
Cuando $\lambda \in \mathbb{Q}$ se define los siguientes conjuntos

$$\mathcal{E}(\mathbb{Q}) = \{(x:y:z) \in \mathbb{P}^2(\mathbb{Q}) \setminus y^2z - x(x-z)(x-\lambda z) = 0\}$$
$$E(\mathbb{Q}) = \{(x,y) \in \mathbb{A}^2(\mathbb{Q}) \setminus y^2 - x(x-1)(x-\lambda) = 0\}$$

son las restricciones de la curva elíptica, proyectiva y afín, a las soluciones con entradas racionales. Aplicando las ecuaciones (5-4),(5-5),(5-6) los conjuntos $\mathcal{E}(\mathbb{Q})$ y $E(\mathbb{Q})$ tienen estructura de grupo abeliano con $\dot{+}$.
Ahora, se puede mencionar un teorema de gran importancia para el resultado principal de este documento.

Teorema 5.9 (Mordell-Weil)**.** $(\mathcal{E}(\mathbb{Q}), \dot{+})$ *es un grupo abeliano finitamente generado.*

Los grupos abelianos tienen estructura natural de $\mathbb{Z}$-modulo, por tanto, aplicando la descomposición de torsión (pag. 332 de [7]) para módulos finitamente generados, existe un entero $r \geq 0$ tal que

$$\mathcal{E}(\mathbb{Q}) = \mathcal{E}(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r$$

donde $\mathcal{E}(\mathbb{Q})_{\text{tor}}$ es el subgrupo de los elementos finitos de $\mathcal{E}(\mathbb{Q})$. A r lo llamamos el *rango algebraico* de $\mathcal{E}(\mathbb{Q})$.

6. Números congruentes

Recuerde el problema de número congruente originalmente estaba escrito como interrogante: ¿para qué enteros n existe un número racional ω tal que $\omega - n$, ω y $\omega + n$ son cuadrados perfectos racionale?. Veremos que la definición actual es equivalente y se encuentra la relación con las curvas elípticas.

Definición 6.1. Un entero positivo n libre de cuadrados es un *número congruente* si existen $x, y, z \in Q^+$ tales que $x^2 + y^2 = z^2$ y $n = \frac{xy}{2}$, es decir, existe un triangulo rectángulo con lados racionales tal que su área sea n.

La definición se restringe a enteros positivos libre de cuadrados, ya que la propiedad de ser congruente es independiente de factor cuadrado. En efecto, sea $n \in \mathbb{Z}$ tal que existen $x, y, z \in \mathbb{Q}$ con $x^2 + y^2 = z^2$ y $n = \frac{xy}{2}$. Note que existe $s \in \mathbb{Q}$ tal que $s^2 n \in \mathbb{Z}$ es libre de cuadrados, además $(sx)^2 + (sy)^2 = (sz)^2$ y $s^2 n = s^2 \frac{xy}{2} = \frac{(sx)(sy)}{2}$. En particular como 1 no es congruente, entonces ningún cuadrado entero es congruente.
Denotemos por $\mathbb{Q}_c$ al conjunto de los números racionales positivos que son cuadrados, es decir

$$\mathbb{Q}_c = \{r^2 \,/\, r \in \mathbb{Q}^+\}.$$

Veamos que esta definición es equivalente a la pregunta inicialmente planteada.

Proposición 6.2. *Un entero $n \geq 1$ libre de cuadrados es congruente si y solo si existe un número racional ω tal que $\omega, \omega + n, \omega - n \in \mathbb{Q}_c$.*

Demostración. Supongamos $x^2 + y^2 = z^2$ y $n = \frac{xy}{2}$ con $x, y, z \in \mathbb{Q}^+$, entonces

$$\left(\frac{x \pm y}{2}\right)^2 = \frac{x^2}{4} \pm \frac{xy}{2} + \frac{y^2}{4} = \left(\frac{z}{2}\right)^2 \pm n \tag{6-1}$$

considerando $\omega = \left(\frac{z}{2}\right)^2$ se tiene que $\omega, \omega + n, \omega - n \in \mathbb{Q}_c$.
Recíprocamente, sea $\omega, \omega+n, \omega-n \in \mathbb{Q}_c$. Defina $x = \sqrt{\omega + n} - \sqrt{\omega - n}$, $y = \sqrt{\omega + n} + \sqrt{\omega - n}$ y $z = 2\sqrt{\omega}$, entonces $x^2 + y^2 = z^2$ y $n = \frac{xy}{2}$. □

Ahora, se establece la relación entre los números congruentes y las curvas elípticas. Sea $n \in \mathbb{Z}$ número congruente, utilizando las ecuaciones (6-1) se sigue

$$\left(\frac{x+y}{2}\right)^2 \left(\frac{x-y}{2}\right)^2 = \left(\left(\frac{z}{2}\right)^2 + n\right)\left(\left(\frac{z}{2}\right)^2 - n\right)$$

$$\left(\frac{x^2 - y^2}{4}\right)^2 = \left(\frac{z}{2}\right)^4 - n^2$$

por tanto, se encontró soluciones racionales $u = \frac{z}{2}$ y $v = \frac{x^2-y^2}{4}$ para la ecuación $v^2 = u^4 - n^2$, luego

$$(uv)^2 = (u^2)^3 - n^2u^2$$

entonces $a = u^2$ y $b = uv$ forman una solución $(a, b) \in \mathbb{Q}^2$ para la ecuación cúbica dada por $Y^2 = X^3 - n^2X$. Es claro que $V(Y^2 - X^3 + n^2X)$ es una curva elíptica.

Definición 6.3. Para un entero $n \geq 1$ libre de cuadrados se definen las curvas eípticas

$$\mathcal{E}_n = \{(x : y : z) \in \mathbb{P}^2(\mathbb{C}) \,/\, y^2z - x^3 + n^2xz^2 = 0\}$$
$$E_n = \{(x, y) \in \mathbb{C}^2 \,/\, y^2 - x^3 + n^2x = 0\}$$

y denotamos por $\mathcal{E}_n(\mathbb{Q})$ y $E_n(\mathbb{Q})$ sus restricciones a $\mathbb{P}^2(\mathbb{Q})$ y $\mathbb{Q}^2$, respectivamente.

Utilizando los procedimientos y formulas del capítulo anterior, las coordenadas de la suma y el inverso del los elementos del grupo $(\mathcal{E}_n, \dot{+})$ se pueden encontrar. Sean $P, Q \in \mathcal{E}_n$ con $P, Q \neq \mathcal{O}$, $Q \neq P$, $Q \neq \dot{-}P$, $P = (x_P, y_P)$ y $Q = (x_Q, y_Q)$, luego

$$\dot{-}P = (x_P, -y_P)$$
$$P\dot{+}Q = (\alpha^2 - x_P - x_Q,\ -\alpha(\alpha^2 - x_P - x_Q) - \beta) \ \text{ con } \alpha = \frac{y_P - y_Q}{x_P - x_Q},\ \beta = y_P - \alpha x_P$$
$$P\dot{+}P = (\alpha^2 - 2x_P,\ -\alpha(\alpha^2 - 2x_P) - \beta) \ \text{ con } \alpha = \frac{3x_P^2 - n^2}{2y_P},\ \beta = y_P - \alpha x_P$$

mas específicamente si $P\dot{+}P = (x_{2P}, y_{2P})$ se tiene que

$$x_{2P} = \frac{x_P^4 + 2n^2x_P^2 + n^4}{4x_P^3 - 4n^2x_P} \tag{6-2}$$

Ejemplo 6.4. Veamos cuales son los elementos de orden 2 y 3 de $\mathcal{E}_n(\mathbb{Q})$. Los elementos de orden 2 son los que cumple $P = \dot{-}P$, entonces $y_P = 0$. Por tanto hay tres puntos de orden 2, a saber

$$P_1 = (0 : 0 : 1), \qquad P_2 = (n : 0 : 1), \qquad P_3 = (-n : 0 : 1).$$

Ahora, los elementos de orden 3 cumplen que $P\dot{+}P = \dot{-}P$, por tanto

$$\begin{aligned} x_P &= \frac{x_P^4 + 2n^2x_P^2 + n^4}{4x_P^3 - 4n^2x_P} \\ 0 &= 3x_P^4 - 6n^2x_P^2 - n^4 \\ x_P^2 &= \frac{6n^2 \pm \sqrt{36n^6 + 12n^4}}{6} \\ &= \frac{3n^2 \pm 2n^2\sqrt{3}}{3} \ \notin \mathbb{Q} \end{aligned}$$

por tanto $x_P \notin \mathbb{Q}$. Se sigue que $\mathcal{E}_n(\mathbb{Q})$ no tiene elementos de orden 3.

Como consecuencia de lo anterior $|\mathcal{E}_n(\mathbb{Q})_{\text{tor}}| \geq 4$. Mas adelante se demuestra que son exactamente cuadro, para estos se necesita un poco de teoría de reducción módulo p.
Veamos como a partir de un elemento de $E_n(\mathbb{Q})$ se puede garantizar que n es congruente.

Proposición 6.5. *Sea $(a, b) \in E_n(\mathbb{Q})$ tal que $a \in \mathbb{Q}_c$ con denominador par, entonces n es un número congruente.*

Demostración. Si $u = \sqrt{a} \in \mathbb{Q}^+$ y $v = \frac{b}{u}$ entonces

$$v^2 = \frac{b^2}{a} = a^2 - n^2, \tag{6-3}$$

ya que (a, b) pertenece a $E_n(\mathbb{Q})$. Sea t el denominador de u, por hipótesis es par, por tanto los denominadores de v^2 y a^2 son iguales a t^4. Se sigue que (t^2v, t^2n, t^2a) es una terna pitagórica con t^2n par y $\text{mcd}(t^2v, t^2n, t^2a) = 1$. En efecto, suponga $a = \frac{c}{t^2}$ con $\text{mcd}(c, t) = 1$, por (6-3) $t^4v^2 = c^2 - t^4n^2 = (c + t^2n)(c - t^2n)$, luego

$$\text{mcd}(c + t^2n, c) = \text{mcd}(c - t^2n, c) = \text{mcd}(t^2, c) = 1,$$

por tanto $1 = \text{mcd}(t^4v^2, c) = \text{mcd}(t^2v, c) = \text{mcd}(t^2v, t^2a)$. Por la forma de las termas pitagóricas primitivas (pag. 120 de [7]), existen enteros positivos r, s tales que

$$t^2v = r^2 - s^2, \qquad t^2n = 2rs, \qquad t^2a = r^2 + s^2.$$

Considere $x = \frac{2r}{t}$, $y = \frac{2s}{t}$ y $z = 2u$ se cumple

$$x^2 + y^2 = \frac{4r^2}{t^2} + \frac{4s^2}{t^2} = 4a = z^2,$$

entonces (x, y, z) es una terna pitagórica y el triangulo con esos lados tiene área n. □

6.1. Reducción módulo p

Sea p un número primo y $\mathbb{F}_p$ el cuerpo finito de p elementos. Dado $(a : b : c) \in \mathbb{P}^2(\mathbb{Q})$ se puede escoger $a_0, b_0, c_0 \in \mathbb{Z}$ con $\text{mcd}(a_0, b_0, c_0) = 1$ tal que $(a : b : c) = (a_0 : b_0 : c_0)$. Se define la aplicación

$$\begin{aligned} \Phi_p : \mathbb{P}^2(\mathbb{Q}) &\longrightarrow \mathbb{P}^2(\mathbb{F}_p) \\ (a : b : c) &\longmapsto (\overline{a_0}, \overline{b_0}, \overline{c_0}). \end{aligned}$$

donde $\overline{a} = a \bmod p$. Como consecuencia, a cada punto de una curva $V_{\mathbb{Q}}(F)$ se le puede asociar un punto en $V_{\mathbb{F}_p}(\overline{F})$. Veamos cuando dos puntos de $\mathbb{P}^2(\mathbb{Q})$ tienen la misma imagen.

Proposición 6.6. *Sea $P_i = (a_i : b_i : c_i) \in \mathbb{P}^2(\mathbb{Q})$ con $a_i, b_i, c_i \in \mathbb{Z}$ y $mcd(a_i, b_i, c_i) = 1$ para $i = 1, 2$. Entonces $\Phi_p(P_1) = \Phi_p(P_2)$ si y solo si p divide a los enteros $b_1c_2 - b_2c_1$, $a_2c_1 - a_1c_2$ y $a_1b_2 - a_2b_1$.*

Demostración. ($\Leftarrow$) Supongamos que

$$\overline{b_1c_2} = \overline{b_2c_1}, \qquad \overline{a_2c_1} = \overline{a_1c_2}, \qquad \overline{a_1b_2} = \overline{a_2b_1}$$

y además que ninguno de esos productos sea nulo, ya que como p es primo esos casos son triviales. Luego $\overline{c_1} = \overline{b_2}^{-1}\overline{b_1}\overline{c_2}$, entonces $\overline{a_1} = \overline{c_2}^{-1}\overline{c_1a_2} = \overline{b_2}^{-1}\overline{b_1}\overline{c_2}$ y claramente $\overline{b_1} = \overline{b_2}^{-1}\overline{b_1b_2}$. Se sigue que $\Phi_p(P_1) = \Phi_p(P_2)$. El reciproco es trivial. □

Considere la curva elíptica $V(Y^2-X^3+n^2X)$, veamos que condiciones debe cumplir p para la reducción de $Y^2-X^3+n^2X$ a $\mathbb{F}_p$ sigue definiendo una curva elíptica. Defina $f(X) = X^3-n^2X$. Como se vio en el ejemplo 2.15, f no tenga raíces múltiples si y solo si $4n^6 \neq 0$, además esto es equivalente a que $Y^2 - f(X)$ sea una curva elíptica. Entonces la condición que debe cumplir p es que no divida a $4n^6$, es decir, $p > 2$ y $p \nmid n$.

Definición 6.7. Sea $p > 2$ primo tal que no divide a n, un entero positivo libre de cuadrados. Si $F_n = Y^2Z - X^3 + n^2XZ^2$ se define

$$\overline{F_n} = Y^2Z - X^3 + \overline{n}^2XZ^2 \ \in \mathbb{F}_p[X, Y, Z]$$

como la *reducción de F_n módulo p*. También se definen

$$\overline{\mathcal{E}_n}(\mathbb{F}_p) = \{\Phi_p(P) \in \mathbb{P}^2(\mathbb{F}_p) \,/\, P \in \mathcal{E}_n(\mathbb{Q})\}$$
$$\overline{E_n}(\mathbb{F}_p) = \{(a, b) \in \mathbb{F}_p^2 \,/\, \overline{F_n}(a, b, 1) = 0\}.$$

Note que Φ_p induce una aplicación

$$\begin{aligned} \Phi_n : \mathcal{E}_n(\mathbb{Q}) &\longrightarrow \overline{\mathcal{E}_n}(\mathbb{F}_p) \\ P &\longmapsto \Phi_p(P). \end{aligned}$$

entonces utilizando las formulas para la operación $\dot{+}$, se puede dotar a $\overline{\mathcal{E}_n}(\mathbb{F}_p)$ como estructura de grupo abeliano tal que Φ_n sea un homomorfismo de grupo.
Veamos un resultado interesante sobre la cardinalidad de $\overline{\mathcal{E}_n}(\mathbb{F}_p)$ para algunos primos.

Proposición 6.8. *Si $p \equiv 3 \ mod 4$ entonces $|\overline{\mathcal{E}_n}(\mathbb{F}_p)| = p + 1$*

Demostración. Note que $(0 : 0 : 1)$, $(\overline{n} : 0 : 1)$, $(-\overline{n} : 0 : 1)$ y $(0 : 1 : 0)$ son puntos distintos de $\overline{\mathcal{E}_n}(\mathbb{F}_p)$. Falta contar el número de puntos $(a, b) \in \overline{\mathcal{E}_n}(\mathbb{F}_p)$ tales que $a \neq \pm\overline{n}, 0$. Divida al conjunto $\{a \in \mathbb{F}_p \,/\, a \neq \pm\overline{n}, 0\}$ en los $\frac{p-3}{2}$ conjuntos $\{a, -a\}$ con $1 \leq a \leq \frac{p-1}{2}$ y $a \neq \pm\overline{n}$. Como $p \equiv 3 \bmod 4$, $f(X) = X^3 - \overline{n}^2X$ es una función impar y el símbolo de Legendre es multiplicativo, entonces

$$\left(\frac{f(-a)}{p}\right) = \left(\frac{-f(a)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{f(a)}{p}\right) = -\left(\frac{f(a)}{p}\right).$$

Se sigue que $f(a)$ o $-f(a)$ es un residuo cuadrático módulo p, pero no ambos, por tanto existe $b \in \mathbb{F}_p$ tal que $(\pm b)^2 = f(a)$ o $(\pm b)^2 = f(-a)$. En cualquiera de los casos, se encuentran dos puntos en $\overline{\mathcal{E}_n}(\mathbb{F}_p)$ por cada uno de los $\frac{p-3}{2}$ conjuntos $\{a, -a\}$, luego

$$|\overline{\mathcal{E}_n}(\mathbb{F}_p)| = 2\frac{p-3}{2} + 4 = p + 1.$$

□

Como consecuencia de esta proposición y el teorema de Dirichlet sobre sucesiones aritméticas, se puede demostrar que los únicos puntos de orden finito de $\mathcal{E}_n(\mathbb{Q})$ son los que se encontraron en el ejemplo 6.4. Recordemos que dice el teorema de Dirichlet.

Teorema 6.9 (Dirichlet)**.** *Sean $a, b \in \mathbb{N}$ tal que $mcd(a, b) = 1$ entonces existen infinitos primos de la forma $ak + b$ con $k \in \mathbb{N}$.*

Teorema 6.10. $|\mathcal{E}_n(\mathbb{Q})_{tor}| = 4$

Demostración. Se sabe que $|\mathcal{E}_n(\mathbb{Q})_{\text{tor}}| \geq 4$ y que $\mathcal{E}_n(\mathbb{Q})$ no tiene elementos de orden tres, por el ejemplo 6.4. Por absurdo, supongamos $|\mathcal{E}_n(\mathbb{Q})_{\text{tor}}| > 4$. Por tanto existe $P \in \mathcal{E}_n(\mathbb{Q})$ de orden N con $N > 3$ y $3 \nmid N$. Sin perdida de generalidad se puede suponer que $N = 4$ o N impar, ya que si $N = 4k + 2$ o $N = 4l$, implica la existencia de elementos de orden $2k + 1$, 4 o l.
Supongamos $N = 4$, como los elementos de orden dos son colineales, ya que perteneces a la recta $Y = 0$, entonces junto con la identidad se forma un subgrupo de $\mathcal{E}_n(\mathbb{Q})$ de orden 4 isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Por tanto, solo un elemento de orden dos pertenece a $\langle P \rangle$. Sea R uno de los elementos de orden dos que no pertenece a $\langle P \rangle$. Se denota por S el producto de $\langle P \rangle$ y $\langle R \rangle$, entonces $S \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4$, por tanto $S = \{P_1, \ldots, P_8\}$.
Para cada $1 \leq i, j \leq 8$ enteros, sea $P_i = (a_i : b_i : c_i)$ tal que $a_i, b_i, c_i \in \mathbb{Z}$ y

$$P_i \times P_j = (b_i c_j - b_j c_i,\ a_j c_i - a_i c_j,\ a_i b_j - a_j b_i) \ \in \mathbb{Z}^3$$

Si $i \neq j$, entonces $P_i \times P_j \neq (0, 0, 0)$. Sea M_{ij} el máximo común divisor de las coordenadas de $P_i \times P_j$. Luego, para un primo q, se tiene que $\overline{P_i} = \overline{P_j}$ en $\mathbb{P}^2_{\mathbb{F}_q}$ si y solo si q divide a M_{ij}, por la proposición 6.6. Denote por $m = |S| = 8$.
Si $q > 2$, $q \nmid n$ y $q > M_{ij}$ para todo $1 \leq i, j \leq m$ enteros, solo una cantidad finita de primos no cumplen estas condiciones, entonces $\overline{P_i} \neq \overline{P_j}$ en $\mathbb{P}^2_{\mathbb{F}_q}$ para $i \neq j$. En particular, S es isomorfo, vía Φ_n, a un subgrupo de $\overline{\mathcal{E}_n}(\mathbb{F}_q)$, entonces por el teorema de Lagrange m divide a $|\overline{\mathcal{E}_n}(\mathbb{F}_q)|$, para casi todos los primos. Suponga $q \equiv 3 \bmod 4$, entonces por la proposicíon 6.8 $|\overline{\mathcal{E}_n}(\mathbb{F}_q)| = q + 1$ y por tanto $q \equiv -1 \bmod m$. En consecuencia la sucesión $\{mk + 3\}_{k=1}^{\infty}$ tiene finitos números primos, ya que si $q = mk + 3 = 8k + 3$ cumple que $q \equiv 3 \bmod 4$ pero no cumple que $q \equiv -1 \bmod m$, por tanto q no puede ser primo. Esto contradice el teorema de Dirichlet ya que $\text{mcd}(8, 3) = 1$.
Para el caso N impar, se procede de manera análoga a la anterior con $\langle S \rangle = \langle P \rangle$, $m = N$ y se llega a la contradicción con la sucesión $\{4mk + 3\}_{k=1}^{\infty}$ ya que $3 \nmid m$.
Se sigue que $|\mathcal{E}_n(\mathbb{Q})_{\text{tor}}| = 4$. □

6.2. Caracterización de número congruente

Con lo estudiado anteriormente se puede hacer una caracterización de número congruente. Se demuestra fácilmente, una equivalencia entre el saber si un entero n es congruente y el grupo $\mathcal{E}_n(\mathbb{Q})$.

Teorema 6.11. *Un número entero n libre de cuadrados es congruente si y solo si el rango algebraico de $\mathcal{E}_n(\mathbb{Q})$ es positivo, es decir, $\mathcal{E}_n(\mathbb{Q})$ tiene un elemento de orden infinito.*

Demostración. ($\Rightarrow$) Suponga n congruente, por la construcción después de la proposición 6.2 se encuentra $(a, b) \in E_n(\mathbb{Q})$ tal que $a \in \mathbb{Q}_c$. Si (a, b) es un elemento de orden finito, entonces a debe ser 0, n o $-n$. Como $0, \pm n \notin \mathbb{Q}_c$, por hipótesis, entonces (a, b) tiene orden infinito. ($\Leftarrow$) Suponga que el rango algebraico de $\mathcal{E}_n(\mathbb{Q})$ es positivo, entonces existe $P = (a, b) \in E_n(\mathbb{Q})$ de orden infinito, entonces $b \neq 0$ y $P \dot{+} P = (a_2, b_2) \in E_n(\mathbb{Q})$ por la ecuación (6-2) cumple que

$$a_2 = \frac{a^4 + 2n^2a^2 + n^4}{4a^3 - 4n^2a} = \frac{(a^2 + n^2)^2}{4b^2} = \left(\frac{a^2 + n^2}{2b}\right)^2. \tag{6-4}$$

Luego, por la proposición 6.5 se sigue que n es congruente. □

Aplicando la demostración del teorema 6.11 y la proposición 6.2, se tiene un método para encontrar los lados del triangulo rectángulo que demuestran la congruencia de un entero. Aunque para esto se necesita un elemento de orden infinito de $\mathcal{E}_n(\mathbb{Q})$ y encontrarlo no es trivial. Para esto se utilizan los ordenadores.

Ejemplo 6.12. El número 15 es congruente dado que el punto $P = (-9, 36)$ es solución de la curva elíptica $Y^2 = X^3 - 15^2X$ y es de orden infinito. Considere la suma de $P \dot{+} P = (a, b)$, entonces por ecuación (6-4) se tiene que

$$a = \left(\frac{(-9)^2 + 15^2}{2(36)}\right)^2 = \left(\frac{17}{4}\right)^2$$

luego

$$a + 15 = \frac{529}{36} = \left(\frac{23}{4}\right)^2 \qquad a - 15 = \frac{49}{16} = \left(\frac{7}{4}\right)^2$$

entonces defina $x = \frac{23}{4} - \frac{7}{4} = 4$, $y = \frac{23}{4} + \frac{7}{4} = \frac{15}{2}$ y $z = 2\left(\frac{17}{4}\right) = \frac{17}{2}$. Se cumple que

$$x^2 + y^2 = z^2 \qquad \text{y} \qquad \frac{xy}{2} = 15$$

Apéndices

A. Clausura algebraica de $\mathbb{F}_p$

Sea K un cuerpo. La clausura algebraica de K se define como el menor cuerpo algebraicamente cerrado que lo contiene, denotado por $\overline{K}$. El propósito de este apéndice es encontrar la clausura algebraica de $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p primo).
Las letras p y n denotaran un número primo y un natural, respectivamente.

Definición A.1. Sea K subcuerpo de Ω. La clausura algebraica de K en Ω se define como

$$C_\Omega(K) = \{\alpha \in \Omega \ / \ \alpha \text{ es algebraico sobre } K\}$$

y es un subcuerpo de Ω.

Proposición A.2. *Sea K un cuerpo. Si Ω es un cuerpo algebraicamente cerrado tal que $K \subseteq \Omega$ entonces $\overline{K} = C_\Omega(K)$.*

Demostración. Supongamos Ω algebraicamente cerrado y $K \subseteq \Omega$. Por definición se sigue que $C_\Omega(K) \subseteq \overline{K}$ y $K \subseteq C_\Omega(K)$, como la clausura algebraica se comporta bien con la contención entonces $\overline{K} \subseteq \overline{C_\Omega(K)}$. Basta probar que $\overline{C_\Omega(K)} \subseteq C_\Omega(K)$. En efecto, sea $f \in C_\Omega(K)[X]$ y $\alpha \in \Omega$ tal que $f(\alpha) = 0$ por lo tanto $C_\Omega(K)(\alpha)|C_\Omega(K)$ es una extensión algebraica y como $C_\Omega(K)|K$ también lo es, entonces $C_\Omega(K)(\alpha)|K$ es algebraica. Luego $\alpha \in \Omega$ es algebraico sobre K, es decir, $\alpha \in C_\Omega(K)$.
Lo anterior prueba que toda raíz de un polinomio en $C_\Omega(K)[X]$ pertenece a $C_\Omega(K)[X]$, por tanto $C_\Omega(K)$ es algebraicamente cerrado, es decir, $\overline{C_\Omega(K)} = C_\Omega(K)$. □

Utilizando la proposición 1 y el hecho de que $\mathbb{F}_p$ es subcuerpo de algún Ω algebraicamente cerrado (tiene característica p) se sigue que $\overline{\mathbb{F}_p} = C_\Omega(\mathbb{F}_p)$. Pero eso no nos dice nada de los elementos de $\mathbb{F}_p$. A partir de ahora Ω denota un cuerpo algebraicamente cerrado con $\mathbb{F}_p$ como subcuerpo.

Definamos el siguiente subconjunto de Ω

$$GF(p^n) = \left\{\alpha \in \Omega \ / \ \alpha^{p^n} - \alpha = 0\right\}$$

donde p es primo y $n \in \mathbb{N}$.

Proposición A.3. *El conjunto $GF(p^n)$ es un subcuerpo de Ω con orden p^n tal que $\mathbb{F}_p$ es subcuerpo de $GF(p^n)$.*

Demostración. Sean α y β en $GF(p^n)$ veamos que $\alpha - \beta$ y $\alpha\beta^{-1}$ pertenecen a $GF(p^n)$. En efecto, ya que $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$ y Ω tiene característica p entonces

$$(\alpha - \beta)^{p^n} = \alpha^{p^n} - \beta^{p^n} = \alpha - \beta \quad \text{y} \quad (\alpha\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{-1})^{p^n} = \alpha^{p^n}(\beta^{p^n})^{-1} = \alpha\beta^{-1}.$$

Se sigue que $GF(p^n)$ es un subcuerpo de Ω.
Para encontrar el orden de $GF(p^n)$ se considera el polinomio $f(x) = x^{p^n} - x$, su derivada en un cuerpo de característica p es $f'(x) = p^n x^{p^n-1} - 1 = -1$. Se sigue que f no tiene raíces múltiples en Ω, ya que $f'(x) = 0$ no tiene solución, por tanto $|GF(p^n)| = \operatorname{grad} f = p^n$.
Por último veamos que $\mathbb{F}_p \subseteq GF(p^n)$. El pequeño teorema de Fermat afirma que para todo $a \in \mathbb{F}_p$ se cumple que $a^p = a$. Luego

$$a^{p^n} = (a^p)^{p^{(n-1)}} = a^{p^{(n-1)}} = (a^p)^{p^{(n-2)}} = a^{p^{(n-2)}} = \cdots = a^p = a,$$

esto garantiza que $a \in GF(p^n)$.

□

De la anterior proposición se sigue que el polinomio $f(x) = x^{p^n} - x \in \mathbb{F}_p[X]$ se factora como producto de polinomios lineales diferentes en $GF(p^n)[x]$, esto implica que $GF(p^n)$ es el campo de división de f sobre $\mathbb{F}_p$.
Veamos que el único cuerpo de orden p^n (bajo isomorfismo) es $GF(p^n)$.

Proposición A.4. *Todo cuerpo K de orden p^n es isomorfo a $GF(p^n)$.*

Demostración. Sea K un cuerpo tal que $|K| = p^n$, entonces tiene característica p y el subcuerpo generado por la unidad (los elementos son de la forma $m \cdot 1 = 1 + \cdots + 1$ (m-veces) con $0 < m \leq p$), denotado por $\langle 1 \rangle$ es isomorfo a $\mathbb{F}_p$. Además todo elemento α del grupo multiplicativo $K^\times$, el cual tiene orden $p^n - 1$, cumple que $\alpha^{p^n-1} = 1$ (Lagrange), por consiguiente todo elemento de K es cero del polinomio $f(x) = x^{p^n} - x$; esto implica que K es el campo de división de $f \in \langle 1 \rangle[X]$. Por la unicidad del campo de división del polinomio f sobre los cuerpo isomorfo $\langle 1 \rangle$ y $\mathbb{F}_p$(teorema 20.4 de [6]) se tiene que $K \simeq GF(p^n)$.

□

El único cuerpo de orden p^n se llama *el cuerpo de Galois de orden p^n*, en honor a Évariste Galois.

Ya se tiene todo lo necesario para demostrar que $\overline{\mathbb{F}_p} = \bigcup_{n\in\mathbb{N}} GF(p^n)$. Se procese por doble contención, ya que ambos son subconjuntos de Ω.
Si $n \in \mathbb{N}$ y $\alpha \in GF(p^n)$ por definición se cumple que $\alpha^{p^n} - \alpha = 0$, por tanto α es raíz del polinomio $f(x) = x^{p^n} - x$; luego α es algebraico sobre $\mathbb{F}_p$. Se sigue que $GF(p^n) \subseteq \overline{\mathbb{F}_p}$ para todo $n \in \mathbb{N}$, entonces $\bigcup_{n\in\mathbb{N}} GF(p^n) \subseteq \overline{\mathbb{F}_p}$.
Sea $\alpha \in \overline{\mathbb{F}_p}$, entonces $\alpha \in \Omega$ y es algebraico sobre $\mathbb{F}_p$. Existe $h \in \mathbb{F}_p[x]$ irreducible tal que $h(\alpha) = 0$, además α se puede identificar como un elemento del cuerpo $\mathbb{F}_p[x]/\langle h(x) \rangle$, el cual tiene orden p^n, donde $n = \operatorname{grad} f$ (teorema 6 y corolario 7, capitulo 13 [3]). Se sigue que $\mathbb{F}_p[x]/\langle h(x) \rangle$ es isomorfo a $GF(p^n)$, entonces $\alpha \in GF(p^n)$ y por tanto $\overline{\mathbb{F}_p} \subseteq \bigcup_{n\in\mathbb{N}} GF(p^n)$.

Bibliografía

[1] Alter Ronald. The Congruent Number Problem. Mathematical Association of America. The American Mathematical Monthly, Vol. 87, No.1 , pp. 43-45, Jan. 1980.

[2] Dickson Leonard. History of the Theory of Numbers. Chelsea, 1952.

[3] Dummit David, Foote Richard. Abstract Algebra, Third Edition. John Wiley and Sons, inc, 2004.

[4] Endler Otto. Teoria dos Corpos. Publicações Matemáticas, IMPA, 2012.

[5] Fulton William. Algebraic Curves, An Introduction to Algebraic Geometry. January 28, 2008.

[6] Gallian Joseph. Contemporary Abstract Algebra, Seventh Edition. Cegage Learning.

[7] Garcia Arnaldo, Lequanin Yves. Elementos de Álgebra. Projeto Euclides, IMPA, 2015.

[8] Pacheco Amílcar. Números congruentes e curvas elípticas. Matemática Universitária. Pag. 18-29, 1997.

[9] Salehyan Parham. Introdução às Curvas Elípticas e Aplicações. Publicações Matemáticas, 30° Coloquío Brasileiro de Matemática, IMPA, julho 2015.

[10] Silverman Joseph, Tate John. Rational Points on Elliptic Curves. UTM, Springer-Verlag, 1992.

[11] Stewart Ian, Los grandes problemas matemáticos, Grupo Planeta Spain, 2014.

[12] Tunnell Jerrold. A classical diophantine problem and modular forms of integral weigth 3/2. Inventiones mathematicae 72, Pag. 323-334, 1983.

[13] Vainsencher Israel. Introdução às Curvas Algébraicas Planas. Matemática Universitária, IMPA, 2009.