Sección de Matemáticas
Universidad de La Laguna

William Giovanni Hernández Yanes

Grupos en curvas elípticas

Groups in Elliptic Curves

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, Junio de 2022

Dirigido por
Evelia Rosa García Barroso

Evelia Rosa García Barroso
Departamento de Matemáticas,
Estadística e Investigación
Operativa.
Universidad de La Laguna
38200 La Laguna, Tenerife

Agradecimientos

En primer lugar me gustaría agradecer todo el esfuerzo y dedicación de mi tutora Evelia para con esta memoria. A todo el profesorado del área de álgebra por hacer de ésta una rama tan bonita.

Por último, me gustaría agradecérselo a todas las personas que han estado ahí brindándome su apoyo.

William Giovanni Hernández Yanes
La Laguna, 13 de junio de 2022

Resumen · Abstract

Resumen

Las raíces de un polinomio en dos variables se pueden representar geométricamente en el plano real dando lugar a las curvas algebraicas afines. De esta manera, podemos estudiar las diferentes propiedades geométricas que pueden albergar. En particular, nos resultará de especial interés el estudio de los puntos de las curvas elípticas, sobre todo, de sus puntos racionales.

En primer lugar, haremos una introducción general a las curvas algebraicas planas afines y al plano proyectivo para poder hablar sobre las curvas algebraicas planas proyectivas y el Teorema de Bézout. Concluiremos el Capítulo 1 mencionando los sistemas lineales de curvas y demostraremos el Teorema de los nueve puntos. En el siguiente capítulo relacionaremos las curvas algebraicas con la Teoría de Grupos centrándonos en las curvas elípticas proyectivas sobre el plano proyectivo complejo y en cómo podremos dotar sus puntos con estructura de grupo abeliano haciendo uso de una operación puramente geométrica. Finalmente, interpretaremos las curvas elípticas proyectivas como curvas afines con un punto en el infinito y pondremos atención en sus puntos racionales, los cuales conformarán un subgrupo del grupo ya estudiado.

En el tercer capítulo, nuestra meta se fijará en probar el conocido Teorema de Mordell sobre $\mathbb{Q}$, el cual establece que el subgrupo formado por los puntos racionales de una curva elíptica está finitamente generado, haciendo uso de la Teoría de Números.

Palabras clave: *Curvas elípticas – Grupos –Puntos racionales – Teorema de Mordell.*

Abstract

The roots of a polynomial in two variables can be represented geometrically in the real plane leading the algebraic curves. In this way, we are able to study the different geometric properties they verify. In particular, we are specially interested in studying the points on elliptic curves, above all, the rational ones.

First of all, we will make a general introduction about algebraic curves in the projective plane in order to be capable of talking about the projectives curves and the Bézout Theorem. We will finish the Chapter 1 by naming the linear systems and we will prove the result known as Nine Points Theorem. Next, we will relate the Group Theory with the algebraic curves by focusing on the projective elliptic curves over the complex projective plane and how we can provide them with a structure of an abelian group by using an operation purely geometric. Finally, we will interpret the projective elliptic curves as affine curves with one point at the infinity and we will concentrate on their rational points which will shape a subgrop of the one we will have already studied.

In the last chapter, our goal will be to prove the Mordell Theorem over $\mathbb{Q}$ which stablishes that the subgroup formed by the rational points on an elliptic curve is finitely generated by applying the Number Theory.

Keywords: *Elliptic Curves – Groups – Rational Points – Mordell Theorem.*

Contenido

Introducción

En nuestro día a día nos topamos con formas y contornos. Entre estos lugares geométricos se encuentran las curvas algebraicas que han sido objeto de estudio desde la antigua Grecia. Las rectas y cónicas ya eran conocidas por matemáticos como Euclides, Arquímedes, Menecmo. Han pasado veinte siglos para poder lograr una clasificación para las curvas de grado tres o mayor. Se trata de un opúsculo titulado *Enumeratio linearum tertii ordinis* redactado por Newton en 1676 y publicado en 1704. Esta considerable brecha en el tiempo da a entender la dificultad que ha tenido hallar métodos para analizar las curvas algebraicas. No obstante, muchos matemáticos han investigado las propiedades de curvas concretas, de ahí que numerosas curvas lleven el nombre de aquellos que las estudiaron por primera vez. Tras el estudio de las curvas de grado uno y dos, el estudio histórico se centró en las cúbicas lisas denominadas *curvas elípticas* y los orígenes de la investigación de tales cúbicas se encuentran en el análisis; en concreto, en la búsqueda de métodos de integración para funciones racionales.

Las curvas elípticas han sido utilizadas para probar el *último Teorema de Fermat*, el cual establece que dado un entero positivo mayor o igual que tres, entonces no existen números enteros positivos tales que la suma de las potencias enésimas de dos sea la potencia enésima del tercero. Además han sido necesarias en la factorización de enteros mediante el *método de factorización de la curva elíptica* de Lenstra, el cual es un algoritmo de tiempo de ejecución subexponencial que, actualmente, es uno de los métodos más rápidos y potentes conocidos para la factorización de enteros. Las curvas elípticas también tienen aplicaciones en criptografía. Por ejemplo el protocolo Bitcoin utiliza el algoritmo *ECDSA (Elliptic Curve Digital Signature Algorithm)* para la creación de claves privadas y públicas. Este algoritmo es una variante del conocido *Digital Signature Algorithm (DSA)* que utiliza la criptografía de curva elíptica *(Elliptic curve cryptography – ECC)* como variante de la criptografía asimétrica o de clave pública. Es por esto que los puntos racionales de las curvas elípticas cobran especial interés, pues dichos puntos tienen estructura de grupo abeliano finitamente generado

bajo cierta operación. La respuesta a este hecho formulado por Poincaré en 1908 la proporciona el *Teorema de Mordell*, demostrado por Louis Mordell en 1922.

Esta memoria tiene como fin estudiar la estructura de grupo abeliano que conforman los puntos sobre las curvas elípticas a través de una operación binaria definida de forma geométrica y el subgrupo finitamente generado por los puntos racionales de éstas sobre $\mathbb{Q}$. Para ello, dedicaremos el Capítulo 1 al estudio de las curvas algebraicas planas proyectivas y de los sistemas lineales de curvas pasando brevemente por las curvas algebraicas planas afines, el plano proyectivo y mencionando el famoso *Teorema de Bézout*, que establece que dos curvas algebraicas planas proyectivas definidas sobre un cuerpo algebraicamente cerrado y sin componentes en cómun tienen exactamente en común tantos puntos como indica el producto de sus grados, y que será un pilar fundamental para con nuestra meta. Cerraremos este capítulo con la prueba del *Teorema de los nueves puntos*, el cual afirma que dadas dos cúbicas proyectivas sobre un cuerpo algebraicamente cerrado y sin componentes en común, entonces cualquier otra cúbica que pase por ocho de sus nueves puntos de intersección debe pasar también por el noveno. En el Capítulo 2 definiremos las curvas elípticas proyectivas sobre $\mathbb{C}$ y estudiaremos cómo una operación binaria geométrica definida a partir de otra operación binaria también geométrica puede dotar al conjunto de todos los puntos de las curvas elípticas proyectivas con estructura de grupo abeliano y utilizaremos el Teorema de los nueve puntos para poder probar exitosamente la asociatividad del mismo. También estudiaremos los puntos racionales de las curvas elípticas proyectivas identíficandolos con los puntos de las cuvas elípticas afines y probaremos que estos puntos forman un subgrupo del grupo original. En el Capítulo 3 iremos más allá y daremos algunas propiedades para poder computar algebraicamente las operaciones entre puntos y demostraremos un criterio que nos proporcionará sobre la expresión que deben tener los puntos racionales. Además, estudiaremos algunos resultados de la *Teoría de Números* que nos permitirán demostrar el Teorema de Mordell. Por tanto, en esta memoria relacionaremos una subrama de la *Geometría Algebraica* (las Curvas algebraicas) con la *Teoría de Grupos* y la Teoría de números.

1

Nociones Básicas

En este capítulo proporcionaremos la teoría necesaria sobre curvas algebraicas en el plano afín y en el plano proyectivo junto con los sistemas lineales de curvas para poder estudiar con detalle los capítulos futuros. Para ello hemos seguido [2].

1.1. Curvas algebraicas afines

Sean $\mathbb{K}$ un cuerpo y $n \in \mathbb{N}\backslash\{0\}$. Denotaremos por $\mathbb{A}^n_{\mathbb{K}}$ al $\mathbb{K}$-espacio afín n-dimensional, es decir, $\mathbb{A}^n_{\mathbb{K}} := \{(a_1, \ldots, a_n) : a_i \in \mathbb{K},\ i \in \{1, \ldots, n\}\}$. A lo largo del capítulo haremos abuso de notación y consideraremos la identificación $\mathbb{A}^n_{\mathbb{K}} \cong \mathbb{K}^n$. Además, centraremos el estudio para el caso $n = 2$.

Definición 1.1. *Se llama curva algebraica plana de grado d a todo conjunto de la forma $\mathcal{C}_f = \{(a, b) \in \mathbb{K}^2 : f(a, b) = 0\} \subset \mathbb{K}^2$, donde $f(x, y) \in \mathbb{K}[x, y]$ es un polinomio de grado $d > 0$. Además, diremos que $\mathcal{C}_f$ es una recta, una cónica o una cúbica si $d = 1, 2, 3$, respectivamente.*

1.1.1. Multiplicidad de un punto sobre una curva

En esta subsección estudiaremos la multiplicidad de un punto sobre una curva algebraica plana. Sean $P, Q \in \mathbb{K}^2$ dos puntos distintos. La recta $\mathcal{L}_{P,Q}$ que pasa por ambos admite una parametrización como $\mathcal{L}_{P,Q} = \{(x(t), y(t)) : t \in \mathbb{K}\}$. Si tomamos la curva plana afín $\mathcal{C}_f$ determinada por el polinomio $f(x, y) \in \mathbb{K}[x, y]$, se tiene que los puntos de intersección entre $\mathcal{L}_{P,Q}$ y $\mathcal{C}_f$ vendrán dados por las raíces del polinomio $\Phi(t) := f(x(t), y(t)) \in \mathbb{K}[t]$. El polinomio $\Phi(t)$ se denomina *polinomio intersección*.

Definición 1.2. *Sean $\mathcal{C}$ una curva algebraica plana y $\mathcal{L}$ una recta con parametrización $(x(t), y(t))$. Sea $P \in \mathcal{L}$ el punto correspondiente al parámetro t_0 ($P = (x(t_0), y(t_0))$). Se define la multiplicidad de intersección entre $\mathcal{L}$ y $\mathcal{C}$ en el punto P, y la denotamos por $I(P, \mathcal{C}, \mathcal{L})$, a la multiplicidad de t_0 como raíz de del polinomio intersección.*

Definición 1.3. *Sean $\mathcal{C}$ una curva algebraica plana y $P \in \mathcal{C}$. Denotemos por $\mathcal{F}_P$ al haz de rectas que pasan por P. Se define la multiplicidad de P sobre la curva $\mathcal{C}$, y la denotamos por $M(P,\mathcal{C})$, como el mínimo de los valores de $I(P,\mathcal{C},\mathcal{L})$, donde $\mathcal{L} \in \mathcal{F}_P$. Además, si $M(P,\mathcal{C}) = 1,2,3$, diremos que P es un punto simple, doble o triple, respectivamente.*

Definición 1.4. *Sean $\mathcal{C}$ una curva algebraica plana y $P \in \mathcal{C}$. Diremos que P es un punto singular de $\mathcal{C}$ si $M(P,\mathcal{C}) > 1$. En caso contrario, diremos que P es un punto liso o no singular. Cuando $\mathcal{C}$ no tenga puntos singulares, diremos que $\mathcal{C}$ es una curva lisa.*

La Definición 1.4 es equivalente a la dada en Geometría Diferencial, esto es, si $\mathcal{C}$ es una curva algebraica plana afín, entonces $P \in \mathcal{C}$ anula sus derivadas parciales si, y sólo si, P es un punto singular.

Definición 1.5. *Sean $\mathcal{C} \subset \mathbb{K}^2$ una curva algebraica plana y $P \in \mathcal{C}$ tal que $M(P,\mathcal{C}) = m$. Consideremos $\mathcal{F}_P$ el haz de rectas que pasan por P. Diremos que $\mathcal{L} \in \mathcal{F}_P$ es una recta tangente a $\mathcal{C}$ en P si $I(P,\mathcal{C},\mathcal{L}) \geq m+1$. Además, si $I(P,\mathcal{C},\mathcal{L}) \geq m+2$, diremos que P es un punto de inflexión. En particular, si $I(P,\mathcal{C},\mathcal{L}) = m+2$, diremos que P es un punto de inflexión ordinario.*

1.2. Curvas algebraicas proyectivas

1.2.1. El Plano Proyectivo

Sean $\mathbb{K}$ un cuerpo y $(x,y,z),(x',y',z') \in \mathbb{K}^3\backslash\{(0,0,0)\}$. Definimos la siguiente relación de equivalencia:

$$(x,y,z) \sim (x',y',z') \text{ si, y sólo si, existe } \lambda \in \mathbb{K}\backslash\{0\} \text{ tal que } (x,y,z) = \lambda(x',y',z'). \tag{1.1}$$

A la clase de (x,y,z) la denotamos por $(x:y:z)$ y la definimos como *coordenadas homogéneas* de (x,y,z), es decir,

$$(x:y:z) = \left\{(x',y',z') \in \mathbb{K}^3\backslash\{(0,0,0)\} : (x,y,z) = \lambda(x',y',z'), \lambda \in \mathbb{K}\backslash\{0\}\right\}.$$

Definición 1.6. *Se define el plano proyectivo sobre $\mathbb{K}$ al conjunto de las clases de equivalencias dadas por (1.1) y lo denotamos por $\mathbb{PK}^2$:*

$$\mathbb{PK}^2 = \left\{(x:y:z) : (x,y,z) \in \mathbb{K}^3\backslash\{(0,0,0)\}\right\}.$$

Nótese que el punto $(0:0:0)$ no existe por cómo hemos definido la relación de equivalencia en (1.1). Además, si suponemos $z \neq 0$, se tiene que $(x:y:z) = (\frac{x}{z} : \frac{y}{z} : 1)$. Supongamos que $z = 0$ y $x \neq 0$, entonces $(x:y:z) = (1 : \frac{y}{x}, 0)$. Por

último, si suponemos que $z = 0$ e $y \neq 0$, obtenemos que $(\frac{x}{y} : 1 : 0)$. Es decir, el plano proyectivo se puede expresar como

$$\mathbb{PK}^2 = \{(x : y : 1) : x, y \in \mathbb{K}\} \cup \{(1 : y : 0) : y \in \mathbb{K}\} \cup \{(x : 1 : 0) : x \in \mathbb{K}\}.$$

De esta forma tenemos que el plano proyectivo está en correspondencia con las rectas que pasan por el origen en $\mathbb{K}^3$, donde las rectas que están contenidas en el plano $z = 0$ son los puntos del plano proyectivo que llamaremos los *puntos del infinito*. Es decir, que el plano afín lo estamos completando con los puntos del infinito. En efecto, definimos la aplicación:

$$\begin{aligned} \Phi\colon \quad \mathbb{K}^2 &\longrightarrow \mathbb{PK}^2 \\ (x, y) &\longmapsto (x : y : 1). \end{aligned}$$

Probemos la inyectividad de Φ. Sean $(x, y), (x', y') \in \mathbb{K}^2$ tales que $\Phi((x, y)) = \Phi((x', y'))$, entonces $(x : y : 1) = (x' : y' : 1)$. De aquí sabemos que existe $\lambda \in \mathbb{K}\backslash\{0\}$ de manera que $(x, y, 1) = \lambda(x', y', 1)$. Necesariamente debe ocurrir que $\lambda = 1$. Luego, $(x, y, 1) = (x', y', 1)$ y por tanto $(x, y) = (x', y')$. Concluimos que Φ es inyectiva y que $\mathbb{K}^2$ está *encajado* en $\mathbb{PK}^2$. De ahora en adelante, vamos a denotarlo como $\mathbb{K}^2 \subset \mathbb{PK}^2$. En la Figura 1.1 se muestra la interpretación geométrica del plano proyectivo $\mathbb{PK}^2$.

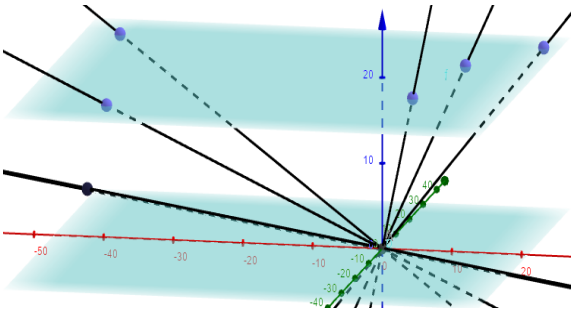

Figura 1.1. Plano Proyectivo $\mathbb{PK}^2$.

Obsérvese que si tenemos un plano afín en $\mathbb{K}^3$ que pasa por el origen, entonces existen dos vectores linealmente independientes en $\mathbb{K}^3$ que lo determinan y, además, dichos vectores se corresponden con dos puntos distintos $P, Q \in \mathbb{PK}^2$ que, a su vez, dan lugar a una *recta proyectiva* en $\mathbb{PK}^2$. Es decir, tenemos que un plano afín que contiene al origen en $\mathbb{K}^3$ es una recta proyectiva en $\mathbb{PK}^2$. Así pues, llamaremos rectas proyectivas en $\mathbb{PK}^2$ a los planos afines que pasan por el origen en $\mathbb{K}^3$. En la Figura 1.2 se muestra cómo un plano que pasa por el origen en $\mathbb{K}^3$ da lugar a una recta proyectiva en $\mathbb{PK}^2$.

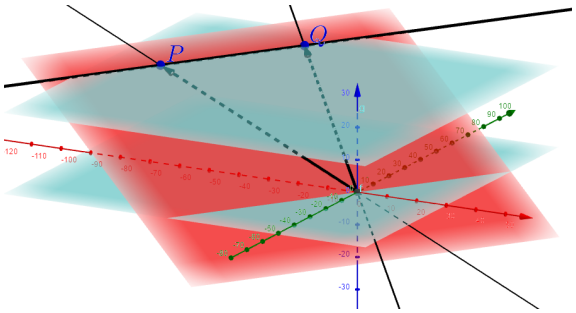

Figura 1.2. Recta Proyectiva $\mathcal{L}_{P,Q}$.

1.2.2. Curvas proyectivas planas

Habiendo visto la teoría desarrollada sobre el plano proyectivo en la Subsección 1.2.1, podemos definir las curvas algebraicas en el plano proyectivo.

Cabe pensar que una curva algebraica proyectiva se defina como el conjunto $\mathcal{C} = \{(a : b : c) \in \mathbb{PK}^2 : F(a, b, c) = 0\}$, donde $F(x, y, z) \in \mathbb{K}[x, y, z]$. Ahora bien, si tomamos el polinomio $F(x, y, z) = x^2 + y + z$ y el punto $(1 : 1 : -2) = (2 : 2 : -4)$, resulta que $F(1, 1, -2) = 0$ y que $F(2, 2, -4) = 2 \neq 0$, es decir, el conjunto $\mathcal{C}$ no está bien definido para los puntos de $\mathbb{PK}^2$. Para que esté bien definido necesitamos la siguiente definición y resultado.

Definición 1.7. *Sea $F(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$. Diremos que F es un polinomio homogéneo (o una forma) de grado d cuando todos sus términos son de grado d.*

Lema 1.8. *Sea $F(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ un polinomio homogéneo de grado d. Entonces, $F(\lambda x_1, \ldots, \lambda x_n) = \lambda^d F(x_1, \ldots, x_n)$ para todo $\lambda \in \mathbb{K}$.*

Demostración. Por hipótesis $F(x_1, \ldots, x_n) = \sum_{|\alpha|=d} a_\alpha x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, donde $\alpha = (\alpha_1, \ldots, \alpha_n)$ y $|\alpha| = \sum_{i=1}^n \alpha_i$. Ahora evaluamos en $(\lambda x_1, \ldots, \lambda x_n)$, con $\lambda \in \mathbb{K}$:

$$F(\lambda x_1, \ldots, \lambda x_n) = \sum_{|\alpha|=d} a_\alpha \lambda x_1^{\alpha_1} \ldots \lambda x_n^{\alpha_n} = \sum_{|\alpha|=d} a_\alpha \lambda^{d)} \lambda x_1^{\alpha_1} \ldots x_n^{\alpha_n} =$$

$$= \sum_{|\alpha|=d} a_\alpha \lambda^d x_1^{\alpha_1} \ldots x_n^{\alpha_n} = \lambda^d \sum_{|\alpha|=d} a_\alpha x_1^{\alpha_1} \ldots x_n^{\alpha_n} = \lambda^d F(x_1, \ldots, x_n).$$

□

En general, el recíproco es falso. En efecto, sea $F(x) = x^2 + x \in \mathbb{Z}_2[x]$. Obsérvese que $F(0 \cdot x) = 0 = 0^2 \cdot F(x)$ y $F(1 \cdot x) = x^2 + x = 1^2 \cdot F(x)$, i.e, F cumple que $F(\lambda x) = \lambda^2 F(x)$ para todo $\lambda \in \mathbb{Z}_2 = \{0, 1\}$ y sin embargo F no es homogéneo.

Ahora, podemos dar una buena definición de una curva algebraica proyectiva.

Definición 1.9. *Se llama curva algebraica proyectiva de grado d a todo conjunto de la forma* $\mathcal{C}_F = \{(a : b : c) \in \mathbb{PK}^2 : F(a, b, c) = 0\}$*, donde* $F(x, y, z) \in \mathbb{K}[x, y, z]$ *es un polinomio homogéneo de grado d. Además, diremos que* $\mathcal{C}_F$ *es una recta, una cónica o una cúbica proyectica cuando* $d = 1, 2, 3$*, respectivamente.*

Nótese que el conjunto $\mathcal{C}_F$ está bien definido para los puntos de $\mathbb{PK}^2$ gracias al Lema 1.8

1.2.3. Vistas afines

Existe cierta relación entre las curvas afines y las curvas proyectivas. Dicha relación nos la proporciona el siguiente resultado.

Proposición 1.10. *Sea* $f(x, y) \in \mathbb{K}[x, y]$ *un polinomio de grado* $d \geq 1$ *y sea* π *un plano afín en* $\mathbb{K}^3$ *que no pase por el origen y que no sea paralelo al eje Z. Entonces, existe una curva proyectiva* $\mathcal{C}_F \subset \mathbb{PK}^2$*, con* $F(x, y, z) \in \mathbb{K}[x, y, z]$ *homogéneo de grado d, tal que* $F(x, y, 1) = f(x, y)$*.*

Demostración. Supongamos que π está dado por la ecuación $\pi \equiv a'x+b'y+c'z = d'$. Como π no pasa por el origen y no es paralelo al eje Z, necesariamente $d' \neq 0$ y $c' \neq 0$. Si dividimos por d', nos queda que $\pi \equiv ax + by + cz = 1$, para ciertos $a, b, c \in \mathbb{K}$ con $c \neq 0$. Además, f será de la forma $f(x, y) = \sum_{finita} a_{ij}x^i y^j$. Podemos obtener F como sigue:

$$\begin{aligned} F(x, y, z) &= (ax + by + cz)^d f\left(\frac{x}{ax + by + cz}, \frac{y}{ax + by + cz}\right) = \\ &= \sum_{finita} (ax + by + cz)^d a_{ij} \left(\frac{x}{ax + by + cz}\right)^i \left(\frac{y}{ax + by + cz}\right)^j = \\ &= \sum_{finita} a_{ij}x^i y^j (ax + by + cz)^{d-i-j}. \end{aligned}$$

□

El proceso llevado a cabo en la prueba de la Proposición 1.10 se denomina *homogenización* de f. Al proceso inverso lo denominamos *deshomogenización* de F. Por tanto, podemos afirmar que toda curva afín es *la vista afín* de una curva proyectiva. En la práctica estos procesos los realizaremos con el plano $z = 1$. Además, nótese que la Proposición 1.10 nos garantiza que si homogenizamos un polinomio y luego lo deshomogenizamos, tenemos de vuelta el polinomio inicial. Sin embargo, el proceso contrario no es cierto. En efecto, sea $F(x, y, z) = x^2z + y^2z + z^3$. Si deshomogenizamos F se tiene que $f(x, y) = F(x, y, 1) = x^2 + y^2 + 1$. Ahora bien, si homogenizamos F, se obtiene que $G(x, y, z) = x^2 + y^2 + z^2 \neq F(x, y, z)$.
A continuación mostramos una consecuencia directa de la Proposición 1.10.

Corolario 1.11. *Sean $f(x,y) \in \mathbb{K}[x,y]$ y $F(x,y,z) \in \mathbb{K}[x,y,z]$ su homogenización respecto de la variable z. Entonces, $f(x,y) = 0$ si, y sólo si, $F(x,y,1) = 0$, para todo $(x,y) \in \mathbb{K}^2$.*

Demostración. Es una consecuencia directa de la Proposición 1.10 dado que $F(x,y,1) = f(x,y)$.

□

1.2.4. Transformaciones proyectivas

Sea Φ un isomorfismo lineal en $\mathbb{K}^3$, i.e,

$$\begin{aligned} \Phi\colon \quad \mathbb{K}^3 &\longrightarrow \mathbb{K}^3 \\ (x,y,z) &\longmapsto \Phi(x,y,z) = A \begin{pmatrix} x \\ y \\ z \end{pmatrix} =: (X,Y,Z), \end{aligned}$$

donde $A \in \mathcal{M}_{3\times 3}(\mathbb{K})$ es no singular.

Definición 1.12. *Se llama transformación proyectiva en $\mathbb{PK}^2$ a toda a aplicación $\tilde{\Phi}$ inducida por Φ como sigue:*

$$\begin{aligned} \tilde{\Phi}\colon \quad \mathbb{PK}^2 &\longrightarrow \mathbb{PK}^2 \\ (x:y:z) &\longmapsto \tilde{\Phi}(x:y:z) = (X:Y:Z). \end{aligned}$$

Si definimos la siguiente aplicación:

$$\begin{aligned} \pi\colon \ \mathbb{K}^3\backslash\{(0,0,0)\} &\longrightarrow \mathbb{PK}^2 \\ (x,y,z) &\longmapsto \pi(x,y,z) = (x:y:z), \end{aligned}$$

entonces $\tilde{\Phi}$ y Φ están relacionadas por π como $\tilde{\Phi} \circ \pi = \pi \circ \Phi$.

Definición 1.13. *Diremos que dos curvas proyectivas $\mathcal{C}_F, \mathcal{C}_G \subset \mathbb{PK}^2$ son proyectivamente equivalentes o equivalentes por transformaciones proyectivas cuando existen un isomorfismo lineal Φ en $\mathbb{K}^3$ y un escalar $\lambda \in \mathbb{K}\backslash\{0\}$ tales que $F(x,y,z) = \lambda G(\Phi(x,y,z))$. En tal caso, lo denotaremos por $\mathcal{C}_F \cong \mathcal{C}_G$.*

En lo que sigue daremos unas definiciones y unos resultados que nos ayudarán en el Capítulo 2.

Definición 1.14. *Se dice que cuatro vectores en $\mathbb{K}^3$ están en posición general cuando tres de ellos son linealmente independientes.*

Lema 1.15. *Sean $u_1, u_2, u_3, u_4 \in \mathbb{K}^3$ cuatro vectores en posición general. Entonces existe un único isomorfismo lineal que envía cada vector a un múltiplo por un escalar no nulo de $e_1 = (1,0,0), e_2 = (0,1,0), e_3 = (0,0,1)$ y $u = (1,1,1)$, respectivamente.*

Demostración. Dado que $u_1, u_2, u_3, u_4 \in \mathbb{K}^3$ se encuentran en posición general, podemos suponer, sin pérdida de generalidad, que u_1, u_2 y u_3 son linealmente independientes y que $u_4 = au_1 + bu_2 + cu_3$, con $a, b, c \in \mathbb{K}$ no nulos. Por el Álgebra Lineal, existe un isomorfismo lineal φ en $\mathbb{K}^3$ de manera que $\varphi(u_1) = e_1, \varphi(u_2) = e_2, \varphi(u_3) = e_3$ y $\varphi(u_4) = ae_1 + be_2 + ce_3 = (a, b, c)$. Si tomamos $\tau(x, y, z) := (\frac{x}{a}, \frac{y}{b}, \frac{z}{c})$, entonces $\tau \circ \varphi(u_4) = (1, 1, 1)$. Por tanto $\Phi := \tau \circ \varphi$ es el isomorfismo buscado y envía u_1, u_2, u_3 y u_4 a $\alpha e_1, \beta e_2, \gamma e_3$ y σu, respectivamente. Probemos que es único. Supongamos que existe Φ' otro isomorfismo lineal de forma que envía u_1, u_2, u_3 y u_4 a $\alpha' e_1, \beta' e_2, \gamma' e_3$ y $\sigma' u$, respectivamente. Entonces $\Phi(u_4) = (a\alpha, b\beta, c\gamma)$ y $\Phi'(u_4) = (a\alpha', b\beta', c\gamma')$. Por tanto, Φ y Φ' difieren sólo en un producto por escalar.

□

Definición 1.16. *Diremos que cuatro puntos en $\mathbb{PK}^2$ están en posición general si sus vectores correspondientes en $\mathbb{K}^3$ están en posición general.*

Lema 1.17. *Sean P_1, P_2, P_3, $P_4 \in \mathbb{PK}^2$ cuatro puntos en posición general. Entonces existe una única transformación proyectiva que envía P_1, P_2, P_3 y P_4 a E_1, E_2, E_3 y P, respectivamente, donde $E_1 = (1 : 0 : 0)$, $E_2 = (0 : 1 : 0)$, $E_3 = (0 : 0 : 1)$ y $P = (1 : 1 : 1)$.*

Demostración. Sean $P_1, P_2, P_3, P_4 \in \mathbb{PK}^2$ cuatro puntos en posición general. Entonces existen $u_1, u_2, u_3, u_4 \in \mathbb{K}^3$ cuatro vectores en posición general que los representan, respectivamente. Por el Lema 1.15, existe un único isomorfismo lineal Φ en $\mathbb{K}^3$ tal que envía u_1, u_2, u_3, u_4 a $\alpha e_1, \beta e_2, \gamma e_3, \sigma u$. Por tanto, como Φ induce una transformación proyectiva en $\mathbb{PK}^2$, se tiene que existe $\tilde{\Phi}$ transformación proyectiva de manera que envía P_1, P_2, P_3 y P_4 a E_1, E_2, E_3 y P, respectivamente. Además, $\tilde{\Phi}$ es única. Sabemos que Φ es único salvo producto por un escalar, es decir, $\Phi = \lambda\Phi'$. Si pasamos al proyectivo, se obtiene que $\tilde{\Phi} = \tilde{\Phi}'$.

□

Obsérvese que si tenemos tres puntos no colineales en $\mathbb{PK}^2$, entonces podemos hallar la recta que determinan dos de ellos. Por el Lema 1.17, tenemos que dicha recta es enviada a otra recta. Es decir, que un punto y una recta son enviados a un punto y una recta.

1.2.5. Multiplicidad de intersección

Sean $P, Q \in \mathbb{PK}^2$ dos puntos distintos. Si tomamos la recta $\mathcal{L}_{P,Q}$ que determinan ambos puntos, entonces la podemos parametrizar como $\mathcal{L}_{P,Q} = \{(x(t, s), y(t, s), z(t, s) : (t, s) \in \mathbb{K}^2\}$. Si tomamos la curva proyectiva $\mathcal{C}_F$ dada por el polinomio homogéneo $F(x, y, z) \in \mathbb{K}[x, y, z]$, entonces los puntos en

común entre $\mathcal{C}_F$ y $\mathcal{L}_{P,Q}$ estarán determinados por las raíces del polinomio $\Phi(t,s) = F(x(t,s), y(t,s), z(t,s)) \in \mathbb{K}[t,s]$, es decir, por los factores lineales de $\mathbb{K}[t,s]$. Llamamos *forma intersección* al polinomio $\Phi(t,s)$. Obsérvese que $\Phi(t,s)$ es un polinomio homogéneo del mismo grado que F.

Definición 1.18. *Sean $\mathcal{C}$ una curva proyectiva y $\mathcal{L}$ una recta proyectiva con parametrización $(x(t,s), y(t,s), z(t,s))$. Sea $P \in \mathcal{L}$ el punto correspondiente a los parámetros $(t_0 : s_0)$ ($P = (x(t_0,s_0), y(t_0,s_0), z(t_0,s_0))$). Se define la multiplicidad de intersección entre $\mathcal{L}$ y $\mathcal{C}$ en el punto P, y la denotamos por $I(P, \mathcal{C}, \mathcal{L})$, a la multiplicidad de (t_0, s_0) como raíz de la forma intersección.*

Definición 1.19. *Sean $\mathcal{C}$ una curva proyectiva y $\mathcal{L}$ una recta proyectiva. Denotemos por $\mathcal{F}_P$ al haz de rectas proyectivas que pasan por P. Se define la multiplicidad de P sobre la curva $\mathcal{C}$, y la denotamos por $M(P, \mathcal{C})$, al mínimo de los valores de $I(P, \mathcal{C}, \mathcal{L})$, donde $\mathcal{L} \in \mathcal{F}_P$. Además, si $M(P, \mathcal{C}) = 1, 2, 3$, diremos que P es un punto simple, doble o triple, respectivamente.*

Proposición 1.20. *Sean $\mathcal{C}_F$ una curva proyectiva y $\mathcal{L}$ una recta proyectiva en $\mathbb{PK}^2$. Sea $P \in \mathcal{C}_F$. Entonces, existe una variable entre x, y y z de manera que si se deshomogeniza F respecto de dicha variable, se obtiene una curva afín $\mathcal{C}_f$, una recta afín ℓ y un punto $p \in \mathbb{K}^2$ tales que $I(P, \mathcal{C}_F, \mathcal{L}) = I(p, \mathcal{C}_f, \ell)$.*

Demostración. Dado que $P \in \mathbb{PK}^2$, entonces P tiene al menos una coordenada no nula. Supongamos, sin pérdida de generalidad, que esta es la coordenada z. Sea $B = (b_1 : b_2 : 0)$ un punto en el infinito de $\mathcal{L}$ y sea $A = (a_1 : a_2 : 1)$ cualquier otro punto de $\mathcal{L}$. Entonces, una parametrización de $\mathcal{L}$ es $sA + tB$. La intersección entre $\mathcal{C}_F$ y $\mathcal{L}$ viene dada por $\Phi(s,t) = F(sA + tB)$. Igualmente, la recta afín ℓ está parametrizada como $a + bt$, donde $a = (a_1, a_2)$ y $b = (b_1, b_2)$. Las intersecciones de $\mathcal{C}_f$ y ℓ vendrán dadas por $\phi(t) = f(a + tb)$. Además, por la identificación $(x, y) \sim (x : y : 1)$, se tiene que los puntos sobre ℓ coinciden con los puntos de $\mathcal{L}$ con parámetros $(1, t)$. Luego, para $s \neq 0$, se tiene que $\Phi(s,t) = F(sA + tB) = s^d f(a + ub) = s^d \phi(u)$, donde $u = \frac{t}{s}$. Por tanto, las raíces de $\Phi(s,t)$ se corresponden con las raíces de $\phi(t)$, i.e, tienen las mismas multiplicidades. Por consiguiente, podemos concluir que $I(P, \mathcal{C}_F, \mathcal{L}) = I(p, \mathcal{C}_f, \ell)$.

□

Corolario 1.21. *Sean $\mathcal{C}_F \subset \mathbb{PK}^2$ y $P \in \mathcal{C}_F$. Entonces, existe una variable entre x, y y z de forma que si deshomogenizamos respecto de esta variable, se obtiene una curva afín $\mathcal{C}_f$ y un punto $p \in \mathbb{K}^2$ tales que $M(P, \mathcal{C}_F) = M(p, \mathcal{C}_f)$.*

Demostración. La prueba es consecuencia directa de la Proposición 1.20.

□

En resumen, para conocer la multiplicidad de un punto sobre una curva proyectiva $\mathcal{C}$, basta con estudiar la multiplicidad del correspondiente punto en el plano afín sobre cierta vista afín de la curva $\mathcal{C}$.

Definición 1.22. *Sean $\mathcal{C} \subset \mathbb{PK}^2$ y $P \in \mathcal{C}$. Diremos que P es un punto singular de $\mathcal{C}$ si $M(P,\mathcal{C}) > 1$. En caso contrario, diremos que P es un punto liso o no singular. Cuando $\mathcal{C}$ no tenga puntos singulares, diremos que $\mathcal{C}$ es una curva lisa.*

Definición 1.23. *Sean $\mathcal{C} \subset \mathbb{PK}^2$ una curva proyectiva y $P \in \mathcal{C}$ con multiplicidad $M(P,\mathcal{C}) = m$. Diremos que $\mathcal{L} \in \mathcal{F}_P$ es una recta tangente a $\mathcal{C}$ en P si $I(P,\mathcal{C},\mathcal{L}) \geq m+1$. Además, si $I(P,\mathcal{C},\mathcal{L}) \geq m+2$, diremos que P es un punto de inflexión. En particular, si $I(P,\mathcal{C},\mathcal{L}) = m+2$, diremos que P es un punto de inflexión ordinario.*

Al igual que en la Subsección 1.1.1, un punto P de una curva proyectiva $\mathcal{C}$ será singular si, y sólo si, anula a sus derivadas parciales. Además, es bien sabido que la multiplicidad de un punto sobre una curva proyectiva se conserva bajo transformaciones proyectivas. En particular, los puntos de inflexión son enviados a puntos de inflexión.
A continuación recordemos el conocido Teorema de Bézout, el cual será uno de nuestros pilares fundamentales para el desarrollo del documento.

Teorema 1.24. *Sea $\overline{\mathbb{K}}$ un cuerpo algebraicamente cerrado. Sean $\mathcal{C}_F, \mathcal{C}_G \subset \mathbb{P}\overline{\mathbb{K}}^2$ dos curvas proyectivas determinadas por los polinomios $F(x,y,z), G(x,y,z) \in \overline{\mathbb{K}}[x,y,z]$, sin componentes en común, de grados n y m, respectivamente. Entonces, $\mathcal{C}_F$ y $\mathcal{C}_G$ tienen exactamente $n \cdot m$ puntos en común (contadas multiplicidades).*

Existen distintas y diversas demostraciones del Teorema de Bézout. Una de ellas, que sólo necesita conocer la división euclidea en polinomios, se recoge en [4].

1.3. Sistemas lineales

En esta sección trataremos la teoría básica necesaria para demostrar el conocido como el *Teorema de los nueve puntos* que, a su vez, nos permitirá alcanzar uno de los objetivos de este trabajo que es dotar con estructura de grupo a las curvas elípticas que estudiaremos en el segundo capítulo.

Definición 1.25. *Sean $\mathcal{C}_F, \mathcal{C}_G \subset \mathbb{PK}^2$ dos curvas proyectivas distintas donde $F(x,y,z), G(x,y,z) \in \mathbb{K}[x,y,z]$ son homogéneos de grado d. Se define el haz de curvas de grado d generado por $\mathcal{C}_F$ y $\mathcal{C}_G$ como el conjunto*

$$\mathscr{H} := \{\lambda \mathcal{C}_F + \mu \mathcal{C}_G : (\lambda, \mu) \neq (0,0)\}.$$

Lema 1.26. *Sea $\mathscr{H}$ el haz de curvas generado por $\mathcal{C}_F, \mathcal{C}_G \subset \mathbb{PK}^2$. Entonces, cualesquiera dos curvas proyectivas distintas $\mathcal{C}_{F'}, \mathcal{C}_{G'} \in \mathscr{H}$ tienen los mismos puntos de intersección que $\mathcal{C}_F$ y $\mathcal{C}_G$.*

Demostración. Dado que $\mathcal{C}_{F'}, \mathcal{C}_{G'} \in \mathscr{H}$, se tiene que $F'(P) = \alpha F(P) + \beta G(P)$ y $G'(P) = \gamma F(P) + \sigma G(P)$ para cualquier $P \in \mathbb{PK}^2$, donde $\alpha, \beta, \gamma, \sigma \in \mathbb{K}$ y $\frac{\alpha}{\beta} \neq \frac{\gamma}{\sigma}$ (para que $\mathcal{C}_{F'}$ y $\mathcal{C}_{G'}$ no sean iguales). De aquí obtenemos que $(F'(P), G'(P)) = (0,0)$ si, y sólo si, $(F(P), G(P)) = (0,0)$. En efecto, si $(F(P), G(P)) = (0,0)$, es inmediato que $(F'(P), G'(P)) = (0,0)$. Supongamos que $(F'(P), G'(P)) = (0,0)$. Equivalentemente, obtenemos que $\alpha F(P) + \beta G(P)$=0 y $\gamma F(P) + \sigma G(P) = 0$, esto es, un sistema lineal homogéneo de dos ecuaciones con dos incógnitas. Como $\frac{\alpha}{\beta} \neq \frac{\gamma}{\sigma}$, también se tiene que la matriz asociada al sistema tiene rango 2, es decir, el sistema tiene una única solución, y por ser un sistema homogéneo, concluimos que $(F(P), G(P)) = (0,0)$.

□

Nótese que la relación de equivalencia (1.1) puede ser generalizada para el caso $n+1$. De esta forma podemos extender el concepto de plano proyectivo al de *espacio proyectivo* como sigue:

Definición 1.27. *Definimos el espacio proyectivo n-dimensional como el conjunto*

$$\mathbb{PK}^n := \left\{ (a_1 : \ldots : a_{n+1}) : (a_1, \ldots, a_{n+1}) \in \mathbb{K}^{n+1} \backslash \{(0, \overset{n+1)}{\ldots}, 0)\} \right\},$$

donde $(a_1 : \ldots : a_{n+1}) = \{\lambda(a_1, \ldots, a_{n+1}) : \lambda \in \mathbb{K}\backslash\{0\}\}$.

El siguiente resultado nos permitirá definir el concepto de *sistema lineal* más adelante.

Proposición 1.28. *Las curvas de grado d en $\mathbb{PK}^2$ forman un espacio proyectivo $\mathbb{PK}^D$, donde $D = \frac{1}{2}d(d+3)$.*

Demostración. Sean $m_1, \ldots, m_{D+1}$ los monomios de grado d en x, y, z. Esto es, los monomios de la forma $x^i y^j z^k$ tales que $i+j+k = d$. Un curva proyectiva de grado d en $\mathbb{PK}^2$ estará determinada por un polinomio homogéneo de la forma $\sum_{i+j+k=d} a_{ijk} x^i y^j z^k = \sum_{l=1}^{D+1} a_l m_l$. Si identificamos esta curva con el punto $(a_1 : \ldots : a_{D+1}) \in \mathbb{PK}^D$, obtenemos una correspondencia entre las curvas de grado d y $\mathbb{PK}^D$. Probemos ahora que $D = \frac{1}{2}d(d+3)$. Escribimos los monomios de grado de d en la siguiente forma:

$$
\begin{array}{ccccccccc}
 & & & & z^d & & & & \\
 & & & xz^{d-1} & & yz^{d-1} & & & \\
 & & x^2z^{d-2} & & xyz^{d-2} & & y^2z^{d-2} & & \\
 & \iddots & \vdots & & \vdots & & \vdots & \ddots & \\
x^d & & x^{d-1}y & \dots & & \dots & xy^{d-1} & & y^d
\end{array}
$$

Nótese que para la fila $k-$ésima hay k monomios, o sea, que para la fila $d+1$ hay $d+1$ monomios. Sumando el número de monomios por filas y sabiendo que la suma es $D+1$ (puesto que $D+1$ es nuestra incógnita), se tiene que $D+1 = 1+2+\ldots+(d+1) = \frac{1}{2}(d+1)(d+2)$. Por tanto $D = \frac{1}{2}d(d+3)$.

□

Estudiamos ahora los *subespacios proyectivos*. Para cualquier subespacio afín $U \subset \mathbb{K}^{n+1}$ de dimensión $m+1$, podemos asociarle el conjunto $PU \subset \mathbb{PK}^n$ compuesto por todas las rectas afines en $\mathbb{K}^{n+1}$ que pasan por el origen y están en U. Al conjunto PU se le denomina subespacio proyectivo de $\mathbb{PK}^n$ de dimensión m y codimensión $n-m$. Al igual que en el espacio afín, en el espacio proyectivo se tiene que si un subespacio proyectivo PU tiene dimensión m y codimensión $n-m$, entonces el subespacio PU está determinado por $n-m$ ecuaciones. Más general, si denotamos por $c = n-m$ y PU está dado por d ecuaciones no necesariamente linealmente independientes, entonces debe ocurrir que $c \leq d$.

Pasemos al estudio de los sistemas lineales de curvas.

Definición 1.29. *A los subespacios proyectivos del espacio $\mathbb{PK}^D$ de las curvas de grado d en $\mathbb{PK}^2$ se les denomina sistemas lineales de curvas.*

Los sistemas lineales más sencillos son aquellos de dimensión 1, que provienen de los planos que pasan por el origen en $\mathbb{K}^{D+1}$, compuestos por todos los elementos de la forma $sF+tG$, fijados F y G. Luego, los haces de curvas son sistemas lineales de dimensión 1.

Lema 1.30. *Sea $\mathscr{L}$ el sistema lineal de curvas de grado d que tiene dimensión s y sean $P_1, \ldots, P_s \in \mathbb{PK}^2$. Entonces, existe al menos una curva en $\mathscr{L}$ que pasa por $P_1, \ldots, P_s$.*

Demostración. Sean $P_1, \ldots, P_s \in \mathbb{PK}^2$ s puntos del plano proyectivo y sea $\mathscr{L}'$ el sistema lineal de curvas de grado d que está formado por todas las curvas de $\mathscr{L}$ que pasan por $P_1, \ldots, P_s$. Entonces $\mathscr{L}'$ está formado por $D-s$ ecuaciones más s ecuaciones que resultan de imponer que cada curva en $\mathscr{L}'$ pasa por $P_1, \ldots, P_s$, i.e, $(D-s)+s = D$ ecuaciones. Por tanto, $\mathscr{L}'$ tiene codimensión $\leq D$ o, equivalentemente, tiene dimensión ≥ 0. Luego, en particular, debe existir una curva en $\mathscr{L}$ que pase por $P_1, \ldots, P_s$.

□

Tenemos ahora las herramientas necesarias y suficientes para probar el Teorema de los nueve puntos.

Teorema 1.31. *Sea $\overline{\mathbb{K}}$ un cuerpo algebraicamente cerrado y sean $\mathcal{C}_F$ y $\mathcal{C}_G$ dos cúbicas contenidas en $\mathbb{P}\overline{\mathbb{K}}^2$ sin componentes en común y supongamos que tienen $P_1, \ldots, P_9$ puntos de intersección. Entonces cualquier cúbica $\mathcal{C}$ que pase por $P_1, \ldots, P_8$ pasa también por P_9.*

Demostración. Consideramos el haz de curvas $\mathscr{H}$ generado por $\mathcal{C}_F$ y $\mathcal{C}_G$. Si probamos que $\mathcal{C}$ está generada por $\mathcal{C}_F$ y $\mathcal{C}_G$, entonces por el Lema 1.26 ya estaría. Por reducción al absurdo, supongamos que $\mathcal{C}_F, \mathcal{C}_G$ y $\mathcal{C}$ generan un sistema lineal $\mathscr{L}$ de dimensión 2 y consideremos $Q_1, Q_2 \in \mathbb{P}\overline{\mathbb{K}}^2$. Por el Lema 1.30, existe al menos una curva proyectiva $\mathcal{C}' \in \mathscr{L}$ que pasa por Q_1 y Q_2. Nótese que en los P_i $(i = 0, 1, \ldots, 8)$ no puede haber cuatro alineados, puesto que si lo estuvieran, se obtendría que $\mathcal{C}_F$ y $\mathcal{C}_G$ tendrían cuatro puntos en común con la recta que une cuatro de esos puntos. Dado que son cúbicas, por el Teorema de Bézout, la recta debe ser una componente común de $\mathcal{C}_F$ y $\mathcal{C}_G$. De esta forma, se llega a que tienen infinitos puntos de intersección, lo cual contradice nuestra hipótesis inicial. Análogamente, no puede haber siete de los P_i que se encuentren sobre una misma cónica debido a que una cónica y una cúbica tienen seis puntos comunes, luego tendrían infinitos puntos de intersección, contradiciéndose de nuevo la hipótesis del teorema. Probado esto, consideremos los siguientes casos:
Caso 1. Supongamos que no hay tres puntos alineados y que no hay seis sobre una misma cónica (ver Figura 1.3). Sea $\mathcal{L}$ la recta que determinan P_1 y P_2 y sea $\mathcal{E}$ la cónica determinada por P_3, P_4, P_5, P_6 y P_7. Tomemos $\mathcal{C}'$ la cúbica que generan $\mathcal{C}_F, \mathcal{C}_G$ y $\mathcal{C}$ y que pasa por Q_1 y Q_2. Como $\mathcal{C}'$ debe pasar por los mismos puntos que $\mathcal{C}_F, \mathcal{C}_G$ y $\mathcal{C}$ por el Lema 1.30, se tiene en particular que $P_1, P_2 \in \mathcal{C}'$. De esta manera, se tiene que $P_1, P_2, Q_1, Q_2 \in \mathcal{C}' \cap \mathcal{L}$ y, por consiguiente, que $\mathcal{L}$ debe ser una componente de $\mathcal{C}'$ (por el Teorema de Bézout). Así pues, podemos escribir $\mathcal{C}' = \mathcal{L}\mathcal{E}'$, donde $\mathcal{E}'$ es una cónica. Probemos ahora que $\mathcal{E} = \mathcal{E}'$. Dado que $P_3, P_4, P_5, P_6, P_7 \in \mathcal{C}'$ por el Lema 1.30, entonces $P_3, P_4, P_5, P_6, P_7 \in \mathcal{E}'$. Tenemos que $\mathcal{E}$ y $\mathcal{E}'$ tienen cinco puntos en común, luego, por el Teorema de Bézout, o son coincidentes o tienen una recta en común. Demostremos que no puede ocurrir lo segundo. Si $\mathcal{E}$ y $\mathcal{E}'$ tuvieran una recta en común, en particular, las dos cónicas serían dos productos de rectas. Si a esto le añadimos que $P_3, P_4, P_5, P_6, P_7 \in \mathcal{E} \cap \mathcal{E}'$, entonces debe ocurrir que al menos tres de estos puntos estén alineados (por ser ambas cónicas productos de rectas). Sin embargo, estamos partiendo de que hay tres puntos alineados. Por tanto, $\mathcal{E}$ y $\mathcal{E}'$ son coincidentes. Tenemos entonces que $\mathcal{C}' = \mathcal{L}\mathcal{E}$. Por otra parte, como estamos partiendo de que no hay tres puntos alineados ni seis sobre una misma cónica, se tiene que $P_8 \notin \mathcal{L}$ y $P_8 \notin \mathcal{E}$ y, por ende, $P_8 \notin \mathcal{C}'$. Sin embargo, por el Lema 1.30, debe ocurrir que $P_8 \in \mathcal{C}'$, lo cual es una contradicción.

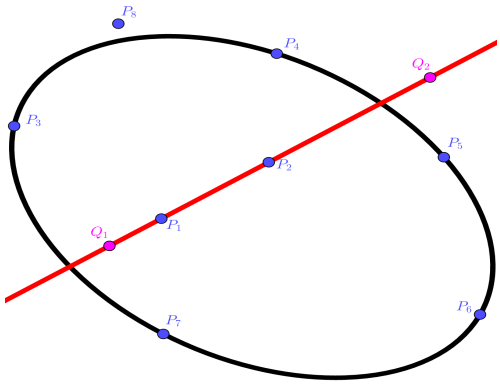

Figura 1.3. Caso 1.

Caso 2. Supongamos que los puntos P_1, P_2 y P_3 están alineados sobre la recta $\mathcal{L}_1$ y que los puntos P_4, P_5 y P_6 están sobre la recta $\mathcal{L}_2$. Tomemos $Q_1 \in \mathcal{L}_1$, con $Q_1 \neq P_1, P_2, P_3$ y $Q_2 \notin \mathcal{L}_1, \mathcal{L}_2$ ni en la recta que determinan P_7 y P_8 (ver Figura 1.4). También tomemos $\mathcal{C}'$ igual que en el caso anterior, entonces $P_1, P_2, P_3, Q_1 \in \mathcal{C}'$, i.e, $\mathcal{L}_1$ es una componente de $\mathcal{C}'$ y $\mathcal{C}' = \mathcal{E}\mathcal{L}_1$, donde $\mathcal{E}$ es una cónica. De esta forma, debe ocurrir que $P_4, P_5, P_6 \in \mathcal{E}$, esto es, la recta $\mathcal{L}_2$ es una componente de $\mathcal{E}$. Como consecuencia se tiene que $\mathcal{E} = \mathcal{L}_2\mathcal{L}'_2$ debe ser un producto de rectas. Por un lado tenemos que $Q_1 \notin \mathcal{L}_1, \mathcal{L}_2$ ni a la recta que determinan P_7 y P_8 y por otro que $P_7, P_8 \in \mathcal{C}'$ y que $P_7, P_8 \notin \mathcal{L}_1$. Entonces, $P_7, P_8 \in \mathcal{E}$. Además, como $P_7, P_8 \notin \mathcal{L}_2$, necesariamente $P_7, P_8 \in \mathcal{L}'_2$. Luego, $Q_2 \notin \mathcal{L}_1, \mathcal{L}_2, \mathcal{L}'_2$ y $Q_2 \in \mathcal{C}'$, lo cual es una contradicción.

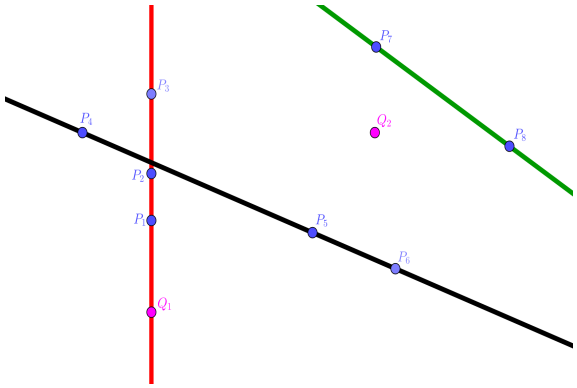

Figura 1.4. Caso 2.

Caso 3. Supongamos que P_1, P_2 y P_3 están alineados sobre una recta $\mathcal{L}$ y que de los puntos P_4, P_5, P_6, P_7 y P_8 no hay tres alineados. Entonces, P_4, P_5, P_6, P_7 y P_8 forman una cónica $\mathcal{E}$ irreducible. Tomemos $Q_1 \in \mathcal{L}$ y $Q_2 \notin \mathcal{L}, \mathcal{E}$ (ver Figura 1.5). De nuevo, consideramos $\mathcal{C}'$ como en los dos casos anteriores, entonces $P_i, Q_j \in \mathcal{C}'$ para cada $(i, j) \in \{1, \ldots, 8\} \times \{1, 2\}$ por el Lema 1.30. De aquí, se

llega a que $\mathcal{L}$ es una componente de $\mathcal{C}'$ ($\mathcal{C}' = \mathcal{L}\mathcal{E}'$), donde $\mathcal{E}'$ es una cónica. Por consiguiente, tenemos que $P_4, P_5, P_6, P_7, P_8 \in \mathcal{E} \cap \mathcal{E}'$. Por el Teorema de Bézout, deben ser coincidentes o tener una recta en común. Dado que $\mathcal{E}$ es irreducible, necesariamente debe ocurrir que $\mathcal{E} = \mathcal{E}'$. Por ende, $P_i, Q_j \in \mathcal{C}'$. Esto es una contradicción porque $Q_2 \notin \mathcal{L}, \mathcal{E}$.

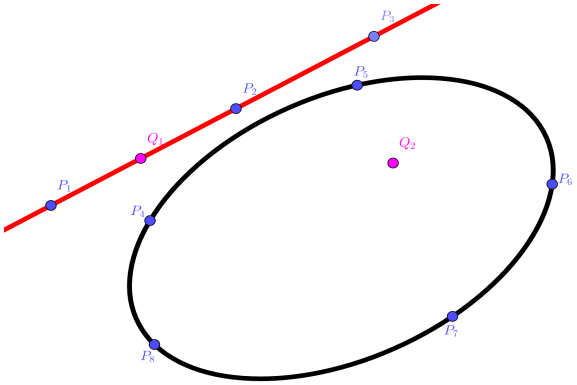

Figura 1.5. Caso 3.

Caso 4. Supongamos que $P_1, \ldots, P_6$ están sobre una cónica $\mathcal{E}$. Tomamos $Q_1 \in \mathcal{E}$ y $Q_2 \notin \mathcal{E}$ ni en la recta $\mathcal{L}$ determinada por P_7 y P_8 (ver Figura 1.6). Nuevamente tomamos $\mathcal{C}'$ como en los tres casos previos. Nótese que $\mathcal{E}$ es una componente de $\mathcal{C}'$ por el Teorema de Bézout, i.e, $\mathcal{C}' = \mathcal{E}\mathcal{L}$. Por tanto, llegamos a que $Q_2 \in \mathcal{C}'$, lo cual es una contradicción.

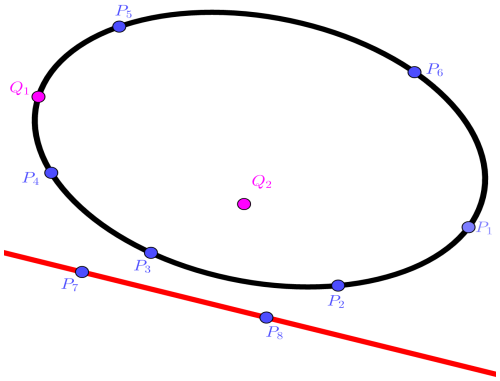

Figura 1.6. Caso 4.

Podemos concluir que $\mathcal{C}_F$, $\mathcal{C}_G$ y $\mathcal{C}$ no generan un sistema lineal de dimensión 2. De esta forma, se tiene que $\mathcal{C} \in \mathscr{H}$. Por el Lema 1.26, se concluye que $\mathcal{C}$ también pasa por P_9.

□

2

Grupos de Curvas Elípticas

En este capítulo definiremos el concepto de curva elíptica proyectiva en $\mathbb{PC}^2$ y veremos cómo podemos asociarle un grupo a partir de una operación binaria construída geométricamente. También estudiaremos el subgrupo que generan los puntos racionales de dichas curvas elípticas proyectivas. Para ello nos hemos basado en [1] y [2].

2.1. Curvas elípticas proyectivas

Gracias a la teoría expuesta en el Capítulo 1 podemos desarrollar el objetivo de esta sección y dar la definición de una curva elíptica proyectiva.

Definición 2.1. *Se dice que una curva plana proyectiva $\mathcal{C}$ en $\mathbb{PC}^2$ es una curva elíptica proyectiva cuando es una cúbica sin puntos singulares.*

2.1.1. Forma de Weierstrass

Dado que una curva elíptica $\mathcal{C}$ es una cúbica proyectiva, vendrá descrita por un polinomio de la forma

$$F(x,y,z) = \sum_{i+j+k=3} a_{ijk} x^i y^j z^k \in \mathbb{C}[x,y,z]. \tag{2.1}$$

Si desarrollamos la expresión (2.1) se obtiene

$$\begin{aligned} F(x,y,z) = {} & a_{300}x^3 + a_{210}x^2y + a_{201}x^2z + a_{111}xyz + a_{120}xy^2 + \\ & + \quad a_{102}xz^2 + a_{021}y^2z + a_{012}yz^2 + a_{030}y^3 + a_{003}z^3. \end{aligned} \tag{2.2}$$

La expresión (2.2) es poco manejable, así que utilizaremos otra que sea equivalente y que nos resulte más sencilla de utilizar. Para ello introducimos primero la siguiente definición.

Definición 2.2. *El polinomio de la forma*

$$F(x,y,z) = a(x-\alpha z)(x-\beta z)(x-\gamma z) - y^2 z \in \mathbb{C}[x,y,z], \tag{2.3}$$

que determina una cúbica proyectiva $\mathcal{C}$, se denomina forma de Weierstrass de $\mathcal{C}$.

Proposición 2.3. *Si una forma de Weierstrass como la recogida en (2.3) determina una curva elíptica proyectiva en $\mathbb{PC}^2$, entonces $\alpha, \beta, \gamma \in \mathbb{C}$ son distintos entre sí.*

Demostración. Sea $F(x,y,z) \in \mathbb{C}[x,y,z]$ una forma de Weierstrass, es decir, que F se puede escribir como sigue:

$$F(x,y,z) = a(x-\alpha z)(x-\beta z)(x-\gamma z) - y^2 z,$$

donde $a \in \mathbb{C}^*$ y $\alpha, \beta, \gamma \in \mathbb{C}$. Las derivadas parciales de F son

$$\begin{aligned} F_x(x,y,z) &= a\big[(x-\beta z)(x-\gamma z) + \\ &\quad + (x-\alpha z)(x-\gamma z) + (x-\alpha z)(x-\beta z)\big], \qquad (2.4)\\ F_y(x,y,z) &= -2yz, \qquad (2.5)\\ F_z(x,y,z) &= a\big[-\alpha(x-\beta z)(x-\gamma z) - \beta(x-\alpha z)(x-\gamma z) - \\ &\quad - \gamma(x-\alpha z)(x-\beta z)\big] - y^2. \qquad (2.6) \end{aligned}$$

Por contrarrecíproco, supongamos que $\alpha, \beta, \gamma \in \mathbb{C}$ no son distintos dos a dos, es decir, que podemos suponer sin pérdida de generalidad que $\alpha = \beta$. Si sustituimos $\alpha = \beta$ en (2.4), (2.5) y (2.6) obtenemos que

$$\begin{cases} F_x(x,y,z) = a\big[2(x-\alpha z)(x-\gamma z) + (x-\alpha z)^2\big], \\ F_y(x,y,z) = -2yz, \\ F_z(x,y,z) = a\big[-2\alpha(x-\alpha z)(x-\gamma z) - \gamma(x-\alpha z)^2\big] - y^2. \end{cases}$$

Nótese que si tomamos $P = (\alpha : 0 : 1) \in \mathbb{PC}^2$, entonces $F_x(P) = F_y(P) = F_z(P) = 0$. Por tanto, podemos concluir que $\mathcal{C}$ no es una curva elíptica puesto que P es un punto singular de $\mathcal{C}$.

□

Establecemos ahora el siguiente resultado.

Lema 2.4. *Cualquier curva elíptica $\mathcal{C}' \subset \mathbb{PC}^2$ es proyectivamente equivalente a otra curva elíptica $\mathcal{C} \subset \mathbb{PC}^2$ que está determinada por una forma de Weierstrass.*

Demostración. Sean $P_1, P_3 \in \mathcal{C}'$ y $P_2,\ P_4 \notin \mathcal{C}'$. Podemos suponer, sin pérdida de generalidad, que P_1, P_2, P_3 y P_4 están en posición general. En particular, asumamos que P_1, P_2 y P_3 son los puntos no colineales. Sabiendo que P_1 y P_2 determinan una recta $\mathcal{L}_{P_1,P_2}$ y aplicando el Lema 1.17, enviamos P_1 a $E_1 = (1 : 0 : 0)$ y $\mathcal{L}_{P_1,P_2}$ a $\mathcal{L}_1 \equiv z = 0$. Consideremos $\mathcal{L}_1$ la recta tangente a $\mathcal{C}$ en E_1 y supongamos que el segundo punto de intersección de $\mathcal{L}_1$ con $\mathcal{C}$ es $E_2 = (0 : 1 : 0)$. Tomemos la recta $\mathcal{L}_2 \equiv x = 0$ como la recta tangente a $\mathcal{C}$ en E_2. Dado que $E_1,\ E_2 \in \mathcal{C}$, se verifica que $F(1,0,0) = F(0,1,0) = 0$ o equivalentemente $a_{300} = a_{030} = 0$; es decir, F tiene la siguiente forma:

$$\begin{aligned} F(x,y,z) = a_{210}x^2y + a_{201}x^z + a_{111}xyz + a_{120}xy^2 + a_{102}xz^2 + a_{021}y^2z + \\ + a_{012}yz^2 + a_{003}z^3. \end{aligned}$$

Calculando la derivadas parciales de F y evaluando en E_1 y E_2 se tiene

$$\begin{cases} F_x(1,0,0) = 0, & F_x(0,1,0) = a_{120}, \\ F_y(1,0,0) = a_{210}, & F_y(0,1,0) = 0, \\ F_z(1,0,0) = a_{201}, & F_z(0,1,0) = a_{021}. \end{cases}$$

Además, como E_1 y E_2 son puntos no singulares, podemos asumir, sin pérdida de generalidad, que $a_{210} = a_{021} = 0$ y $a_{201},\ a_{120} \neq 0$. Obsérvese que ahora F tiene la expresión

$$F(x,y,z) = a_{201}x^2z + a_{111}xyz + a_{120}xy^2 + a_{102}xz^2 + a_{012}yz^2 + a_{003}z^3.$$

Si deshomogenizamos respecto de z tenemos

$$F(x,y,1) = a_{201}x^2 + a_{111}xy + a_{120}xy^2 + a_{102}x^2 + a_{012}y + a_{003}.$$

Igualando a 0, dividiendo por a_{120} y reagrupando los términos de la izquierda en función de la variable y se llega a que $xy^2 + (ax + b)y = cx^2 + dx + e$. Si multiplicamos la expresión por x, obtenemos que $(xy)^2 + (ax + b)xy = cx^3 + dx^2 + ex$. Ahora, consideramos el cambio de variable $v = xy$ y $u = x$ para llegar a la expresión $v^2 + (au + b)v = cu^3 + du^2 + eu$. Completando cuadrados en el primer miembro se verifica

$$v^2 + (au + b)v - \frac{1}{4}(au + b)^2 + \frac{1}{4}(au + b)^2 = cu^3 + du^2 + eu.$$

Y si operamos a la izquierda de la igualdad, entonces

$$\left(u + \frac{1}{2}(au + b)\right)^2 - \frac{1}{4}(au + b)^2 = cu^3 + du^2 + eu.$$

Si utilizamos el cambio de variable $\psi = v - \frac{1}{2}(au + b)$ y $\varphi = u$, se tiene que $\psi^2 = p(\varphi)$, donde $p(\varphi) \in \mathbb{C}[\varphi]$ y $deg(p(\varphi)) = 3$. O sea, hemos obtenido la

expresión de una cúbica de la forma $y^2 = p(x)$, con $p(x) \in \mathbb{C}[x]$ de grado 3. Si ahora aplicamos el Teorema Fundamental del Álgebra, se cumple que $y^2 = a(x-\alpha)(x-\beta)(x-\gamma)$, con $a \in \mathbb{C}^*$ y $\alpha, \beta, \gamma \in \mathbb{C}$ distintos entre sí por la Proposición 2.3. Por último, homogenizamos respecto de la variable z y, por consiguiente, $y^2z = a(x-\alpha z)(x-\beta z)(x-\gamma z)$. Por tanto, la expresión resultante corresponde al polinomio $F(x,y,z) = a(x-\alpha z)(x-\beta z)(x-\gamma z) - y^2z$. Concluimos que F es una forma de Weierstrass.

□

A partir de ahora la expresión recogida en (2.3) la tomaremos mónica puesto que determinan la misma curva elíptica proyectiva. Si además la desarrollamos, la podemos expresar como

$$F(x,y,z) = x^3 + ax^2z + bxz^2 + cz^3 - y^2z, \tag{2.7}$$

para ciertos $a, b, c \in \mathbb{C}$. Por tanto, de ahora en adelante supondremos que una curva elíptica proyectiva $\mathcal{C}$ está dada por la ecuación $\mathcal{C} \equiv y^2z = x^3 + ax^2 + bxz^2 + cz^3$. Además, dado que en la Subsección 1.2.1 estudiamos que el plano proyectivo es el plano afín unido a los puntos en el infinito, entonces una curva elíptica proyectiva es la unión de los puntos $(x : y : 1)$, donde (x, y) son los puntos de su vista afín para $z = 1$, dada por $f(x, y) = x^3 + ax^2 + bx + c$; junto con sus puntos en el infinito. Sin embargo, sólo existe un único punto en el infinito para la vista afín $z = 1$. En efecto, sean $\mathcal{C}$ una curva elíptica proyectiva determinada por la expresión (2.7) y $\mathcal{L} \equiv z = 0$ la recta del infinito. Si intersecamos $\mathcal{C}$ con $\mathcal{L}$, se comprueba que $x^3 = 0$, esto es, $x = 0$. Luego, $P = (0 : 1 : 0)$ es el único punto en el infinito de $\mathcal{C}$. Además, por el Teorema de Bézout tenemos que $I(P, \mathcal{C}, \mathcal{L}) = 3$, es decir, el punto en el infinito es un punto de inflexión con coordenadas enteras.

2.2. Estructura de Grupo

En esta sección definiremos una operación binaria, que se obtiene por construcción geométrica a través de otra operación binaria definida previamente, que nos permitirá dotar a los puntos de las curvas elípticas proyectivas con una estructura de grupo. Para ello, enunciamos y demostramos el siguiente resultado.

Lema 2.5. *Sean $\mathcal{C}$ una curva elíptica y $\mathcal{L}$ una recta en $\mathbb{PC}^2$. Entonces $\mathcal{C}$ y $\mathcal{L}$ no tienen componentes en común.*

Demostración. Sean $\mathcal{C}, \mathcal{L} \subset \mathbb{PC}^2$ una curva elíptica y una recta, respectivamente. Entonces, en particular, $\mathcal{C}$ no tiene puntos singulares. Además, sean F,

$G \in \mathbb{C}[x, y, z]$ los polinomios de grado 3 y 1 asociados a $\mathcal{C}$ y $\mathcal{L}$, respectivamente, y supongamos que ambas curvas tienen componentes en común. Entonces $F = GH$, donde $H \in \mathbb{C}[x, y, z]$ define una cónica proyectiva $\mathcal{C}'$. Si aplicamos el Teorema de Bézout, $\mathcal{L}$ y $\mathcal{C}'$ tienen al menos un punto de intersección $P \in \mathbb{PC}^2$. Por otro lado, si hallamos las derivadas parciales de F y evaluamos en P tenemos que

$$\begin{cases} F_x(P) = G_x(P)H(P) + G(P)H_x(P) = 0, \\ F_y(P) = G_y(P)H(P) + G(P)H_y(P) = 0, \\ F_z(P) = G_z(P)H(P) + G(P)H_z(P) = 0. \end{cases}$$

Dado que P anula simultáneamente las derivadas parciales de F, se tiene que P es un punto singular de $\mathcal{C}$. Esto es una contradicción, ya que estamos partiendo de una curva sin puntos singulares.

□

Corolario 2.6. *Toda curva elíptica proyectiva $\mathcal{C} \subset \mathbb{PC}^2$ es irreducible.*

Demostración. Sea $\mathcal{C} \subset \mathbb{PC}^2$ una curva elíptica proyectiva determinada por $F(x, y, z) \in \mathbb{C}[x, y, z]$ homogéneo y supongamos que no es irreducible. Entonces existen $G(x, y, z), H(x, y, z) \in \mathbb{C}[x, y, z]$ homogéneos no constantes tales que $F = GH$. Como $deg(F) = 3$, necesariamente debe ocurrir que $deg(G) = 1$ o $deg(H) = 1$, es decir, que $\mathcal{C}$ contiene una recta, lo cual es absurdo por el Lema 2.5.

□

2.2.1. La Operación Binaria *

El Lema 2.5 nos sirve para afirmar, junto con el Teorema de Bézout, que una curva elíptica y una recta se intersecan en exactamente tres puntos (contadas multiplicidades). Este hecho motiva a definir la siguiente operación binaria: sean $P, Q \in \mathbb{PC}^2$. Si $P \neq Q$, denotamos por $\mathcal{L}_{P,Q}$ a la recta que pasa por P y Q. Si $P = Q$, denotamos por $\mathcal{L}_{P,P}$ a la recta tangente a $\mathcal{C}$ en P. Obsérvese que si C es una curva elíptica proyectiva y $P, Q \in \mathcal{C}$, entonces $\mathcal{C}$ y $\mathcal{L}_{P,Q}$ tienen un tercer punto en común que denotaremos por $P * Q$. En las Figuras 2.1 y 2.2 se muestra cómo funciona la operación $*$.

Lema 2.7. *Sea $\mathcal{C}$ una curva elíptica contenida en $\mathbb{PC}^2$. La correspondencia*

$$\begin{aligned} *\colon\ & \mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C} \\ & (P, Q) \longmapsto R = P * Q \end{aligned}$$

es ley de composición interna.

Demostración. Supongamos que $P \neq Q$, por el Lema 2.5 y por el Teorema de Bézout, la recta que determinan P y Q tiene exactamente tres puntos de intersección con $\mathcal{C}$, i.e, como P, $Q \in \mathcal{C}$, necesariamente $P * Q$ debe ser el tercer punto de intersección por cómo hemos definido $*$. Por tanto, $P*Q \in \mathcal{C}$ y además es único. Supongamos que $P = Q$ y consideremos la recta tangente $\mathcal{L}_{P,P}$ a $\mathcal{C}$ en P. Si P es un punto de inflexión, entonces el tercer punto de intersección de $\mathcal{C}$ con $\mathcal{L}_{P,P}$ vuelve a ser P puesto que $I(P, \mathcal{C}, \mathcal{L}_{P,P}) = 3$. Por otro lado, si P no es un punto de inflexión, se tiene que $\mathcal{C}$ y $\mathcal{L}_{P,P}$ se intersecan en otro punto $P * P$ ya que $I(P, \mathcal{C}, \mathcal{L}_{P,P}) = 2$. De nuevo, por el Lema 2.5 y el Teorema de Bézout, se cumple que $P * P \in \mathcal{C}$ y es único.

□

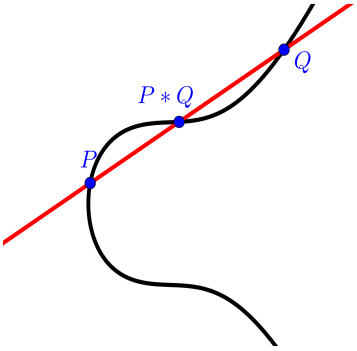

Figura 2.1. Operación $*$ con $P \neq Q$.

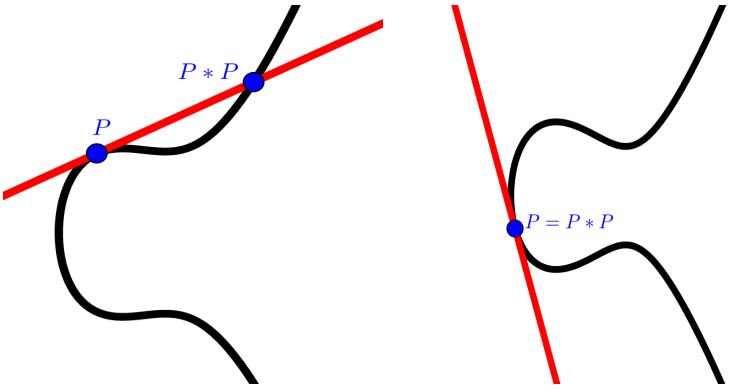

Figura 2.2. Operación $*$ con $P = Q$ no inflexión e inflexión, respectivamente.

Lema 2.8. *Sea $\mathcal{C}$ una curva elíptica contenida en $\mathbb{PC}^2$ y sean $P, Q, R, S \in \mathcal{C}$. Entonces la operación $*$ definida en el Lema 2.7 verifica las siguientes propiedades:*

1. $P * Q = Q * P$.
2. $(P * Q) * P = Q$.
3. $((P * Q) * R) * S = P * ((Q * S) * R)$.

Demostración. Dado que $P * Q$ es el tercer punto de intersección de la recta que forman P y Q con $\mathcal{C}$, por definición de $*$ se tiene que $P * Q = Q * P$. Además, si consideramos la recta que definen P y $P*Q$, el punto de intersección con $\mathcal{C}$ necesariamente debe ser Q (ver Figura 2.1). Por otro lado, sean $X := ((P * Q) * R) * S$, $Y := P * ((Q * S) * R) \in \mathcal{C}$ y consideramos las cúbicas proyectivas $\mathcal{C}_1 = \mathcal{L}_{P,Q} \cdot \mathcal{L}_{Q*S,R} \cdot \mathcal{L}_{(P*Q)*R,S}$ y $\mathcal{C}_2 = \mathcal{L}_{Q,S} \cdot \mathcal{L}_{P*Q,R} \cdot \mathcal{L}_{(Q*S)*R,P}$ (observar la Figura 2.3). Por el Teorema de Bézout y por cómo hemos definido la curva $\mathcal{C}_1$, tenemos que $\mathcal{C}$ y $\mathcal{C}_1$ se intersecan en P, Q, R, S, $P * Q$, $Q * S$, $(Q * S) * R$, $(P * Q) * R$ y X . Nótese también, que por la definición de $\mathcal{C}_2$, se cumple que P, Q, R, S, $P * Q$, $Q * S$, $(Q * S) * R$, $(P * Q) * R \in \mathcal{C}_2$. Luego, si aplicamos el Teorema 1.31 debe ocurrir que $X \in \mathcal{C}_2$. Análogamente, se llega a que $Y \in \mathcal{C}_1$. Por tanto, si nuevamente hacemos uso del Teorema de Bézout, obtenemos que $X = Y$.

□

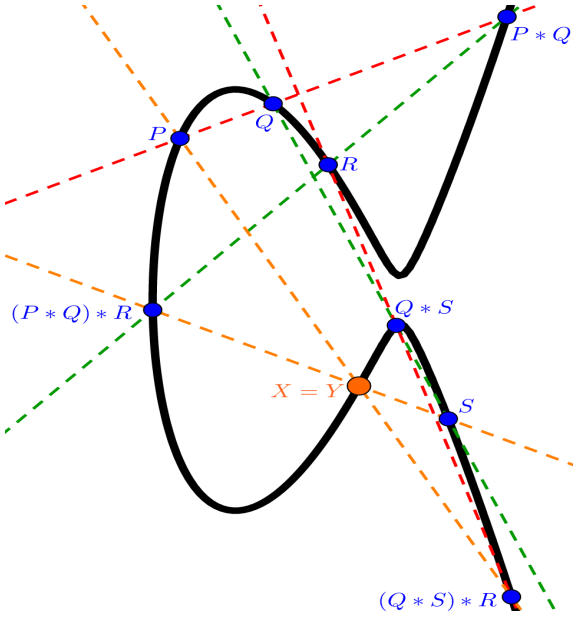

Figura 2.3. $((P * Q) * R) * S = P * ((Q * S) * R)$.

A pesar de que $*$ cumple las propiedades probadas en el Lema 2.8, la operación $*$ no resulta suficiente para dotar a las curvas elípticas proyectivas con una estructura de grupo puesto que $(\mathcal{C}, *)$ carece de elemento neutro. En efecto, supongamos que existe $O \in \mathcal{C}$ tal que $O * P = P$ para todo $P \in \mathcal{C}$.

Entonces, la recta $\mathcal{L}_{O,P}$ coincide con la recta tangente en P a $\mathcal{C}$ ($\mathcal{L}_{P,P}$). Luego, se cumple que para todo $P \in \mathcal{C}$, el punto O pertenece a $\mathcal{L}_{P,P}$, es decir, todas las rectas tangentes a $\mathcal{C}$ en todos sus puntos pasan por O. Sin embargo, esto no puede ocurrir ya que contradice al *Teorema de Samuel*, el cual se puede encontrar en el Teorema 3.9 en la página 312 de [8].

2.2.2. La Operación Binaria +

Aunque en la Subsección 2.2.1 hemos probado que la operación $*$ definida en el Lema 2.7 no puede proporcionar estructura de grupo a las curvas elípticas proyectivas, sí que la podemos utilizar para definir una operación que reúne las condiciones necesarias para tal fin.

Lema 2.9. *Sean $\mathcal{C}$ una curva elíptica contenida en $\mathbb{PC}^2$ y $O \in \mathcal{C}$ un punto. La correspondencia*

$$\begin{aligned} +\colon\ & \mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C} \\ & (P, Q) \longmapsto R = P + Q = (P * Q) * O \end{aligned}$$

es ley de composición interna.

Demostración. Es una consecuencia del Lema 2.7.

□

Se muestra en la Figura 2.4 la interpretación geométrica de la operación +.

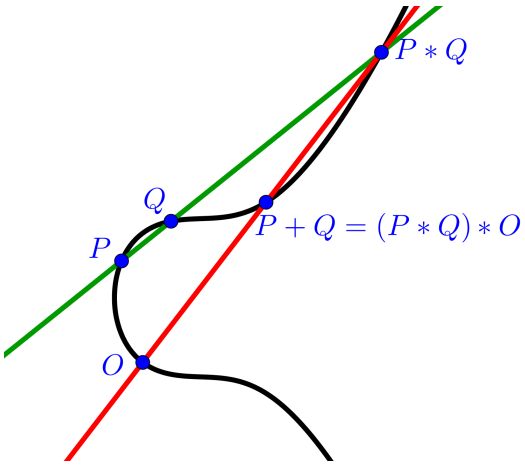

Figura 2.4. Operación +.

Obsérvese que si tomamos $O = (0 : 1 : 0)$ el punto en el infinito de $\mathcal{C}$, entonces la operación + tiene un funcionamiento *especial*. Dados dos puntos $P, Q \in \mathcal{C}$ y considerando $P * Q$, se tiene que $P + Q = (P * Q) * O$ es la intersección de la

recta paralela a $x = 0$ que pasa por $P * Q$ con $\mathcal{C}$. Esto significa que $P + Q$ es el punto simétrico a $P * Q$ respecto al eje X. En el caso en el que $P = Q$, la operación $+$ funciona igual, pero tomando la recta tangente a $\mathcal{C}$ en P. En la Figura 2.5 puede apreciarse la operación $+$ cuando $O = (0 : 1 : 0)$.

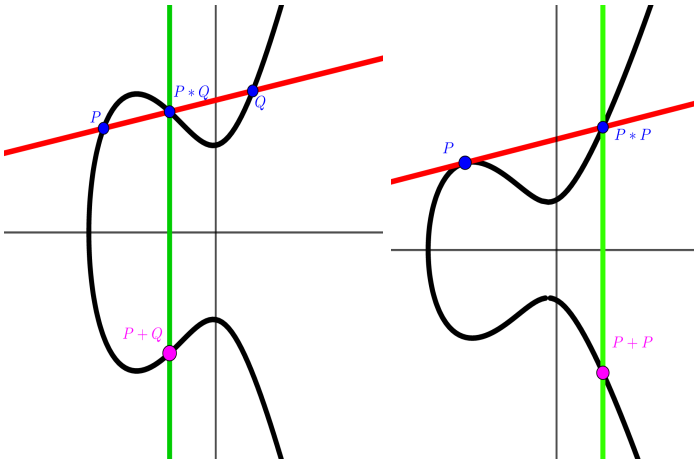

Figura 2.5. Operación $+$ cuando $O = (0 : 1 : 0)$.

2.2.3. Grupo Asociado a una Curva Elíptica

Con la teoría desarrollada en este capítulo ya disponemos de las condiciones necesarias para enunciar y demostrar el teorema siguiente.

Teorema 2.10. *Sea $\mathcal{C}$ una curva elíptica contenida en $\mathbb{PC}^2$ y sea $+$ la operación definida en el Lema 2.9. Entonces el par $(\mathcal{C}, +)$ es un grupo abeliano.*

Demostración. Fijamos $O \in \mathcal{C}$. En primer lugar, obsérvese que $\mathcal{C} \neq \emptyset$, puesto que se trata de una curva. Demostraremos el resto de condiciones aplicando el Lema 2.8 y la propia definición de $+$.

1. **Asociatividad**. Sean P, Q, $R \in \mathcal{C}$. Entonces, por la definición de $+$ se tiene que $(P+Q)+R = ((P+Q)*R)*O = (((P*Q)*O)*R)*O$. Si aplicamos que $*$ es conmutativa, se cumple que $(((P*Q)*O)*R)*O = ((O*(P*Q))*R)*O$. Si utilizamos la tercera propiedad del Lema 2.8, tenemos

$$((O * (P * Q)) * R) * O = O * (((P * Q) * O) * R).$$

De nuevo, podemos hacer uso de la conmutatividad de $*$ para obtener

$$O * (((P * Q) * O) * R) = (((P * Q) * O) * R) * O.$$

Nuevamente, de la tercera propiedad del Lema 2.8 llegamos a

$$(((P * Q) * O) * R) * O = (P * ((Q * R)) * O) * O.$$

Por último, si usamos una vez más la definición de $+$, concluimos

$$(P * ((Q * R)) * O) * O = (P * (Q + R)) * O = P + (Q + R).$$

2. **Conmutatividad**. Sean $P, Q \in \mathcal{C}$. De la definición de $+$ y la conmutatividad de $*$ se cumple que $P + Q = (P * Q) * O = (Q * P) * O = Q + P$.
3. **Existencia de elemento neutro**. Afirmamos que $O \in \mathcal{C}$ es el elemento neutro. En efecto, sea $P \in \mathcal{C}$. Si aplicamos la segunda propiedad del Lema 2.8, llegamos a que $O + P = (O * P) * O = P$.
4. **Existencia de elemento opuesto**. Sea $P \in \mathcal{C}$. Afirmamos que el opuesto de P es $-P := P * (O * O) \in \mathcal{C}$. En efecto, $P + (-P) = P + (P * (O * O))$. Por la definición de $+$, se tiene que $P + (P * (O * O)) = (P * (P * (O * O))) * O$. Si utilizamos la propiedad conmutativa de $*$, obtenemos que

$$(P * (P * (O * O))) * O = ((P * (O * O)) * P) * O.$$

Finalmente, si hacemos uso de la segunda propiedad del Lema 2.8, podemos concluir que $((P * (O * O)) * P) * O = (O * O) * O = O$.

□

Obsérvese que cuando tomamos como neutro al punto $O = (0 : 1 : 0)$, entonces el opuesto de un punto $P = (x : y : 1)$ es $-P = (x : -y : 1)$ al ser $+$ una simetría respecto del eje X como vimos en la Subsección 2.2.2. En las Figuras 2.6, 2.7 y 2.8 mostramos gráficamente las propiedades demostradas en el Teorema 2.10.

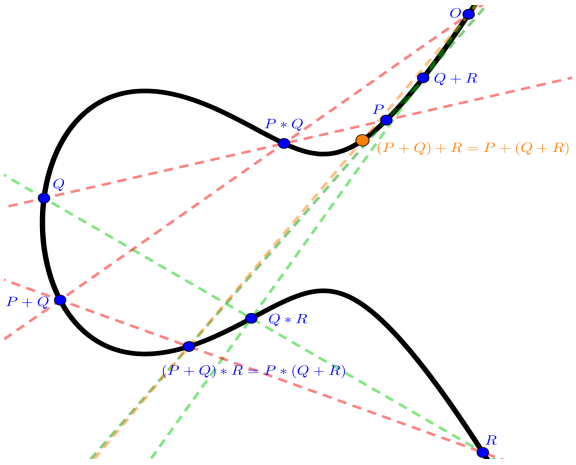

Figura 2.6. Asociatividad de $+$.

Hemos demostrado que dada una curva elíptica $\mathcal{C}$ y fijado un punto $O \in \mathcal{C}$, por el Teorema 2.10 se tiene que el par $(\mathcal{C}, +)$ es un grupo abeliano, donde $+$

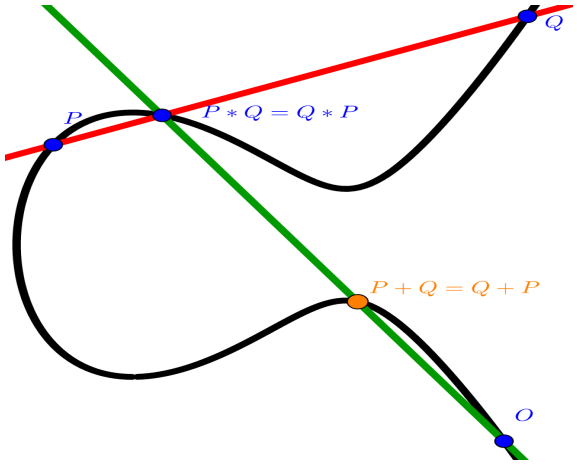

Figura 2.7. Conmutatividad de $+$.

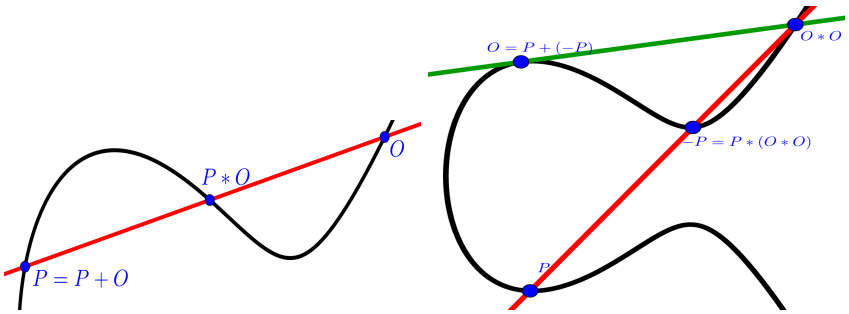

Figura 2.8. Existencia de elemento neutro y opuesto, respectivamente.

es la operación binaria definida en el Lema 2.9. A raíz de este resultado, cabe plantearse si este grupo depende del punto base que hemos fijado, es decir, ¿qué ocurre si fijamos otro punto base $O' \in \mathcal{C}$? La respuesta a esta cuestión nos la proporciona la siguiente proposición.

Proposición 2.11. *Sea $\mathcal{C} \subset \mathbb{PC}^2$ una curva elíptica y sean O, $O' \in \mathcal{C}$ dos puntos fijos. Entonces los grupos $(\mathcal{C}, +)$ y $(\mathcal{C}, +')$ asociados a O y O', respectivamente, son isomorfos.*

Demostración. Sea $(\mathcal{C}, +)$ el grupo asociado a $\mathcal{C}$ respecto del punto O y sea $(\mathcal{C}, +')$ el grupo asociado a $\mathcal{C}$ respecto del punto O'. Tomemos el punto $A := O * O'$ y definamos la siguiente correspondencia:

$$\begin{aligned} \Phi\colon\ (\mathcal{C}, +) &\longrightarrow (\mathcal{C}, +') \\ P &\longmapsto \Phi(P) = A * P. \end{aligned}$$

Afirmamos que Φ es un isomorfismo de grupos. En efecto,

1. Φ es aplicación por el Lema 2.7.
2. Φ es biyectiva:

- Φ es inyectiva. Sean P, $Q \in \mathcal{C}$ tales que $\Phi(P) = \Phi(Q)$. Entonces por definición de Φ, se tiene que $A * P = A * Q$. Si operamos por la derecha de ambos miembros de la igualdad por A, obtenemos que $(A * P) * A = (A * Q) * A$. Por tanto, si aplicamos la segunda propiedad del Lema 2.8, se cumple que $P = Q$.
- Φ es sobreyectiva. Sea $Q \in \mathcal{C}$. Consideremos $P := A * Q \in \mathcal{C}$. Tenemos que $\Phi(P) = \Phi(A * Q)$, i.e, $A * P = A * (A * Q)$. Esta expresión es la misma que $A * P = A * (Q * A)$ por la conmutatividad de $*$. Además, si aplicamos la segunda propiedad del Lema 2.8, obtenemos que $A * P = Q$.

3. Φ es homomorfismo de grupos. En efecto, sean P, $Q \in \mathcal{C}$. Por la definición de $+'$, se observa que

$$\Phi(P) +' \Phi(Q) = (A * P) +' (A * Q) = ((A * P) * (A * Q)) * O'.$$

De la propiedad conmutativa de $*$ tenemos

$$((A * P) * (A * Q)) * O' = ((A * P) * (Q * A)) * O'.$$

Por la tercera propiedad del Lema 2.8 obtenemos

$$((A * P) * (Q * A)) * O' = A * ((P * O') * (Q * A)).$$

Nuevamente, por la propiedad conmutativa de $*$ se tiene

$$A * ((P * O') * (Q * A)) = A * ((P * O') * (A * Q)) = A * ((A * Q) * (P * O')).$$

Ahora aplicamos la conmutatividad de $*$ y que $A = O * O'$ y llegamos a

$$A * ((A * Q) * (P * O')) = A * (((O * O') * Q) * (P * O')).$$

De nuevo, si hacemos uso de la tercera propiedad del Lema 2.8, tenemos

$$A * (((O * O') * Q) * (P * O')) = A * (O * (O' * (P * O') * Q)).$$

Utilizamos la primera y segunda propiedad del Lema 2.8:

$$A * (O * (O' * (P * O') * Q)) = A * (O * (P * Q)).$$

Por último, usamos la conmutatividad de $*$ y la definición de $+$ para concluir que

$$A * (O * (P * Q)) = A * ((P * Q) * O) = A * (P + Q) = \Phi(P + Q).$$

Luego Φ es un isomorfismo de grupos y por tanto los grupos $(\mathcal{C}, +)$ y $(\mathcal{C}, +')$ son isomorfos.

□

La siguiente proposición muestra el comportamiento de los grupos asociados a dos curvas equivalentes por transformaciones proyectivas.

Proposición 2.12. *Sean $\mathcal{C}$ y $\mathcal{C}'$ dos curvas elípticas contenidas en $\mathbb{PC}^2$. Si $\mathcal{C}$ y $\mathcal{C}'$ son proyectivamente equivalentes, entonces sus grupos asociados son isomorfos.*

Demostración. Sean $O \in \mathcal{C}$ y $O' \in \mathcal{C}'$ los neutros de los grupos $(\mathcal{C}, +)$ y $(\mathcal{C}', +')$, respectivamente. Como $\mathcal{C}$ y $\mathcal{C}'$ son equivalentes por transformaciones proyectivas, entonces existe $\Phi\colon\ \mathcal{C} \longrightarrow \mathcal{C}'$ aplicación proyectiva de tal manera que $\Phi(O) = O'$ y recíprocamente $\Phi^{-1}(O') = O$. En particular, todos los puntos de $\mathcal{C}$ son enviados por Φ a todos los puntos de $\mathcal{C}'$. Probemos ahora que Φ es un isomorfismo de grupos. Como Φ es una aplicación proyectiva, Φ es un isomorfismo lineal, es decir, que Φ es una aplicación lineal biyectiva. Luego, sólo nos hace falta demostrar que Φ es un homomorfismo de grupos. Para ello, primero vamos a mostrar que dados dos puntos P, $Q \in \mathcal{C}$, entonces $\Phi(P * Q) = \Phi(P) * \Phi(Q)$. Lo hacemos por casos:

1. Supongamos que $P \neq Q$. Sabemos entonces por el Teorema de Bézout que $P * Q$ es el tercer punto de intersección de $\mathcal{C}$ con la recta $\mathcal{L}_{P,Q}$. Nótese que como $\Phi(P) \neq \Phi(Q)$, debe ocurrir que $\Phi(P) * \Phi(Q)$ sea el tercer punto de intersección de $\mathcal{L}_{\Phi(P),\Phi(Q)}$ con $\mathcal{C}'$. Como $\Phi(\mathcal{L}_{P,Q}) = \mathcal{L}_{\Phi(P),\Phi(Q)}$, se llega a que $\Phi(P) * \Phi(Q) = \Phi(P * Q)$.
2. Supongamos ahora que $\mathcal{L}_{P,Q}$ es tangente a $\mathcal{C}$ en P (respectivamente en Q). Entonces, se tiene que $P * Q = P$ (respectivamente $P * Q = Q$). Luego, $\Phi(\mathcal{L}_{P,Q})$ es tangente a $\mathcal{C}'$ en $\Phi(P)$ (respectivamente en $\Phi(Q)$), es decir, que debe ocurrir que $\Phi(P*Q) = \Phi(P) = \Phi(P)*\Phi(Q)$ (respectivamente $\Phi(P*Q) = \Phi(Q) = \Phi(P) * \Phi(Q)$).
3. Si suponemos que $P = Q$ y que no es un punto de inflexión, entonces $\mathcal{L}_{P,P}$ es la recta tangente a $\mathcal{C}$ en P y, además, $P * P$ es el segundo punto de intersección de $\mathcal{L}_{P,P}$ con $\mathcal{C}$. Como $\Phi(P) = \Phi(Q)$, se cumple que $\Phi(\mathcal{L}_{P,P})$ es la recta tangente a $\mathcal{C}'$ en $\Phi(P)$ y $\Phi(P * P)$ es el punto simple donde $\Phi(\mathcal{L}_{P,P}) = \mathcal{L}_{\Phi(P),\Phi(P)}$ se interseca con $\mathcal{C}'$, entonces se tiene que $\Phi(P * P) = \Phi(P) * \Phi(P)$.
4. Por último, supongamos que $P = Q$ es un punto de inflexión. Entonces $\Phi(P) = \Phi(Q)$ es un punto de inflexión y por tanto $\Phi(P * Q) = \Phi(P) = \Phi(P) * \Phi(Q)$.

Se sigue de aquí que Φ es un homomorfismo puesto que:

$$\begin{aligned}\Phi(P + Q) = \Phi((P * Q) * O) = \Phi(P * Q) * \Phi(O) = \\ = (\Phi(P) * \Phi(Q)) * O' = \Phi(P) +' \Phi(Q).\end{aligned}$$

□

En la práctica resulta de mayor utilidad elegir como punto base un punto de inflexión. Nótese que en este caso $O * O = O$ y como consecuencia $-P = P * O$.

Lema 2.13. *Sea $\mathcal{C} \subset \mathbb{PC}^2$ una curva elíptica. Sean $P, Q, R, O \in \mathcal{C}$, donde O es un punto de inflexión. Se tiene:*

1. *Si P, Q y R son distintos entre sí, entonces $P + Q + R = O$ si, y sólo si, P, Q y R son colineales.*
2. *$P \neq O$ tiene orden 2 si, y sólo si, la recta tangente a $\mathcal{C}$ en P pasa por O.*
3. *$P \neq O$ tiene orden 3 si, y sólo si, P es un punto de inflexión.*

Demostración. 1. Supongamos que P, Q y R son colineales, entonces $P*Q = R$. Si calculamos $P+Q+R$, se tiene que $P+Q+R = ((P*Q)*O)+R = (((P*Q)*O)*R)*O$. Cambiamos $P*Q$ por R para obtener que $(((P*Q)*O)*R)*O = ((R*O)*R)*O$. Si aplicamos la segunda propiedad del Lema 2.8, se tiene que $((R*O)*R)*O = O*O$. Además, como O es un punto de inflexión, podemos concluir que $P+Q+R = O$. Supongamos ahora que $P+Q+R = O$, entonces $1P+Q = -R$. Como O es un punto de inflexión, se tiene que $(P+Q) = R*O$ o, equivalentemente, $(P*Q)*O = R*O$. Si operamos en ambos miembros a la derecha por O, se llega a que $((P*Q)*O)*O = (R*O)*O$ es equivalente a $(P*Q)+O = R+O$ y por tanto, $P*Q = R$, es decir, que P, Q y R son colineales.

2. Un punto $P \neq O$ tiene orden 2 si, y sólo si, $P+P = O$. Equivalentemente, se tiene que $(P*P)*O = O$. Si operamos por la derecha de ambos miembros por O, obtenemos que $((P*P)*O)*O = O*O$. Como O es un punto de inflexión, entonces $(P*P)+O = O$, es decir, que $P*P = O$. De aquí, se concluye que la recta tangente a $\mathcal{C}$ en P pasa por O. Recíprocamente, si la recta tangente a $\mathcal{C}$ en P pasa por O, se cumple que $P*P = O$. Si operamos a la derecha de ambos miembros por O, se verifica que $(P*P)*O = O*O$. Como O es un punto de inflexión, entonces $P+P = O$ y, por consiguiente, P es de orden 2.

3. Supongamos que $P \neq O$ es un punto de inflexión de $\mathcal{C}$, entonces $P*P = P$. Si operamos a la derecha de ambos miembros por O, se cumple que $(P*P)*O = P*O$. Dado que O es un punto de inflexión, se verifica que $P+P = -P$, es decir, que $P+P+P = O$. Por tanto, P tiene orden 3. Recíprocamente, supongamos que $P \neq O$ tiene orden 3, esto es, $P+P+P = O$ o, equivalentemente, $P+P = -P$. Como O es un punto de inflexión, se tiene que $(P*P)*O = P*O$. Por tanto, si operamos por la derecha de ambos miembros por O, se llega a que $((P*P)*O*)O = (P*O)*O$. Esto es equivalente a que $(P*P)+O = (O*P)*O$. Si aplicamos la segunda propiedad del Lema 2.8, se concluye que $P*P = P$ y, por consiguiente, que P es un punto de inflexión.

□

En las Figuras 2.9, y 2.10 se muestran gráficamente las propiedades probadas en el Lema 2.13.

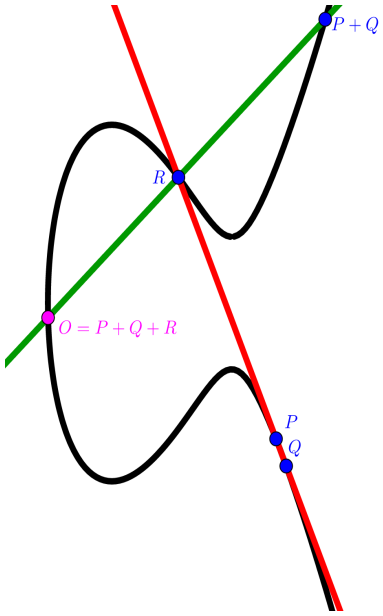

Figura 2.9. $P + Q + R = O$.

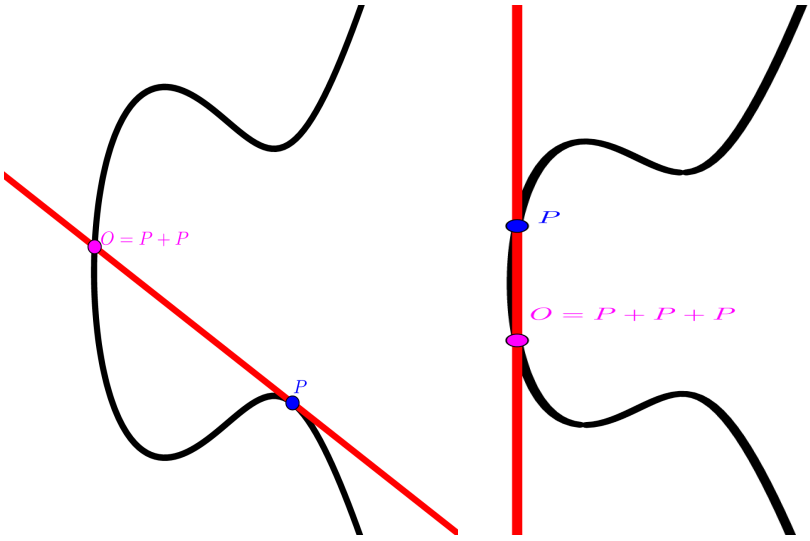

Figura 2.10. $P + P = O$ **y** $P + P + P = O$, **respectivamente.**

2.3. Subgrupo de los Racionales

En esta sección centraremos nuestra atención en los puntos racionales de una curva elíptica proyectiva y probaremos que este conjunto de puntos forma un subgrupo del grupo estudiado en la Sección 2.2. En la Sección 2.1 probamos que las curvas elípticas proyectivas sólo tenían un punto en el infinito, $(0:1:0)$, y que éstas se podían ver como los puntos de su vista afín para $z=1$ junto con el punto en el infinito. Por tanto, para estudiar sus puntos racionales basta con estudiar los puntos racionales de su vista afín $z=1$. Así, de ahora en adelante supondremos que una curva elíptica estará dada por los puntos $P=(x,y)\in\mathbb{C}^2$ que verifican la ecuación $\mathcal{C}\equiv y^2=x^3+ax^2+bx+c$ junto con el punto $(0:1:0)$; gracias a la identificación $(x,y)\sim(x:y:1)$ que vimos en la Subsección 1.2.1. Diremos que $P\in\mathbb{C}^2$ es un *punto racional* si $P=(x,y)\in\mathbb{Q}^2$. También diremos que la cúbica $\mathcal{C}$ es *racional* si $\mathcal{C}$ admite una ecuación en términos de coeficientes racionales. A los puntos racionales de $\mathcal{C}$ los denotaremos por $\mathbb{Q}(\mathcal{C})$ y demostraremos que $(\mathbb{Q}(\mathcal{C}),+)$ es un subgrupo de $(\mathcal{C},+)$.

Lema 2.14. *Sea $\mathcal{C}$ una curva elíptica racional y sean $P,Q\in\mathcal{C}$ dos puntos racionales. Entonces la recta $\mathcal{L}_{P,Q}$ es racional y los puntos de intersección de $\mathcal{L}_{P,Q}$ con $\mathcal{C}$ son puntos racionales.*

Demostración. Supongamos que $P\neq Q$. Para demostrar que $\mathcal{L}_{P,Q}$ es racional simplemente hallamos su ecuación. Sean $P=(p_1,p_2)$, $Q=(q_1,q_2)\in\mathbb{Q}^2\subset\mathbb{C}^2$ dos puntos racionales y consideramos el vector $\overrightarrow{PQ}=(q_1-p_1,q_2-p_2)$. Sabemos que la ecuación de la recta que determinan P y Q es

$$\mathcal{L}_{P,Q}\equiv(q_2-p_2)x+(p_1-q_1)y+(p_2q_1-p_1q_2)=0.$$

Dado que todos los coeficientes son elementos que pertenecen a $\mathbb{Q}$, se tiene que $\mathcal{L}_{P,Q}$ es una curva racional. Ahora tenemos que probar que el tercer punto de intersección de $\mathcal{L}_{P,Q}$ con $\mathcal{C}$ también es racional, sabiendo que P y Q lo son por hipótesis. Tanto la recta como la curva elíptica están determinadas por las expresiones

$$\begin{aligned}\mathcal{L}_{P,Q}&\equiv mx+ny+p=0.\\ \mathcal{C}\quad&\equiv x^3+ax^2+bx+c-y^2=0,\end{aligned}\tag{2.8}$$

donde $m,n,p,a,b,c\in\mathbb{Q}$. Supongamos sin pérdida de generalidad que $n\neq 0$, entonces $y=-\frac{mx+p}{n}$ y la sustituimos en (2.8):

$$x^3+ax^2+bx+c-\left(-\frac{mx+n}{p}\right)^2=0.$$

Desarrollamos el cuadrado:

$$x^3 + ax^2 + bx + c - \left(\frac{m^2x^2}{p^2} + \frac{2mnx}{p^2} + \frac{n^2}{p^2}\right) = 0.$$

Si agrupamos los términos como coeficientes de un polinomio en la variable x, se tiene que

$$x^3 + \left(a - \frac{m^2}{p^2}\right)x^2 + \left(b - \frac{2mn}{p^2}\right)x + \left(c - \frac{n^2}{p^2}\right) = 0.$$

Si llamamos $A = a - \frac{m^2}{p^2}$, $B = b - \frac{2mn}{p^2}$ y $C = b - \frac{n^2}{p^2}$, obtenemos la expresión

$$x^3 + Ax^2 + Bx + C = 0, \tag{2.9}$$

donde $A, B, C \in \mathbb{Q}$. Dado que (2.9) es un polinomio cúbico mónico, por el Teorema Fundamental del Álgebra se tiene que

$$x^3 + Ax^2 + Bx + C = (x - \alpha)(x - \beta)(x - \gamma), \tag{2.10}$$

con $\alpha, \beta, \gamma \in \mathbb{C}$. Como P y Q son dos puntos distintos de intersección de $\mathcal{L}_{P,Q}$ con $\mathcal{C}$, podemos suponer que $\alpha = p_1, \beta = q_1$ y $\gamma \neq p_1, q_1$, puesto que corresponde al tercer punto de intersección de $\mathcal{L}_{P,Q}$ con $\mathcal{C}$. Además, no puede ocurrir que $(B, C) = (0, 0)$. En efecto, $(B, C) = (0, 0)$ es equivalente (multiplicando e igualando coeficientes en (2.10)) a que $(p_1q_1 + p_1\gamma + q_1\gamma, -p_1q_1\gamma) = (0, 0)$. A su vez, es equivalente a que $(p_1, q_1) = (0, 0)$ o $(p_1, \gamma) = (0, 0)$ o $(q_1, \gamma) = (0, 0)$, lo cual no es posible debido a que p_1, q_1 y γ son todos distintos. A continuación, distinguimos dos casos:

1. Supongamos que $C \neq 0$, luego $(x - p_1)(x - q_1)(x - \gamma) = x^3 + Ax^2 + Bx + C$ es equivalente a $x^3 - (p_1 + q_1 + \gamma)x^2 + (p_1q_1 + p_1\gamma + q_1\gamma)x - p_1q_1\gamma = x^3 + Ax^2 + Bx + C$. De aquí se llega a que $-p_1q_1\gamma = C$, i.e, $\gamma = -\frac{C}{p_1q_1} \in \mathbb{Q}$.
2. Supongamos que $B \neq 0$. Análogamente, obtenemos la expresión $p_1q_1 + p_1\gamma + q_1\gamma = B$ que nos permite concluir que $\gamma = \frac{B - p_1q_1}{p_1 + q_1} \in \mathbb{Q}$.

Dado que $y = -\frac{mx+p}{n}$, si sustituimos el valor de γ, se tiene que $y \in \mathbb{Q}$. Por tanto, el tercer punto de intersección entre $\mathcal{L}_{P,Q}$ y $\mathcal{C}$ es un punto racional.
Supongamos que $P = Q$ es un punto de inflexión. Entonces, el único punto de intersección de $\mathcal{L}_{P,P}$ con $\mathcal{C}$ es P que es racional por hipótesis. Tenemos que demostrar que $\mathcal{L}_{P,P}$ es racional. Hallamos la derivadas parciales de $F(x, y) = x^3 + ax^2 + bx + c - y^2 \in \mathbb{Q}[x, y]$ en $P = (p_1, p_2) \in \mathbb{Q}^2$:

$$\begin{cases} F_x(p_1, p_2) = 3p_1^2 + 2ap_1 + b \in \mathbb{Q}, \\ F_y(p_1, p_2) = -2p_2 \in \mathbb{Q}. \end{cases}$$

Por tanto,

$$\mathcal{L}_{P,P} \equiv F_x(p_1, p_2)(x - p_1) + F_y(p_1, p_2)(y - p_2) = 0. \tag{2.11}$$

es racional.
Supongamos que $P = Q$ no es un punto de inflexión. La recta $\mathcal{L}_{P,P}$ es racional porque tiene la ecuación recogida en (2.11). Ahora debemos probar que el otro punto de intersección con $\mathcal{C}$ es racional ya que P es racional por hipótesis. Si despejamos y en (2.11), entonces

$$y = -\frac{F_x(p_1,p_2)(x-p_1)}{F_y(p_1,p_2)} + p_2 = \frac{(3p_1^2+2ap_1+b)(x-p_1)}{2p_2} + p_2. \tag{2.12}$$

Si sustituimos (2.12) en (2.8), obtenemos

$$x^3 + ax^2 + bx + c - \left(\frac{(3p_1^2+2ap_2+b)(x-p_1)}{2p_2} + p_2\right)^2 = 0.$$

Si se desarrolla el cuadrado:

$$x^3+ax^2+bx+c-\left(\frac{(3p_1^2+2ap_1+b)^2(x-p_1)^2}{4p_2^2} + (3p_1^2+2ap_1+b)(x-p_1) + p_2^2\right) = 0.$$

Agrupamos los términos en función de un polinomio en la variable x:

$$\begin{aligned} &x^3 + \left(a - \frac{(3p_1^2+2ap_1+b)^2}{4p_2^2}\right)x^2 + \\ &+ \left(b + \frac{(3p_1^2+2ap_1+b)^2p_1}{2p_2^2} - (3p_1^2+2ap_1+b)\right)x + \\ &+ \left(c - \frac{(3p_1^2+2ap_1+b)^2p_1^2}{4p_2^2} + (3p_1^2+2ap_1+b)p_2 - p_2^2\right) = 0. \end{aligned}$$

Si llamamos $A' = a - \frac{(3p_1^2+2ap_1+b)^2}{4p_2^2}$, $B' = b + \frac{(3p_1^2+2ap_1+b)^2p_1}{2p_2^2} - (3a^2+2ap_1+b)$ y $C' = c - \frac{(3p_2^2+2ap_1+b)^2p_1^2}{4p_2^2} + (3p_1^2+2ap_1+b)p_1 - p_2^2$, se tiene la ecuación

$$x^3 + A'x^2 + B'x + C' = 0, \tag{2.13}$$

donde $A', B', C' \in \mathbb{Q}$. Como (2.13) es una ecuación polinómica de grado 3, aplicando el Teorema Fundamental del Álgebra, obtenemos

$$x^3 + A'x^2 + B'x + C' = (x-\alpha)(x-\beta)(x-\gamma),$$

donde $\alpha, \beta, \gamma \in \mathbb{C}$. Como estamos en el supuesto de que P no es un punto de inflexión, tenemos que $I(P, \mathcal{C}, \mathcal{L}_{P,P}) = 2$. Luego, podemos suponer que $\alpha = \beta = p_1$ y $\gamma \neq p_1$. De aquí

$$x^3 + A'x^2 + B'x + C' = (x-p_2)^2(x-\gamma).$$

Si operamos en el segundo miembro, entonces

$$A'x^2 + B'x + C' = -(2p_1 + \gamma)x^2 + (p_1^2 + 2p_1\gamma)x - p_1^2\gamma.$$

Nótese que $(A', C') \neq (0, 0)$. En efecto, supongamos que $(A', C') = (0, 0)$, entonces $\gamma = 0$ o $p_1 = 0$ y $\gamma = -2p_1$, i.e, $\gamma = p_1 = 0$, lo cual es una contradicción porque estamos partiendo de que $p_1 \neq \gamma$. Estudiamos entonces los dos siguientes casos:

1. Si $C' \neq 0$, entonces $C' = -p_1\gamma$ y, equivalentemente, $\gamma = -\frac{C'}{p_1} \in \mathbb{Q}$.
2. Si $A' \neq 0$, se tiene que $A' = -(2p_1 + \gamma)$ y por tanto $\gamma = -(A' + 2p_1) \in \mathbb{Q}$.

En ambos casos, si sustituimos el valor de γ en (2.12), se llega a que $y \in \mathbb{Q}$.

□

Ya podemos enunciar y demostrar el siguiente teorema.

Teorema 2.15. *Sean $\mathcal{C}$ una curva elíptica racional y $O \in \mathcal{C}$ un punto racional, entonces el par $(\mathbb{Q}(\mathcal{C}), +)$ es un subgrupo de $(\mathcal{C}, +)$.*

Demostración. Utilizamos la caracterización de subgrupos. Por hipótesis $O \in \mathbb{Q}(\mathcal{C})$. Por el Lema 2.14, si $P, Q \in \mathbb{Q}(\mathcal{C})$, entonces tenemos $P+Q = (P*Q)*O \in \mathbb{Q}(\mathcal{C})$. Por último, si $P \in \mathbb{Q}(\mathcal{C})$, sabemos que $-P = (O * O) * P$ por el Teorema 2.10, y aplicando el Lema 2.14, se tiene que $-P \in \mathbb{Q}(\mathcal{C}')$.

□

Encontrar los puntos racionales de una curva elíptica presenta bastante complejidad. A continuación mostramos unos ejemplos en los que nos hemos ayudado de [5].

Ejemplo 2.16. Sea $\mathcal{C}$ la curva elíptica dada por $\mathcal{C} \equiv y^2 = x^3 - x^2 + x$. Por inspección, se observa que $Q = (0, 0) \in \mathbb{Q}(\mathcal{C})$. Además nótese que el punto $P = (1, 1) \in \mathbb{Q}(\mathcal{C})$ y por tanto $-P = (1, -1) \in \mathbb{Q}(\mathcal{C})$. La recta tangente a $\mathcal{C}$ en Q es $x = 0$, luego $Q * Q = O = (0 : 1 : 0)$. Dado que O es un punto de inflexión tenemos que $O * O = O$ y como consecuencia que $2Q = O$, i.e, Q tiene orden 2. Por otro lado, la recta tangente a $\mathcal{C}$ en P es $y = x$. Luego, si computamos $P + P$ llegamos a que $2P = Q$. De aquí se deduce que $4P = O$, esto es, el orden de P es 4. Análogamente se obtiene que el orden de $-P$ también es 4. Por tanto, si no existiesen más puntos racionales concluiríamos que $\mathbb{Q}(\mathcal{C}) \cong \mathbb{Z}_4$. En efecto, ver en [5].

Ejemplo 2.17. Sea $\mathcal{C}$ la curva elíptica dada por $\mathcal{C} \equiv y^2 = x^3 - x^2 - 24x - 36$. De nuevo por inspección, se observa que $P = (6, 0), Q = (-2, 0) \in \mathbb{Q}(\mathcal{C})$. Además, trazando la recta que pasa por P y Q se verifica que $R := P*Q = (-3, 0) \in \mathbb{Q}(\mathcal{C})$. Nótese que las rectas tangentes a $\mathcal{C}$ en P, Q y R son $x = 6, x = -2$ y $x = -3$, respectivamente. Por tanto, se tiene que $2P = 2Q = 2R = O$, esto es, P, Q y R tienen orden 2. Concluimos que $\mathbb{Q}(\mathcal{C}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Consultar [5].

Ejemplo 2.18. Sea $\mathcal{C}$ la curva elíptica dada por $\mathcal{C} \equiv y^2 = x^3 + \frac{1}{4}$. Obsérvese que $P = (0, \frac{1}{2}) \in \mathbb{Q}(\mathcal{C})$ y que la recta tangente a $\mathcal{C}$ en P es $y = \frac{1}{2}$. El único punto de intersección de $y = \frac{1}{2}$ con $\mathcal{C}$ es P, por tanto P es un punto de inflexión. Por la tercera propiedad del Lema 2.13, tenemos que P es de orden 3. Análogamente, se llega a que $-P = (0, -\frac{1}{2})$ también tiene orden 3. Concluimos que $\mathbb{Q}(\mathcal{C}) \cong \mathbb{Z}_3$. En [5] puede encontrarse esta curva en la forma $y^2 + y = x^3$.

Nótese que cuando una curva elíptica $\mathcal{C}$ carece de puntos racionales, entonces $\mathbb{Q}(\mathcal{C})$ es el trivial. Ver ejemplos en [5].

En las Figuras 2.11 y 2.12 se muestran gráficamente los Ejemplos 2.16, 2.17 y 2.18. Nótese que los grupos de los ejemplos anteriores son finitamente generados. Esto no se trata de un hecho casual, sino que es cierto en general y es donde centraremos nuestro foco de atención en el Capítulo 3.

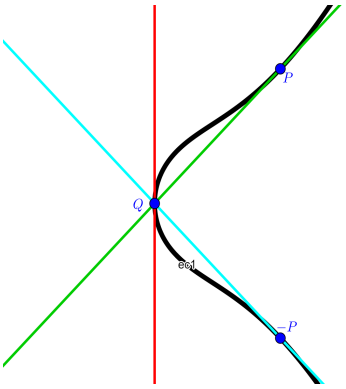

Figura 2.11. Ejemplo 2.16.

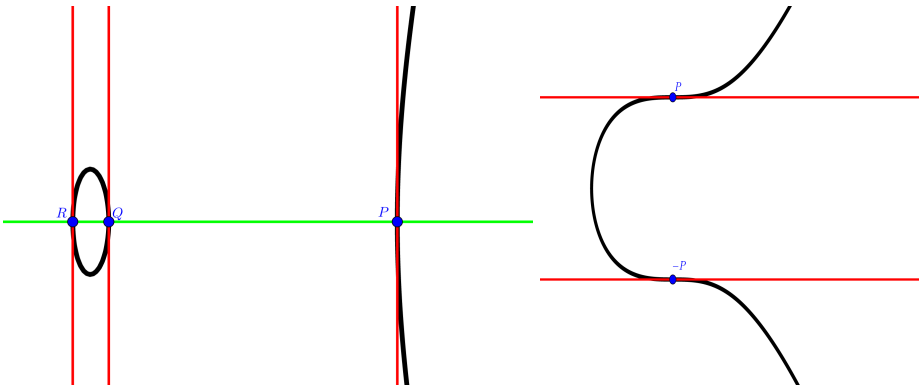

Figura 2.12. Ejemplos 2.17 y 2.18, respectivamente.

3

Teorema de Mordell

En lo que sigue demostraremos el *Teorema de Mordell* haciendo uso de [3] y [10], el cual afirma que el subgrupo formado por los puntos racionales de las curvas elípticas está finitamente generado. Para ello, necesitaremos enunciar y demostrar algunos resultados. De ahora en adelante, supondremos que $O = (0 : 1 : 0)$, es decir, que el punto base que consideraremos será el punto en el infinito de las curvas elípticas y además supondremos que es un punto racional puesto que lo es para la vista afín $y = 1$. Recordemos que $\mathcal{C}$ está dada por

$$\mathcal{C} \equiv y^2 = x^3 + ax^2 + bx + c. \tag{3.1}$$

Además, recordemos que para $O = (0 : 1 : 0)$, la operación $+$ consistía en una simetría respecto del eje X y por tanto, dado un punto $P = (x, y) \in \mathcal{C}$, entonces su opuesto es $-P = (x, -y)$.

Lema 3.1. *Sea $P \in \mathbb{Q}(\mathcal{C})$, con $P \neq O$. Entonces, las coordenadas de P son de la forma $(\frac{k}{j^2}, \frac{l}{j^3})$, donde $k, l, j \in \mathbb{Z}$ y $m.c.d(k, j) = m.c.d(l, j) = 1$.*

Demostración. Sea $P = (\frac{k}{n}, \frac{l}{t}) \in \mathbb{Q}(\mathcal{C})$, con $m.c.d(k, n) = m.c.d(l, t) = 1$. Si sustutimos P en (3.1), obtenemos que

$$\frac{l^2}{t^2} = \frac{k^3}{n^3} + a\frac{k^2}{n^2} + b\frac{k}{n} + c.$$

Multiplicamos en ambos miembros por t^2n^3:

$$l^2n^3 = k^3t^2 + ak^2nt^2 + bkn^2t^2 + cn^3t^2. \tag{3.2}$$

Si sacamos factor común t^2 en (3.2), obtenemos que t^2 divide a l^2n^3. Dado que $m.c.d(t, l) = 1$, entonces $m.c.d(t^2, l^2) = 1$. Por tanto, si aplicamos el Lema de Euclides, se cumple que t^2 divide a n^3. Si ahora despejamos k^3t^2 en (3.2) y sacamos factor común n en el segundo miembro, se llega a que n divide a k^3t^2. De nuevo, debido a que $m.c.d(n, k) = 1$, tenemos que $m.c.d(n, k^3) = 1$ y, aplicando el Lema de Euclides, se tiene que n debe dividir a t^2. Como n divide

a t^2, entonces existe $\lambda \in \mathbb{Z}$ tal que $t^2 = \lambda n$. Sustituimos en (3.2) ak^2nt^2 por $ak^2n^2\lambda$ y tenemos

$$l^2n^3 = k^3t^2 + ak^2n^2\lambda + bkn^2t^2 + cn^3t^2.$$

Si despejamos k^3t^2 y sacamos factor común n^2, se tiene que n^2 divide a k^3t^2. Como $m.c.d(n,k) = 1$, entonces $m.c.d(n^2,k^3) = 1$. Si aplicamos el Lema de Euclides, se llega a que n^2 divide a t^2. Tomamos la descomposición en factores primos de n y t, es decir, $n = n_1^{\alpha_1} \dots n_r^{\alpha_r}$ y $t = t_1^{\beta_1} \dots t_s^{\beta_s}$, donde $n_i, \alpha_i \in \mathbb{N}\backslash\{0\}$ para todo $i \in \{1,\dots,r\}$ y $t_j, \beta_j \in \mathbb{N}\backslash\{0\}$ para todo $j \in \{1,\dots,s\}$. Como n^2 divide a t^2 existe $\mu \in \mathbb{Z}$ tal que $t^2 = \mu n^2$, es decir, $n^2 = n_1^{2\alpha_1} \dots n_r^{2\alpha_r}$ y $t^2 = \mu n_1^{2\alpha_1} \dots n_r^{2\alpha_r}$. De aquí obtenemos que n_i divide a t^2 para todo $i \in \{1,\dots,r\}$. Como n_i es irreducible, se tiene que existe t_{j_i} ($j_i \in \{1,\dots,s\}$) de forma que n_i divide a t_{j_i}. Como t_{j_i} es también irreducible y $n_i, t_{j_i} \in \mathbb{N}$, necesariamente debe ocurrir que $n_i = t_{j_i}$ para ciertos $j_i \in \{1,\dots,s\}$ e $i \in \{1,\dots,r\}$. Tenemos que $n = n_1^{\alpha_1} \dots n_r^{\alpha_r} = t_1^{\alpha_1} \dots t_r^{\alpha_r}$ y $\alpha_i \leq \beta_i$, puesto que n^2 divide a t^2. Por tanto, $t_1^{\alpha_1} \dots t_r^{\alpha_r}$ divide a $t_1^{\beta_1} \dots t_s^{\beta_s}$, i.e, n divide a t. De esta forma concluimos que $\frac{t}{n} \in \mathbb{Z}$. Como n divide a t, existe $\gamma \in \mathbb{Z}$ de forma que $t = \gamma n$. Si sustuimos esto en (3.2) y despejamos k^3t^2 se tiene que

$$k^3t^2 = l^2n^3 - cn^3\gamma n^2 - ak^2n^3\gamma^2 - bkn^4\gamma.$$

Si sacamos factor común n^3, obtenemos que n^3 divide a k^3t^2. Como $m.c.d(n,k) = 1$, se tiene que $m.c.d(n^3,k^3) = 1$. Por el Lema de Euclides, concluimos que n^3 divide a t^2. Luego, tenemos que n^3 divide a t^2 y que t^2 divide a n^3 y ambos son no negativos, es decir, $n^3 = t^2$. Ahora tomamos $j := \frac{t}{n}$ y reescribimos las coordenadas de P:

$$\frac{k}{n} = \frac{kn^2}{n^3} = \frac{kn^2}{t^2} = \frac{k}{(\frac{t}{n})^2} = \frac{k}{j^2}$$
$$\frac{l}{t} = \frac{lt^2}{t^3} = \frac{ln^3}{t^3} = \frac{l}{(\frac{t}{n})^3} = \frac{l}{j^3}.$$

□

Lema 3.2. *Sea $\mathcal{C} \equiv y^2 = x^3 + ax^2 + bx + c$ y sean $P = (k,l), Q = (m,n) \in \mathbb{Q}(\mathcal{C})$ dos puntos distintos y supongamos que $P + Q \neq O$. Entonces, las coordenadas de $P + Q$ están dadas por $x = \lambda^2 - a - k - m$ e $y = -(\lambda x + p)$, donde $\lambda = \frac{n-l}{m-k}$ y $p = l - \lambda k$.*

Demostración. Sea $\mathcal{L}_{P,Q}$ la recta que pasa por P y Q. Entonces su pendiente está dada por $\lambda = \frac{n-l}{m-k}$. Supongamos que $\mathcal{L}_{P,Q} \equiv y = \lambda x + p$. Si sustituimos P en $\mathcal{L}_{P,Q}$, entonces $p = l - \lambda k$. Ahora intersecamos $\mathcal{L}_{P,Q}$ con $\mathcal{C}$:

$$(\lambda x + p)^2 = x^3 + ax^2 + bx + c.$$

Reordenando y agrupando, se llega a

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda p)x + (c - p^2) = 0. \tag{3.3}$$

La suma de las raíces de (3.3) debe ser $-(a-\lambda^2)$. Además, como $P, Q \in \mathbb{Q}(\mathcal{C})$, dos de estas raíces son k y m. Por tanto, $x+k+m = \lambda^2-a$, es decir, $x = \lambda^2-a-k-m$. La coordenada y de intersección es $y = \lambda x + p$. Como la operación $+$ es una simetría respecto al eje X, la coordenada y de $P + Q$ es $y = -(\lambda x + p)$.

□

Lema 3.3. *Sea $\mathcal{C} \equiv y^2 = x^3+ax^2+bx+c$ y sea $P = (k, l) \in \mathbb{Q}(\mathcal{C})$ y supongamos que $P + P \neq O$. Entonces las coordenadas de $P + P$ son $x = \lambda^2 - a - 2k$ e $y = -(\lambda x + p)$, donde $\lambda = \frac{f'(k)}{2l}$, $p = l - \lambda x$ y $f(x) = x^3 + ax^2 + bx + c$.*

Demostración. La demostración es análoga al Lema 3.2. Sólo resta probar el valor de λ. Sea $\mathcal{L}_{P,P}$ la recta tangente a $\mathcal{C}$ en P. La pendiente de $\mathcal{L}_{P,P}$ resulta de derivar en la ecuación de $\mathcal{C}$:

$$2y\frac{dy}{dx} = f'(x)$$

Si evaluamos en P, se obtiene que $\lambda = \frac{f'(k)}{2l}$.

□

En el siguiente corolario, extraído de [7], mostramos la versión algebraica de los apartados segundo y tercero del Lema 2.13.

Corolario 3.4. *Sea $\mathcal{C} \subset \mathbb{PC}^2$ una curva elíptica y denotemos por $\mathcal{C}(2)$ y $\mathcal{C}(3)$ a los puntos de orden 2 y orden 3 (incluyendo al neutro) de $\mathcal{C}$, respectivamente. Si $O = (0 : 1 : 0)$, entonces:*

1. $\mathcal{C}(2) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
2. $\mathcal{C}(3) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Demostración. Sea $P = (x, y) \in \mathcal{C}(2)$. Sabemos que $2P = O$ es quivalente a $P = -P$. Dado que para $O = (0 : 1 : 0)$ la operación $+$ es una simetría respecto del eje X, se verifica que $(x, y) = (x, -y)$, es decir, $P = (x, 0)$. Si sustituimos P en la ecuación de $\mathcal{C} \equiv y^2 = x^3 + ax^2 + bx + c$, se tiene que $x^3 + ax^2 + bx^2 + c = 0$. Por la Proposición 2.3 y por el Teorema Fundamental del Álgebra, se cumple que dicha ecuación tiene tres raíces $\alpha, \beta, \gamma \in \mathbb{C}$ distintas entre sí. Así, tenemos que $\mathcal{C}(2) = \{O, (\alpha, 0), (\beta, 0), (\gamma, 0)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
Sea $P = (x, y) \in \mathcal{C}(3)$, entonces $3P = O$ es equivalente a $2P = -P$. Esto quiere decir que $2P = (x, -y)$. Por el Lema 3.3, debe ocurrir que $x = \lambda^2 - a - 2x$.

Usando esta igualdad y teniendo en cuenta que $y^2 = x^3 + ax^2 + bx + c$, llegamos a la expresión $g(x) = 0$, donde $g(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2$. Probemos que $g(x)$ tiene cuatro raíces simples. En efecto, derivando se obtiene que $g'(x) = 12x^3 + 12ax^3 + 12bx + 12c = 12f(x)$. Dado que $f''(x) = 2(3x + a)$, podemos reescribir g como $g(x) = 2f(x)f''(x) - f'(x)^2$. Por tanto, g y g' no pueden tener raíces comunes porque de ser así f y f' también tendrían raíces en común, lo cual es una contradicción ya que las raíces de f son simples. Debido a que todas las raíces de g son simples, se tiene que la primera coordenada de P puede tomar cuatro valores distintos. De aquí, tenemos que la coordenada y puede tomar ocho valores distintos, ya que $y = \pm\sqrt{f(x)}$. Por tanto, existen ocho puntos de orden 3 junto con el neutro O. Concluimos que $\mathcal{C}(3) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

El Corolario 3.4 es cierto en general para puntos de orden m, esto es, $\mathcal{C}(m) \cong \mathbb{Z}_m \times \mathbb{Z}_m$. Puede encontrarse una prueba en la Proposición 5.4 de [9].

□

Definición 3.5. *Sea $P \in \mathbb{Q}(\mathcal{C})$. Definimos la altura de P, y lo denotaremos por $H(P)$, a la aplicación*

$$\begin{aligned} H\colon \quad \mathbb{Q}(\mathcal{C}) &\longrightarrow \mathbb{Z} \\ P = (\tfrac{m}{n}, y) &\longmapsto H(P) = max\{|m|, |n|\}, \end{aligned} \tag{3.4}$$

donde $m.c.d(m, n) = 1$. Además, si $P = O$, definimos su altura como $H(O) = 1$.

Lema 3.6. *Sea $M \in \mathbb{Z}^+$, entonces el conjunto $A = \{P \in \mathbb{Q}(\mathcal{C}) : H(P) \leq M\}$ tiene cardinal finito.*

Demostración. Sea $P \in A$. Tenemos $H(P) \leq M$, esto es, $max\{|m|, |n|\} \leq M$. De aquí, podemos afirmar que hay un número finito de números enteros que cumplen la desigualdad. Por consiguiente, el número de posibilidades para $\frac{m}{n}$ es finita, i.e, para la coordenada x de P. Debido a que P debe satisfacer (3.1), se tiene que para una coordenada x fija, hay al menos dos posibilidades para la coordenada de y. Por tanto, el número de posibilidades para las coordenadas de P son finitas, luego el conjunto A debe ser finito.

□

Definición 3.7. *Sea $P \in \mathbb{Q}(\mathcal{C})$. Definimos la altura logarítmica de P, y la denotaremos por $h(P)$, a la aplicación*

$$\begin{aligned} h\colon \quad \mathbb{Q}(\mathcal{C}) &\longrightarrow \mathbb{Z} \\ P = (\tfrac{m}{n}, y) &\longmapsto h(\tfrac{m}{n}, y) = \ln(H(P)), \end{aligned}$$

donde $m.c.d(m, n) = 1$. Si $P = O$, entonces $h(P) = 0$.

Corolario 3.8. *Sea $m \in \mathbb{Z}^+$. Entonces, el conjunto $B = \{P \in \mathbb{Q}(\mathcal{C}) : h(P) \leq m\}$ tiene cardinal finito.*

Demostración. La prueba es una consecuencia directa del Lema 3.6.

□

Lema 3.9. *Sea $P \in \mathbb{Q}(\mathcal{C})$. Entonces existe una constante $\mu \in \mathbb{R}^+$, que depende de P, de tal manera que $h(P+Q) \leq 2h(Q) + \mu$, para todo $Q \in \mathbb{Q}(\mathcal{C})$, siendo $\mathcal{C} \equiv y^2 = x^3 + ax^2 + bx + c$.*

Demostración. Sea $P = O$. Entonces, $h(P+Q) = h(Q) \leq 2h(Q)$. Luego, para este caso, se tiene que $\mu = 0$. Supongamos que $P = (x_0, y_0) \neq O$ y que $Q = (x, y) \notin \{O, P, -P\}$. Por el Lema 3.2, se verifica que la primera coordenada de $P + Q$ es $\lambda^2 - a - x - x_0$, donde $\lambda = \frac{y-y_0}{x-x_0}$, es decir,

$$\frac{(y-y_0)^2 - (x-x_0)(x+x_0+a)}{(x-x_0)^2} = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}, \tag{3.5}$$

para ciertos A, B, C, D, E, F y G racionales que dependen de a, b, c, x_0 e y_0. Además podemos suponer que A, B, C, D, E, F y G son enteros, puesto que si no lo fueran, multiplicaríamos numerador y denominador por el mínimo común múltiplo. Por el Lema 3.1, podemos reescribir $x = \frac{k}{j^2}$ e $y = \frac{l}{j^3}$ y eliminar sus denominadores en (3.5):

$$\frac{Alj + Bk^2 + Ckj^2 + Dj^4}{Ek^2 + Fkj^2 + Gj^4}. \tag{3.6}$$

De la Definición 3.5, tenemos que $k, j^2 \leq H(Q)$, es decir, $j \leq H(Q)^{\frac{1}{2}}$. Además, si sustituimos $x = \frac{k}{j^2}$ e $y = \frac{l}{j^3}$ en (3.1) y eliminamos los denominadores, se obtiene que $l^2 = k^3 + aj^2k^2 + bkj^4 + cj^6$. Dado que $k, j^2 \leq H(Q)$, se comprueba que $|l^2| \leq |H(Q)^3 + aH(Q)^3 + bH(Q)^3 + cH(Q)^3|$. Por tanto, sacando factor común $H(Q)$, tomando valor absoluto y aplicando la Desigualdad Triangular, se cumple que $|l^2| \leq |H(Q)^3|(1 + |a| + |b| + |c|)$. Equivalentemente, tenemos que $l \leq KH(Q)^{\frac{3}{2}}$, donde $K = \sqrt{1 + |a| + |b| + |c|}$. Si acotamos el numerador y el denominador en (3.6), llegamos a que $|Alj + Bk^2 + Ckj^2 + Dj^4| \leq |Alj| + |Bk^2| + |Ckj^2| + |Dj^4|$ y $|Ek^2 + Fkj^2 + Gj^4| \leq |Ek^2| + |Fkj^2| + |Gj^4|$. Si usamos que $k, j^2 \leq H(Q)$ y que $l \leq KH(Q)^{\frac{3}{2}}$, entonces $|Alj + Bk^2 + Ckj^2 + Dj^4| \leq |AKH(Q)^{\frac{3}{2}}H(Q)^{\frac{1}{2}}| + |BH(Q)^2| + |CH(Q)H(Q)| + |DH(Q)^2| = H(Q)^2(|AK| + |B| + |C| + |D|)$ y $|Ek^2 + Fkj^2 + Gj^4| \leq H(Q)^2(|E| + |F| + |G|)$. Por tanto, $H(P+Q) \leq H(Q)^2 max\{|A| + |B| + |C| + |D|, |E| + |F| + |G|\}$. Tomando logaritmo neperiano en ambos lados de la desigualdad, se alcanza la desigualdad deseada, donde $\mu' = ln(max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\})$. Para $Q = (x, y) \in \{O, P, -P\}$, sólo es necesario observar que $h(P+P) - 2h(P) \leq \mu_1$, $h(P+(-P)) - 2h(-P) \leq \mu_2$ y $h(P+O) - 2h(O) \leq \mu_3$ para ciertos $\mu_1, \mu_2, \mu_3 \in \mathbb{R}^+$. Luego, basta con tomar $\mu = max\{\mu_1, \mu_2, \mu_3, \mu'\}$.

□

Lema 3.10. *Sean $p(x), q(x) \in \mathbb{Z}[x]$ dos polinomios sin raíces en común. Supongamos que $d = max\{deg(p(x)), deg(q(x))\}$. Entonces, existe $z \in \mathbb{Z}$ que verifica que $m.c.d(n^d p(\frac{m}{n}), n^d q(\frac{m}{n}))$ divide a z para todo $\frac{m}{n} \in \mathbb{Q}$.*

El Lema 3.10 de la Teoría de Anillos se desvía del objetivo de esta memoria. Puede encontrarse una prueba en el Lema 3′ del Capítulo 3 de [10].

Lema 3.11. *Existe una constante μ tal que $h(2P) \geq 4h(P) - \mu$, para cada $P \in \mathbb{Q}(\mathcal{C})$, siendo $\mathcal{C} \equiv y^2 = x^3 + ax^2 + bx + c$.*

Demostración. Sea $P = (x, y)$, supongamos que $2P \neq O$ y denotemos por $f(x) = x^3 + ax^2 + bx + c$. El Lema 3.3 garantiza que la primera coordenada de $2P$ es $\lambda^2 - a - 2x$, donde $\lambda = \frac{f'(x)}{2y}$, es decir,

$$\frac{f'(x)^2 - 4f(x)(2x + a)}{4f(x)}. \tag{3.7}$$

Denotemos por $\psi(x)$ al numerador y por $\varphi(x)$ al denominador de (3.7), que son de grados 4 y 3, respectivamente. Podemos suponer que ψ y φ tienen coeficientes enteros, ya que si no fuera así, multiplicaríamos por el mínimo común múltiplo. Además, como estamos trabajando con curvas elípticas, sabemos que $f(x)$ y $f'(x)$ no tienen raíces en común, i.e, ψ y φ no comparten raíces. Por consiguiente, aplicamos el Lema 3.10. Sea $Z \in \mathbb{Z}$ tal que $m.c.d(n^4\psi(\frac{m}{n}), n^4\varphi(\frac{m}{n}))$ divide a Z para todo $\frac{m}{n} \in \mathbb{Q}$. Supongamos que $x = \frac{m}{n}$ y reescribamos (3.7) en la forma $\frac{n^4\psi(\frac{m}{n})}{n^4\varphi(\frac{m}{n})}$. Entonces,

$$H(2P) = max\left\{\left|n^4\psi\left(\frac{m}{n}\right)\right|, \left|n^4\varphi\left(\frac{m}{n}\right)\right|\right\} \geq \frac{1}{Z} max\left\{\left|n^4\psi\left(\frac{m}{n}\right)\right|, \left|n^4\varphi\left(\frac{m}{n}\right)\right|\right\}. \tag{3.8}$$

Aplicamos la desigualdad $max\{a, b\} \geq \frac{a+b}{2}$ en (3.8) y concluimos

$$H(2P) \geq \frac{1}{2Z}\left(\left|n^4\psi\left(\frac{m}{n}\right)\right| + \left|n^4\varphi\left(\frac{m}{n}\right)\right|\right). \tag{3.9}$$

Si dividimos (3.10) por $H(P)^4 = (max\{|m|, |n|\})^4 = max\{|m|^4, |n|^4\}$, se tiene

$$\frac{H(2P)}{H(P)^4} \geq \frac{1}{2Z}\frac{|n^4\psi(\frac{m}{n})| + |n^4\varphi(\frac{m}{n})|}{max\{|m|^4, |n|^4\}}. \tag{3.10}$$

Definimos la función $g(x) = \frac{|\psi(x)|+|\varphi(x)|}{max\{x^4,1\}}$. Obsérvese que g nunca se anula puesto que ψ y φ no tienen raíces comunes. Además, g es una función continua, esto es, alcanzará su mínimo en un intervalo cerrado, denotemos por W a este mínimo. Por tanto, en (3.10) se verifica

$$\frac{H(2P)}{H(P)^4} \geq \frac{W}{2Z}. \tag{3.11}$$

Despejando $H(2P)$ y tomando logaritmo neperiano en (3.11) se concluye que $h(2P) \geq 4h(p) - \mu_1$, donde $\mu_1 = -\ln \frac{W}{2Z}$. Supongamos que $2P = O$, entonces podemos tomar $4h(P) - h(2P) \leq \mu_2$, para cierto $\mu_2 \in \mathbb{R}^+$. Para concluir la prueba basta tomar $\mu = min\{\mu_1, \mu_2\}$.

□

En lo que sigue vamos a proporcionar una serie de resultados para probar un último lema que nos permitirá demostrar el Teorema de Mordell. De ahora en adelante supondremos que $T = (0,0) \in \mathcal{C}$ y que los coeficientes de la ecuación de la curva son enteros, esto es, que $c = 0$ y $a, b \in \mathbb{Z}$ en (3.1). Además, denotaremos por $\mathbb{Q}(\overline{\mathcal{C}})$ a la curva elíptica determinada por $y^2 = x^3 + \overline{a}x^2 + \overline{b}x$, donde $\overline{a} = -2a$ y $\overline{b} = a^2 - 4b$. Nótese que $\mathbb{Q}(\overline{\overline{\mathcal{C}}})$, que tiene por ecuación a $y^2 = x^3 + \overline{\overline{a}}x^2 + \overline{\overline{b}}x$, verifica que $y^2 = x^3 + 4ax^2 + 16bx$. Por abuso de notación hemos identificado $\mathcal{C}$ con su versión proyectiva. Si vemos $\mathcal{C}$ y $\overline{\mathcal{C}}$ como dos curvas proyectivas, podemos ir de una a otra con la trasformación proyectiva que tiene asociada la matriz

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & \frac{1}{4} \end{pmatrix}.$$

Por tanto, por la Proposición 2.12, se verifica que $\mathcal{C} \cong \overline{\overline{\mathcal{C}}}$ y, por consiguiente, que $\mathbb{Q}(\mathcal{C}) \cong \mathbb{Q}(\overline{\overline{\mathcal{C}}})$. Definimos ahora las siguientes aplicaciones:

$$\begin{aligned} \phi\colon\ & \mathbb{Q}(\mathcal{C}) \longrightarrow \mathbb{Q}(\overline{\mathcal{C}}) \\ & (x,y) \longmapsto \phi(x,y) = \begin{cases} \left(\frac{y^2}{x^2}, y\left(\frac{x^2-b}{x^2}\right)\right), & x \neq 0, \\ \overline{O}, & x = 0. \end{cases} \end{aligned} \tag{3.12}$$

$$\begin{aligned} \overline{\phi}\colon\ & \mathbb{Q}(\overline{\mathcal{C}}) \longrightarrow \mathbb{Q}(\overline{\overline{\mathcal{C}}}) \\ & (\overline{x},\overline{y}) \longmapsto \overline{\phi}(\overline{x},\overline{y}) = \begin{cases} \left(\frac{\overline{y}^2}{\overline{x}^2}, \overline{y}\left(\frac{\overline{x}^2-b}{\overline{x}^2}\right)\right), & \overline{x} \neq 0, \\ \overline{\overline{O}}, & \overline{x} = 0. \end{cases} \end{aligned} \tag{3.13}$$

Dado que $\mathbb{Q}(\mathcal{C}) \cong \mathbb{Q}(\overline{\overline{\mathcal{C}}})$, se tiene que existe $\varphi : \mathbb{Q}(\mathcal{C}) \longrightarrow \mathbb{Q}(\overline{\overline{\mathcal{C}}})$ isomorfismo. Entonces $\overline{\phi}$ puede ser interpretada como una aplicación $\psi : \mathbb{Q}(\overline{\mathcal{C}}) \longrightarrow \mathbb{Q}(\mathcal{C})$, donde

$$\psi = \varphi^{-1} \circ \overline{\phi}. \tag{3.14}$$

Proposición 3.12. *Las aplicaciones ϕ y ψ son homomorfismos de grupos cuyos núcleos son $\{O, T\}$ y $\{\overline{O}, \overline{T}\}$, respectivamente. Además, la composición $\psi \circ \phi$ es la aplicación que envía P a $2P$.*

Demostración. Basta probar que ϕ es un homomorfismo pues para ψ el procedimiento es análogo. Sean $P, Q \in \mathbb{Q}(\mathcal{C})$:
Caso 1. Supongamos $P = O$, entonces es inmediato comprobar que $\phi(P+Q) = \phi(P) + \phi(Q)$.
Caso 2. Supongamos $P = Q = T$, entonces $\phi(T+T) = \phi(T)+\phi(T)$ puesto que $T + T = O$. En efecto, si tomamos la recta tangente $\mathcal{L}_{T,T}$ $\mathcal{C}$ en T, se tiene que esta recta es paralela a $x = 0$, es decir, que los puntos de intersección entre $\mathcal{L}_{T,T}$ y $\mathcal{C}$ son T y O, luego $T + T = O$. Supongamos que $P = T$ y $Q = (x, y) \neq T$. Como $T+T = O$, entonces $T+Q \neq O$, luego si aplicamos el Lema 3.2 a $T+Q$, se comprueba que $T + Q = \left(\frac{b}{x}, -\frac{by}{x^2}\right)$. Calculamos $\phi(T + Q)$:

$$\phi(T+Q) = \left(\frac{\left(-\frac{by}{x^2}\right)^2}{\left(\frac{b}{x}\right)^2}, \frac{-\frac{by}{x^2}\left(\left(\frac{b}{x}\right)^2 - b\right)}{\left(\frac{b}{x}\right)^2}\right) = \left(\frac{y^2}{x^2}, y\left(\frac{x^2-b}{x^2}\right)\right) = \phi(Q).$$

Nótese que $\phi(T) = \overline{O}$ por definición de ϕ. Luego, para este caso $\phi(T + Q) = \phi(T) + \phi(Q)$.
Caso 3. Para este caso primero probaremos que $\phi(-Q) = -\phi(Q)$ para todo $Q = (x, y) \in \mathbb{Q}(\mathcal{C})$, $x \neq 0$. Para ello recordemos que el opuesto de un punto $Q = (x, y)$ viene dado por $-Q = (x, -y)$:

$$\phi(-Q) = \phi(x,-y) = \left(\frac{(-y)^2}{x^2}, -y\left(\frac{x^2-b}{x^2}\right)\right) = -\phi(x,y) = -\phi(Q). \quad (3.15)$$

Ahora, probaremos que dados $P, Q, R \in \mathbb{Q}(\mathcal{C})$ distintos entre sí y no iguales a O y T y tales que $P + Q + R = O$, entonces $\phi(P) + \phi(Q) + \phi(R) = \overline{O}$. En efecto, supongamos que $P + Q + R = O$. Por la primera propiedad del Lema 2.13, se cumple que P, Q y R son colineales. Tomamos $y = mx + n$ la recta que contiene a P, Q y R. Nótese que $n \neq 0$, ya que si $n = 0$, entonces $T = (0, 0)$ sería P, Q o R, lo cual es una contradicción porque estamos partiendo de que $P, Q, R \neq T$. Definimos la recta $y = \overline{m}x + \overline{n}$, donde $\overline{m} = \frac{nm-b}{n}$ y $\overline{n} = \frac{n^2-anm+bm^2}{n}$. Esta recta contiene a $\phi(P), \phi(Q)$ y $\phi(R)$. Para probarlo basta con sustituir cada punto en la ecuación $y = \overline{m}x + \overline{n}$. Por tanto, de nuevo por el Lema 2.13 se tiene que

$$\phi(P) + \phi(Q) + \phi(R) = \overline{O}. \quad (3.16)$$

De (3.15) y (3.16) tenemos que $\phi(P) + \phi(Q) = -\phi(R) = \phi(-R)$. Por otro lado, como $P + Q = -R$, entonces $\phi(P + Q) = \phi(-R)$. Por tanto, concluimos que $\phi(P + Q) = \phi(P + Q)$ y que ϕ es un homomorfismo de grupos.
Calculamos ahora el núcleo de ϕ; de la definición de ϕ se obtiene que sólo los puntos de la forma $(0, y)$ y O pertenecen a $ker(\phi)$. Como además los puntos $(0, y)$ deben cumplir la ecuación de $\mathcal{C}$, se tiene que $y^2 = 0^3 + a0^2 + b0$, i.e,

$y = 0$. Por tanto, $ker(\phi) = \{O, T\}$. Por el mismo razonamiento, se concluye que $\ker(\psi) = \{\overline{O}, \overline{T}\}$. Para probar que $\psi \circ \phi$ envía P a $2P$ sólo es necesario realizar la composición de ambas aplicaciones y operar.

□

Proposición 3.13. *Sea $\overline{P} = (\overline{x}, \overline{y}) \in \mathbb{Q}(\overline{\mathcal{C}})$, con $\overline{x} \neq 0$. Entonces, $\overline{P} \in Im(\phi)$ si, y sólo si, $\overline{x}$ es el cuadrado de un número racional.*

Demostración. Sean $\mathcal{C} \equiv y^2 = x^3 + ax^2 + bx$ y $\overline{\mathcal{C}} \equiv y^2 = x^3 + \overline{a}x^2 + \overline{b}x$. Supongamos que $\overline{P} \in Im(\phi)$. Entonces, por cómo está definida ϕ, se tiene que $\overline{x} = \frac{m^2}{n^2}$, para cierto $\frac{m}{n} \in \mathbb{Q}$. Luego, $\overline{x}$ es un cuadrado perfecto. Recíprocamente, supongamos que $\overline{x} = p^2$ para algún racional $p \in \mathbb{Q}$ y tengamos en cuenta que $\overline{P} = (\overline{x}, \overline{y})$ verifica

$$\overline{\mathcal{C}} \equiv y^2 = x^3 + \overline{a}x^2 + \overline{b}x \equiv y^2 = x^3 - 2ax^2 + (a^2 - b)x. \tag{3.17}$$

Afirmamos que $P := (\alpha, \alpha p) \in \mathbb{Q}(\mathcal{C})$, donde $\alpha = \frac{1}{2}(p^2 - a + \frac{\overline{y}}{p})$. En efecto, si $\alpha = 0$ no hay nada que probar. Supongamos que $\alpha \neq 0$ y tomemos $Q := (\beta, -\beta p)$, con $\beta = \frac{1}{2}(p^2 - a - \frac{\overline{y}}{p})$. Se comprueba que $\alpha\beta = b$ simplemente operando y haciendo uso de (3.17). Nótese que podemos escribir $p^2 = \alpha + a + \beta$ (se comprueba simplemente sustituyendo). Por tanto, mulplicando la expresión por α^2, se tiene que $(\alpha p)^2 = \alpha^3 + a\alpha^2 + \alpha^2\beta$. Dado que $\alpha\beta = b$, concluimos que $(\alpha p)^2 = \alpha^3 + a\alpha^2 + b\alpha$, i.e, $P \in \mathbb{Q}(\mathcal{C})$. Probemos que $\phi(P) = \overline{P}$. Debido a que $\overline{x} = p^2$, tenemos que es equivalente a $\frac{(\alpha p)^2}{\alpha^2} = \overline{x}$. Además, $\frac{\alpha p(\alpha^2 - \alpha\beta)}{\alpha^2} = p(\alpha - \beta)$. Si sustituimos los valores de α y β en esta expresión, se llega a $p(\alpha - \beta) = \overline{y}$, esto es, $\frac{\alpha p(\alpha^2 - b)}{\alpha^2} = \overline{y}$. Por tanto, por la definición de ϕ, concluimos que $\phi(P) = \overline{P}$.

□

Observación 3.14. Nótese que la Proposición 3.13 también es cierta para $Im(\psi)$. La prueba es análoga.

Definimos la siguiente aplicación:

$$\begin{aligned} \Gamma: \quad \mathbb{Q}(\mathcal{C}) &\longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*^2} \\ P = (x, y) &\longmapsto \Gamma(x, y) = \begin{cases} 1 \,(mod\, \mathbb{Q}^{*^2}) \,, & P = O, \\ b \,(mod\, \mathbb{Q}^{*^2}) \,, & P = T = (0, 0), \\ x \,(mod\, \mathbb{Q}^{*^2}) \,, & otro\, caso, \end{cases} \end{aligned}$$

donde $\mathcal{C} \equiv y^2 = x^3 + ax^2 + bx$.

Proposición 3.15. *La aplicación Γ es un homomorfismo de grupos.*

Demostración. En primer lugar, veamos que Γ envía los elementos opuestos a los inversos cuando $P = (x, y) \in \mathbb{Q}(\mathcal{C})$ distinto de T y O:

$$\Gamma(-P) = \Gamma(x, -y) = x \equiv x^{-1} = \Gamma(x, y)^{-1} = \Gamma(P)^{-1} (mod\, \mathbb{Q}^{*^2}).$$

Probemos que dados $P, Q, R \in \mathbb{Q}(\mathcal{C})$ tales que $P + Q + R = O$, entonces $\Gamma(P)\Gamma(Q)\Gamma(R) \equiv 1\ (mod\, \mathbb{Q}^{*^2})$. Sean $y = mx + n$ la recta que contiene a P, Q y R, con $m, n \in \mathbb{Q}$ por el Lema 2.14. Tomemos $P = (p_1, p_2), Q = (q_1, q_2)$ y $R = (r_1, r_2)$. Entonces se tiene que p_1, q_1 y r_1 verifican la ecuación $x^3 + (a - m^2)x^2 + (b - 2mn)x + n^2 = 0$ (ver el prodecimiento análogo realizado en el Lema 2.14). De aquí, obtenemos que $p_1 q_1 r_1 = n^2$, esto es, $\Gamma(P)\Gamma(Q)\Gamma(R) = p_1 q_1 r_1 = n^2 \equiv 1\, (mod\, \mathbb{Q}^{*^2})$. Por tanto, $\Gamma(P+Q) = \Gamma(-R) \equiv \Gamma(R)^{-1}\ (mod\, \mathbb{Q}^{*^2})$. Además, $\Gamma(R)^{-1} \equiv \Gamma(P)\Gamma(Q) (mod\, \mathbb{Q}^{*^2})$. Concluimos que $\Gamma(P + Q) = \Gamma(P)\Gamma(Q)$ y, por ende, que Γ es un homomorfismo.

□

Obsérvese que $Im(\psi) = Ker(\Gamma)$, donde ψ está dada por (3.14). En efecto, $Ker(\Gamma) = \{P \in \mathbb{Q}(\mathcal{C}) : \Gamma(P) = 1\} = \{P = (x, y) \in \mathbb{Q}(\mathcal{C}) : x = p^2, p \in \mathbb{Q}\}$. Por la Observación 3.14 y la Proposición 3.13, este conjunto es exactamente $Im(\psi)$.

Proposición 3.16. *La imagen de Γ está contenida en el subconjunto finito de $\mathbb{Q}^*/\mathbb{Q}^{*^2}$ que contiene a todos los divisores de b, con b el coeficiente del término x en la ecuación de $\mathcal{C}$.*

Demostración. Sea $P = O, T$, entonces $\Gamma(P) = 1, b$, respectivamente. De aquí, se tiene que las imágenes de O y T están en el conjunto de los divisores de b. Supongamos que $P = (x, y) \neq O, T$. Por el Lema 3.1, podemos escribir $P = (\frac{k}{j^2}, \frac{l}{j^3})$ y sustituirlo en (3.1) para obtener que $l^2 = k(k^2 + aj^2k + bj^4)$. Si k y $k^2 + aj^2k + bj^4$ son coprimos, se cumple que k y $k^2 + aj^2k + bj^4$ son el cuadrado de un racional y, por consiguiente, también lo sería $\frac{k}{j^2}$. Supongamos que $m.c.d(k, (k^2 + aj^2k + bj^4)) = d$, entonces d divide a k y a bj^4. Además, dado que k y j son coprimos, se tiene que d también divide a b. Por consiguiente, algunos factores primos de m se encontrarán entre los factores primos de b, esto es, si $b = p_1 \dots p_t$, entonces $m = \pm z^2 p_1^{\alpha_1} \dots p_t^{\alpha_t}$, donde $z \in \mathbb{Z}$ y $\alpha_i \in \{0, 1\}$ para cada $i \in \{1, \dots, t\}$. De aquí, tenemos que $\frac{m}{j^2} = \pm p_1^{\alpha_1} \dots p_t^{\alpha_t} (mod \mathbb{Q}^{*^2})$. Por tanto, $Im(\Gamma)$ está contenida en el subconjunto de $\mathbb{Q}^*/\mathbb{Q}^{*^2}$ que contiene a los divisores de b. Además, dicho conjunto es finito, porque b tiene finitos divisores, luego $Im(\Gamma)$ es finita.

□

Dado que $Im(\Gamma)$ es finita y $Ker(\Gamma) = Im(\psi)$, por el Primer Teorema de isomorfía, se tiene que $\mathbb{Q}(\mathcal{C})/Im(\psi) \cong Im(\Gamma)$ y por tanto $\mathbb{Q}(\mathcal{C})/Im(\psi)$ es finito. Análogamente, se llega a que $\mathbb{Q}(\overline{\mathcal{C}})/Im(\phi)$ es finito.

Lema 3.17. *El subgrupo* $2\mathbb{Q}(\mathcal{C}) = \{P + P \in \mathbb{Q}(\mathcal{C}) : P \in \mathbb{Q}(\mathcal{C})\}$ *tiene índice finito.*

Demostración. Dado que $\mathbb{Q}(\mathcal{C})/Im(\psi)$ y $\mathbb{Q}(\overline{\mathcal{C}})/Im(\phi)$ son finitos, existen subconjuntos de $\mathbb{Q}(\mathcal{C})$, $\{P_1, \ldots, P_n\}$ y $\{Q_1, \ldots, Q_m\}$, cuyos elementos son los representantes de las clases de $\mathbb{Q}(\mathcal{C})/Im(\psi)$ y $\mathbb{Q}(\overline{\mathcal{C}})/Im(\phi)$, respectivamente. Sea $P \in \mathbb{Q}(\mathcal{C})$, entonces debe existir un $i \in \{1, \ldots, n\}$ tal que $P - P_i \in Im(\psi)$, esto es, $P - P_i = \psi(\overline{P})$ para algún $\overline{P} \in \mathbb{Q}(\overline{\mathcal{C}})$ y, equivalentemente, $P = P_i + \psi(\overline{P})$. Análogamente, existe $j \in \{1, \ldots, m\}$ de forma que $\overline{P} - \overline{P}_j = \phi(Q)$ para cierto $Q \in \mathbb{Q}(\mathcal{C})$, i.e, $\overline{P} = \overline{P}_j + \phi(Q)$. Si aplicamos ψ a $\overline{P}$, se tiene que $\psi(\overline{P}) = \psi\left(\overline{P}_j + \phi(Q)\right)$. Dado que ψ es un homomorfismo de grupos por la Proposición 3.12, se verifica que $\psi(\overline{P}) = \psi(\overline{P}_j) + \psi(\phi(Q))$. Además, de nuevo por la Proposición 3.12 se tiene que $\psi(\phi(Q)) = 2Q$. Por tanto, sustituyendo la expresión de $\psi(\overline{P})$ en P llegamos a que $P = P_i + \psi(\overline{P}_j) + 2Q$. Como hemos escrito cualquier punto de $\mathbb{Q}(\mathcal{C})$ como suma de un elemento de $2\mathbb{Q}(\mathcal{C})$ y una combinación finita de los elementos representantes de las clases en $\mathbb{Q}(\mathcal{C})/Im(\psi)$ y $\mathbb{Q}(\overline{\mathcal{C}})/Im(\phi)$ concluimos que $2\mathbb{Q}(\mathcal{C})$ tiene índice finito.

□

Finalmente, reunimos todos los resultados necesarios para probar el Teorema de Mordell.

Teorema 3.18. *Sea* $\mathcal{C}$ *una curva elíptica. Entonces el subgrupo* $\mathbb{Q}(\mathcal{C})$ *de* $\mathcal{C}$ *está finitamente generado.*

Demostración. Sea $P \in \mathbb{Q}(\mathcal{C})$. Por el Lema 3.17, podemos tomar $Q_1, \ldots, Q_n \in \mathbb{Q}(\mathcal{C})$ los representantes de las clases de $\mathbb{Q}(\mathcal{C})/2\mathbb{Q}(\mathcal{C})$. Luego, existe $i_0 \in \{1, \ldots, n\}$ tal que $P - Q_{i_1} = 2P_1$, para cierto $P_1 \in \mathbb{Q}(\mathcal{C})$. Análogamente, existe $i_1 \in \{1, \ldots, n\}$ de manera que $P_1 - Q_{i_2} = 2P_2$, para algún $P_2 \in \mathbb{Q}(\mathcal{C})$. En general, podemos encontrar $i_j \in \{1, \ldots, n\}$ de forma que $P_{j-1} - Q_{i_j} = 2P_j$, donde $P_j \in \mathbb{Q}(\mathcal{C})$. De esta manera, podemos escribir P como

$$P = Q_{i_1} + 2Q_{i_1} + 2^2 Q_{i_2} + \ldots + 2^{n-1} Q_n + 2^n P_n. \tag{3.18}$$

Por el Lema 3.9, existen $k_i \in \mathbb{R}^+$ de manera que $h(Q_i - Q) \leq h(2Q) + k_i$, para cada $Q \in \mathbb{Q}(\mathcal{C})$, con $i \in \{1, \ldots, n\}$. Definimos $k = \underset{i \in \{1,\ldots,n\}}{\text{máx}} \{k_i\}$, esto es, $h(Q_i - Q) \leq h(2Q) + k$, para todo $Q \in \mathbb{Q}(\mathcal{C})$. Además, por el Lema 3.11, se tiene que existe $l \in \mathbb{R}^2$ que verifica que $h(2Q) \geq 4h(Q) - l$, para cada $Q \in \mathbb{Q}(\mathcal{C})$. Dado que $P_{j-1} - Q_{i_j} = 2P_j$, entonces $h(P_{j-1} - Q_i) = h(2P_j)$ y, por consiguiente, $h(2P_j) \leq 2h(P_{j-1}) + k$ y $4h(P_j) - l \leq 2h(P_{j-1}) + k$. De aquí, se sigue que

$$h(P_j) \leq \frac{1}{2} h(P_{j-1}) + \frac{k+l}{4},$$

y, equivalentemente,

$$h(P_j) \leq \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (k+l)).$$

Si $h(P_{j-1}) \geq k+l$, entonces $h(P_j) \leq \frac{3}{4}h(P_{j-1})$. Esta secuencia se va aproximando a cero, es decir, que llegará un punto en el que se verifique que $h(P_n) \leq k+l$. De aquí, tenemos

$$P_n \in \{R \in \mathbb{Q}(\mathcal{C}) : R \leq k+l\}, \tag{3.19}$$

donde (3.19) es un conjunto finito por el Corolario 3.8. Por tanto, de (3.18) y de (3.19) se concluye que P es combinación de elementos del conjunto

$$\{Q_1, \ldots, Q_n\} \cup \{R \in \mathbb{Q}(\mathcal{C}) : R \leq k+l\},$$

y, por ende, el subgrupo de los puntos racionales de una curva elíptica está finitamente generado.

□

Conclusiones

En el Capítulo 1 hablamos sobre curvas algebraicas afines y proyectivas sobre cuerpos en general. Un estudio complementario a esta memoria podría ser investigar qué ocurre con las curvas elípticas sobre cuerpos finitos, ya que estas tienen diversas aplicaciones como las que mencionamos en la Introducción y estudiar la generalización que existe para el Teorema de Mordell sobre estos conjuntos.

Al final del Capítulo 2 dimos algunos ejemplos ayudándonos de [5] para hallar el grupo de los puntos racionales de las curvas elípticas que allí se mencionaron. Sin embargo, aun sabiendo que el grupo de los puntos racionales está finitamente generado, sigue existiendo mucha complejidad a la hora de encontrarlo debido a la dificultad latente en los puntos racionales de las curvas elípticas y es por eso que este documento motiva el estudio para dar con una caracterización de los mismos puesto que sigue siendo un problema abierto encontrar los puntos racionales de las curvas elípticas en un número finito de pasos. Cabe destacar que estas investigaciones desembocan en uno de los problemas del milenio; la *Conjetura de Birch y Swinnerton-Dyer* (para más información ver [6]).

Con el estudio de esta memoria podría quedar abierta otra cuestión; con la operación $+$ del Capítulo 2 los puntos de las curvas elípticas tienen estructura de grupo abeliano. Dado este hecho, ¿se podría encontrar otra operación interna $\times$ de forma que $(\mathcal{C}, +, \times)$ tenga estructura de anillo?

Bibliografía

[1] AGUILAR ALARCÓN, Jhon Jane. y ROMERO VALENCIA, Jesús. *Estructura de grupo en una curva elíptica,* Miscelánea Matemática 63 (2016) 77-92.

[2] GIBSON, C.G. *Elementary Geometry of Algebraic Curves,* Cambridge University Press, 1998

[3] GONDI, Suhan V. *An Elementary Proof of Mordell's Theorem,* Chicago University, 2018. Accesible en http://math.uchicago.edu/~may/REU2018/REUPapers/Gondi.pdf

[4] HILMAR, Jan. y SMYTH, Chris. *Euclid Meets Bézout: Intersecting Algebraic Plane Curves with the Euclidean Algorithm,* The American Mathematical Monthly , Vol. 117, No. 3 (March 2010), pp. 250-260.

[5] LMFDB. Accesible en https://www.lmfdb.org/EllipticCurve/Q/

[6] MATES MIKE. *El Problema del Milenio que relaciona 5 Ramas de las Matemáticas Diferentes*. Accesible en https://youtu.be/9mR_h9ufs4E.

[7] NAVAS OROZCO, Jesús. *Curvas Elípticas y el Teorema de Mordell* Universidad de Sevilla.

[8] ROBIN, H. *Algebraic Geometry*, Graduate Texts in Mathematics, Springer Science & Business Media, 1977.

[9] SILVERMAN, Joseph H. *The Arithmetic of Elliptic Curves,* 2nd edition, Springer Science+Business Media, LLC 2009, 1986.

[10] SILVERMAN, Joseph H. y TATE, John. *Rational Points on Elliptic Curves,* 2nd edition, Springer-Verlag New York, INC, 1992.

Groups in Elliptic Curves

William Giovanni Hernández Yanes
Facultad de Ciencias • Sección de Matemáticas
Universidad de La Laguna
alu0101106113@ull.edu.es

Abstract

The roots of a polynomial in two variables are represented geometrically in the real plane as algebraic curves. In this way, we are able to study the different geometric properties they verify. In particular, we are specially interested in studying the points on elliptic curves, above all, the rational ones.

1. Elliptic Curves

Definition. A projective elliptic curve $\mathscr{C} \subset \mathbb{PC}^2$ is a non-singular cubic.

Proposition. Any elliptic curve $\mathscr{C} \subset \mathbb{PC}^2$ admits an equation of the form $y^2z = x^3 + bx^2z + bxz^2 + cz$, which is called the Weierstrass form.

We define a binary operation $*$ in $\mathscr{C}$ by taking two points P,Q on the curve $\mathscr{C}$ and intersecting the line they determine with $\mathscr{C}$.

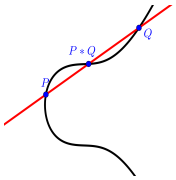

Figure 1: ***Operation*** $*$**.**

Lemma. Let $\mathscr{C}$ be a projective elliptic curve in $\mathbb{PC}^2$. Let $P,Q,R,S \in \mathscr{C}$, then the operation $*$ verifies:

1. $P * Q = Q * P$.
2. $(P * Q) * P = Q$.
3. $((P * Q) * R) * S = P * ((Q * S) * R)$.

2. Groups in Elliptic Curves

By fixing a point O on $\mathscr{C}$, we define another binary operation $+$ in $\mathscr{C}$: if $P,Q \in \mathbb{PC}^2$, then $P + Q = (P * Q) * O$:

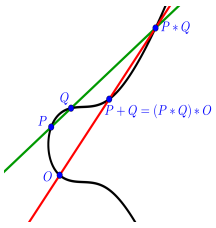

Figure 2: ***Operation*** $+$**.**

Theorem. Let $\mathscr{C} \subset \mathbb{PC}^2$. The tuple $(\mathscr{C},+)$ forms a group.

Proposition. Let $\mathscr{C} \subset \mathbb{PC}^2$ an elliptic curve and let $O,O' \in \mathscr{C}$. Then the groups $(\mathscr{C},+)$ and $(\mathscr{C},+')$ associated with O and O', respectivaly, are isomorphic.

Lemma. Let $\mathscr{C} \subset \mathbb{PC}^2$ an elliptic curve and let $P,Q,R,O \in \mathscr{C}$, where O is a flex point. Then:

1. If P,Q y R are all different, then $P+Q+R=O$ if, and only if, P,Q y R are collineal.
2. $P \neq O$ has order 2 if, and only if, O lies on the tangent line to $\mathscr{C}$ at P.
3. $P \neq O$ has order 3 if, and only if, P is a flex.

By identifying a proyective elliptic curve with an affine elliptic curve, we can study their rational points $\mathbb{Q}(\mathscr{C})$.

Theorem. Let $\mathscr{C}$ be an elliptic curve. Then the tuple $(\mathbb{Q}(\mathscr{C}),+)$ is a subgroup of $(\mathscr{C},+)$.

3. Mordell Theorem

By taking $O = (0:1:0)$, the operation $+$ has this form:

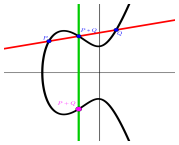

Figure 3: ***Operation*** $+$ ***with*** $O = (0:1:0)$**.**

Lemma. Let $P \in \mathbb{Q}(\mathscr{C})$, with $P \neq O$. Then, $P(\frac{k}{j^2}, \frac{l}{j^3})$, for some $k,l,j \in \mathbb{Z}$ and $g.c.d(k,j) = m.c.d(l,j) = 1$.

Lemma. Let $\mathscr{C} \equiv y^2 = x^3 + ax^2 + bx + c$ and $P = (k,l), Q = (m,n) \in \mathbb{Q}(\mathscr{C})$ two different points of $\mathscr{C}$ and assume $P + Q \neq O$. Then, $P+Q = (x,y)$ where $x = \lambda^2 - a - k - m$ and $y = -(\lambda x + p)$, with $\lambda = \frac{n-l}{m-k}$ and $p = l - \lambda k$.

Mordell Theorem. Let $\mathscr{C}$ be an elliptic curve. Then the subgroup $\mathbb{Q}(\mathscr{C})$ of $\mathscr{C}$ is finitely generated.

Example. Let $\mathscr{C}$ a projective elliptic curve determined by $\mathscr{C} \equiv y^2 = x^3 - x^2 + x$, then $\mathbb{Q}(\mathscr{C}) \cong \mathbb{Z}_4$.

References

[1] GIBSON, C.G. *Elementary Geometry of Algebraic Curves,* Cambridge University Press, 1998

[2] GONDI, Suhan V. *An Elementary Proof of Mordell's Theorem,* Chicago University, 2018. Accesible en http://math.uchicago.edu/ may/REU2018/REUPapers/Gondi.pdf

[3] SILVERMAN, Joseph H. y TATE, John. *Rational Points on Elliptic Curves,* 2nd edition, Springer-Verlag New York, INC, 1992.