PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Escuela de Posgrado

Isomorfismo de curvas elípticas mediante el invariante j

Tesis para obtener el grado académico de Magíster en Matemáticas que presenta:

Richard Andres Villajuan Guzman

Asesor:
Dr. Alfredo Bernardo Poirier Schmitz

Lima, 2022

Isomorfismo de curvas elípticas mediante el invariante j

Richard Andres Villajuan Guzman

Tesis presentada a consideración del Cuerpo Docente de la Escuela de Posgrado, de la PUCP, como parte de los requisitos para obtener el grado académico de Magister en Matemáticas.

Miembros del jurado:

Dr. Jaime Cuadros Valle, PUCP
https://orcid.org/0000-0000-0000-0000
(Presidente del jurado)

Dr. Alfredo Bernardo Poirier Schmitz, PUCP
https://orcid.org/0000-0003-2789-3630
(Asesor)

Dr. Richard Gonzáles Vilcarromero, PUCP
https://orcid.org/0000-0000-0000-0000
(Tercer miembro)

Lima - Perú
Marzo - 2022

Resumen

Comenzamos con un breve recordatorio sobre algunas nociones de conjuntos algebraicos, morfismos racionales y regulares. Por otro lado, veremos que la forma de Weierstrass de una cúbica tiene asociado dos elementos importantes. El primero es el discriminante τ que nos permite decidir si una cúbica es singular o no. El segundo elemento, muy importante en este trabajo, es el invariante j, cuyo nombre se debe a que éste no varía a pesar de los cambios de coordenadas que se realicen en la curva. Éste elemento cobra gran importancia pues nos ayuda a reconocer cuándo dos curvas elípticas son isomorfas. Y además, también nos permite contar el número de automorfismos sobre una curva elíptica dada.

Palabras clave: *curva elíptica, invariante j, morfismo algebraico.*

Abstract

We start with a brief reminder on some notions of algebraic sets, rational and regular maps. On the other hand, we will see that the Weierstrass form of a cubic has two important elements associated to it. The first is the discriminant τ that allows us to decide whether a cubic is singular or not. The second element, very important in this work, is the j invariant, whose name is due to the fact that it does not vary despite the changes in coordinates that are made in the curve. This element is crutial because it helps us to recognize when two elliptic curves are isomorphic. And in addition, it also allows us to count the number of automorphisms on a given elliptic curve.

Keywords: elliptic curve, the j invariant, algebraic maps.

... A mi familia. Por la confianza que depositan en mí y por su apoyo sobre todo en los momentos más difíciles.

Contenido

Lista de figuras

Agradecimientos

Agradezco a mi padres por darme una educación muy buena que me ha permitido crecer mucho profesionalmente. A mis hijas por haber dado alegrías a mi vida, y sobre todo a mi hija Camille por haberme dado mucha fuerza.

A todos mis profesores de los cuales tengo gratos recuerdos, en especial al Dr. Alfredo Poirier por su infinita paciencia y su constante apoyo.

Y además a mis amigos más cercanos, los cuales siempre me apoyaron en todo.

Introducción

En el presente trabajo veremos cómo a cada curva elíptica se le puede asociar una ecuación de Weierstrass. Dada esa presentación, asignaremos a sus coeficientes un par de números que serán de vital importancia.

El primero es el discriminante, el mismo que distingue si una cúbica en forma de Weierstrass es singular o no. El otro valor es más importante aún, pues nos permite determinar si dos curvas elípticas son isomorfas sobre la clausura algebraica del cuerpo donde están definidos los coeficientes. Este valor es el llamado invariante j. Recibe el apelativo de invariante pues para cada par de curvas isomorfas este valor j no cambia.

Si bien el invariante j nos permite concluir si dos curvas elípticas son isomorfas sobre un cuerpo algebraicamente cerrado, no nos especifica si lo son sobre el cuerpo original. Para decidir lo último introduciremos el concepto de *twist*. Gracias al invariante j también podremos determinar la pertinencia o no de estudiar familias específicas.

Richard Andres Villajuan Guzman
Lima, Perú.
2022

Capítulo 1

Equivalencia birracional de ciertas cúbicas

Iniciaremos nuestra presentación con algunas definiciones de la geometría algebraica. Para el desarrollo de este capítulo se puede consultar [4], [5], [6], [10], [15].

Recordemos algunos nociones de la geometría algebraica. Un subconjunto X sobre el espacio afín $A^n_{\mathbb{K}}$ (o sobre el proyectivo $\mathbb{P}^n_{\mathbb{K}}$) es **algebraico** si existe $S \subseteq \mathbb{K}[x_1, \cdots, x_n]$ familia de polinomios (o $S \subseteq \mathbb{K}[x_1, \cdots, x_{n+1}]$ familia de polinomios homogéneos), tal que $X = V(S)$, donde $V(S)$ es el conjunto de ceros comunes de los polinomios de la familia S.

Ejemplo 1.1. Sean los polinomios $f,\ g \in \mathbb{K}[x, y]$, dados por $f(x, y) = y - x^3$ y $g(x, y) = y - x^5$. Con ellos el conjunto $X = V(f, g) = \{(0, 0),\ (1, 1),\ (-1, -1)\}$ es algebraico sobre el espacio afín $A^2_{\mathbb{K}}$.

Ejemplo 1.2. Sobre el espacio proyectivo $P^2_{\mathbb{K}}$, el conjunto formado por un solo punto $a = (a_0 : a_1 : a_2)$ es algebraico, pues $\{a\} = V(\{a_i x_j - a_j x_i : 0 \leq i < j \leq 2\})$.

Dados los polinomios $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, ellos determinan una aplicación polinomial $\phi : \mathbb{A}^n_{\mathbb{K}} \to \mathbb{A}^m_{\mathbb{K}}$, vía evaluación. En efecto, si $x \in \mathbb{A}^n_{\mathbb{K}}$, entonces las coordenadas de $\phi(x)$ son $f_1(x), \ldots, f_m(x)$. Sean $X \subset \mathbb{A}^n_{\mathbb{K}}$ y $Y \subset \mathbb{A}^m_{\mathbb{K}}$ conjuntos algebraicos afines (o variedades afines). Una función $\phi : X \to Y$ es **regular** si es la restricción a X de una función polinomial $\mathbb{A}^n_{\mathbb{K}} \to \mathbb{A}^m_{\mathbb{K}}$. En particular, notemos que dos polinomios $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ determinan la misma funcón regular $X \to \mathbb{K}$ si y sólo si la diferencia $f - g$ se anula en todo punto de X.

Sea $X \subset \mathbb{A}^n_{\mathbb{K}}$ un conjunto algebraico. Una función racional en X es el cociente de dos funciones regulares.

Sean $X \subset \mathbb{P}^n$ y $Y \subset \mathbb{P}^m$ variedades proyectivas. Una función $\phi : X \to Y$ se denomina **racional** si se puede escribir como

$$\phi(x_0 : \cdots : x_n) = [F_0(x_0, \ldots, x_n) : \cdots : F_m(x_0, \ldots, x_n)]$$

para ciertos polinomios homogéneos $F_0, \ldots, F_m \in \mathbb{K}[x_0, \ldots, x_n]$ del mismo grado, donde al menos uno de ellos no se anula completamente en X.

Decimos que ϕ es regular en el punto $p \in X$ si se puede representar por polinomios homogéneos $F_0, \ldots, F_m$ que no se anulan simultáneamente en p.

En principio, una función racional está definida sobre el abierto $X \backslash V(F_0, \ldots, F_m)$, pero su dominio de definición (como función regular) puede ser más grande.

Si ϕ es regular en todo punto de X, entonces decimos que ϕ es un morfismo regular.

Nota para el lector. Para una discusión clara y detallada ver el libro [12].

Ejemplo 1.3. Sea el conjunto algebraico $X = V(x^2+y^2-1)$. La función $f : X \to \mathbb{R}$, dada por $f(x, y) = \dfrac{y}{x}$, es una función racional sobre el conjunto X.

Ejemplo 1.4. Sea C la curva en $\mathbb{P}^2$ dada por $xz = y^2$ y considere la función racional $C \to \mathbb{P}^1$ definida por $[x : y : z] \to [x : y]$. Esta función es regular pues $[0 : 0 : 1]$ no pertenece a C. Notemos que $[x : y]$ e $[y : z]$ definen la misma función racional en C.

Vamos a tratar en términos generales de la equivalencia de ciertas curvas cúbicas, es decir, de la interrelación de los lugares geométricos de ceros de diversos polinomios cúbicos en dos variables (realmente en tres, pues en ciertos casos es preferible trabajar con polinomios homogéneos en el espacio proyectivo).

Acá es importante plantearnos la siguiente pregunta: si los polinomios a tratar están definidos sobre un cuerpo $\mathbb{K}$, la equivalencia a considerar deberá estar definida sobre este cuerpo, o es lícito trabajar en una clausura algebraica?

La pregunta anterior nos conduce casi de inmediato a parte del tema a tratar en esta tesis. Supongamos que tenemos una relación polinomial —cúbica, digamos— definida sobre un cuerpo $\mathbb{K}$, que no es algebraicamente cerrado. Supongamos también que por un motivo u otro conocemos uno o más puntos "racionales" sobre esta curva. Nuestro interés se centra en saber cómo conseguir, en base a este conocimiento, puntos adicionales con coordenadas en el cuerpo base $\mathbb{K}$.

Ejemplo 1.5. Sobre el espacio proyectivo $\mathbb{P}^2_{\mathbb{Q}}$ consideremos las curvas

$$C_1 : xy^2 - x^2z + 2xyz - 4xz^2 + 3yz^2 = 0,$$

y

$$C_2 : v^2w + 2uvw + 3vw^2 = u^3 + 4u^2w.$$

Si a la ecuación de la curva C_1 la multiplicamos por xz^2 y hacemos el cambio de variable $u = xz$, $v = xy$, $w = z^2$, se consigue $(u : v : w) \in C_2$. Es decir tenemos el morfismo $\alpha : C_1 \to C_2$, definido por $\alpha(x : y : z) = (xz : xy : z^2)$. Cuando aplicamos α debemos de tener cuidado en el caso que xz, xy, z^2 se anulen simultáneamente, pues allí vamos a tener que trabajar con los puntos $(x : 0 : 0) = (1 : 0 : 0)$ y $(0 : y : 0) = (0 : 1 : 0)$. Aquí el problema es que $\alpha(1 : 0 : 0) = \alpha(0 : 1 : 0) = (0 : 0 : 0)$ no pertenece al espacio proyectivo, y en este caso para hallar la imagen de $(1 : 0 : 0)$ y $(0 : 1 : 0)$ es necesario tomar otro representante racional de α. Para obtener la imagen de $(0 : 1 : 0)$, debemos de tener en cuenta que estamos trabajando con morfismos racionales en variedades proyectivas, y por ello es posible reemplazar la definición dada de α por otra equivalente, a saber:

$$[xz : xy : z^2] = [xyz : xy^2 : yz^2].$$

Asimismo, usando el hecho de que para puntos $(x : y : z) \in C_1$ se cumple $3yz^2 = x^2z - 2xyz + 4xz^2 - xy^2$, obtenemos

$$[xz : xy : z^2] = [xyz : xy^2 : yz^2] = \left[xyz : xy^2 : \frac{-xy^2 + x^2z - 2xyz + 4xz^2}{3}\right].$$

Ahora factorizamos x y obtenemos

$$[xz : xy : z^2] = \left[yz : y^2 : \frac{-y^2 + xz - 2yz + 4z^2}{3}\right]$$

como funciones racionales en C_1. Evaluando el lado derecho de la última igualdad en $[0 : 1 : 0]$ obtenemos

$$\alpha(0 : 1 : 0) = \left(0 : 1 : -\frac{1}{3}\right) = (0 : 3 : -1).$$

Con ello se obtuvo finalmente la imagen de $(0 : 1 : 0)$ mediante α.

Ahora para hallar la imagen de $(1 : 0 : 0)$ seguiremos un argumento similar. En coordenadas homogéneas se tiene

$$[xz : xy : z^2] = [xyz : xy^2 : yz^2].$$

Dado que para puntos $(x : y : z) \in C_1$ se tiene la identidad $xy^2 = x^2z - 2xy + 4xz^2 - 3yz^2$, el lado derecho es equivalente a

$$[xz : xy : z^2] = [xyz : xy^2 : yz^2] = [xyz : x^2z - 2xyz + 4xz^2 - 3yz^2 : yz^2].$$

Podemos ahora factorizar z y obtenemos finalmente

$$[xz : xy : z^2] = [xy : x^2 - 2xy + 4xz - 3yz : yz],$$

como funciones racionales en C_1. Evaluando el lado derecho de la última igualdad en el punto $[1 : 0 : 0]$ nos da finalmente

$$\alpha(1 : 0 : 0) = (0 : 1 : 0).$$

De esta manera, tenemos que el morfismo α está definido sobre todo C_1

Por otro lado, existe una forma para regresar de la curva C_2 a C_1 y es de la siguiente manera: si a la ecuación de la curva C_2 la multiplicamos por u^2w y hacemos el cambio de variable $x = u^2$, $y = vw$, $z = uw$, obtenemos $(x : y : z) \in C_1$. Es decir tenemos el morfismo $\beta : C_2 \to C_1$ definido por $\beta(u : v : w) = (u^2 : vw : uw)$. Al igual que para el morfismo α, debemos de tener cuidado cuando u^2, vw, uw se anulen simultáneamente, pues allí vamos a tener que trabajar con los puntos $(0 : v : 0) = (0 : 1 : 0)$ y $(0 : 0 : w) = (0 : 0 : 1)$, puntos que se encuentran en C_2. Para obtener la imagen de $(0 : 1 : 0)$, debemos de tener en cuenta que estamos trabajando con morfismos racionales en variedades proyectivas, y por ello es posible reemplazar la definición dada de α por otra equivalente, a saber:

$$[u^2 : vw : uw] = [u^3 : uvw : u^2w].$$

Asimismo, usando el hecho de que para puntos $(u : v : w) \in C_2$ se cumple $u^3 = v^2w + 2uvw + 3vw^2 - 4u^2w$, obtenemos

$$[u^2 : vw : uw] = [u^3 : uvw : u^2w] = [v^2w + 2uvw + 3vw^2 - 4u^2w : uvw : u^2w].$$

Ahora factorizamos w y obtenemos

$$[u^2 : vw : uw] = [v^2 + 2uv + 3vw - 4u^2 : uv : u^2],$$

como funciones racionales en C_2. Evaluando el lado derecho de la última igualdad en $[0 : 1 : 0]$ se tiene

$$\beta(0 : 1 : 0) = (1 : 0 : 0).$$

Ahora para hallar la imagen de $(0 : 0 : 1)$ seguiremos un argumento similar. En coordenadas homogéneas tenemos

$$[u^2 : vw : uw] = [u^2(v + 2u + 3w) : vw(v + 2u + 3w) : uw(v + 2u + 3w)].$$

Dado que para puntos $(u : v : w) \in C_2$ se tiene la identidad $vw(v + 2u + 3w) = u^2(u + 4w)$, el lado derecho es equivalente a:

$$[u^2 : vw : uw] = [u^2(v + 2u + 3w) : u^2(u + 4w) : uw(v + 2u + 3w)].$$

Podemos ahora factorizar u y obtenemos finalmente

$$[u^2 : vw : uw] = [u(v + 2u + 3w) : u(u + 4w) : w(v + 2u + 3w)],$$

como funciones racionales en C_2. Evaluando el lado derecho de la última igualdad en el punto $[0 : 0 : 1]$ nos da finalmente

$$\beta(0 : 0 : 1) = (0 : 0 : 3) = (0 : 0 : 1).$$

De esta manera, tenemos que el morfismo β está definido sobre todo C_2.

Ahora veamos los puntos en el infinito de la curva C_1. Al reemplazar $z = 0$ en la ecuación de la curva C_1 se tiene $xy^2 = 0$, de ello se desprende que los puntos en el infinito de la curva C_1 son $(1 : 0 : 0)$ y $(0 : 1 : 0)$.

En el caso de la curva C_2, para hallar los puntos en el infinito reemplazamos $w = 0$ en la ecuación de la curva C_2 obteniendo $0 = u^3$. Es decir que el punto en el infinito de la curva C_2 es $(0 : 1 : 0)$.

Tenemos que se cumple $\alpha(1 : 0 : 0) = (0 : 1 : 0)$ y $\alpha(0 : 1 : 0) = (0 : 3 : -1)$, y por ello observamos que el morfismo α no preserva los puntos en el infinito.

Notamos que α no es una biyección pues $\alpha(1 : 1 : 0) = \alpha(1 : 0 : 0) = (0 : 1 : 0)$.

Los morfismos de interés en esta tesis son aquellos que preservan la colinealidad pues ellos corresponden a los homomorfismos de grupos algebraicos.

Capítulo 2

Curvas elípticas

A lo largo de este capítulo veremos las formas canónicas de las curvas elípticas según la característica del cuerpo donde se trabaje. Para este capítulo se pueden consultar [1], [3], [7], [8], [10], [11].

2.1 Singularidades de curvas cúbicas

Sea $\mathbb{K}$ un cuerpo. Un polinomio no constante $f \in \mathbb{K}[x, y]$ define una curva afín $\mathcal{C}$ en $\mathbb{K}^2$ vía

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

Todo punto $(x, y) \in \mathbb{K}^2$ que satisface

$$\frac{\partial f}{\partial x}(x, y) = \frac{\partial f}{\partial y}(x, y) = 0$$

se dice **singular** si $(x, y) \in \mathcal{C}$; caso contrario decimos que es **no singular** o **regular**.

Ejemplo 2.1. Sea la curva $\mathcal{C} = \{(x, y) \in \mathbb{F}_2^2 : f(x, y) = y^2+y+xy-x^3-x^2-x-1 = 0\}$. Determinemos los puntos singulares de $\mathcal{C}$ mediante el sistema

$$\begin{aligned} \frac{\partial f}{\partial x}(x, y) &= y - 3x^2 - 2x - 1 = 0, \\ \frac{\partial f}{\partial y}(x, y) &= 2y + 1 + x = 1 + x = 0. \end{aligned}$$

De la segunda ecuación obtenemos $x = 1$ y al reemplazarlo en la primera ecuación se tiene $y = 0$, y como $(1, 0)$ pertenece a la curva $\mathcal{C}$ concluimos que es el único punto singular.

Ejemplo 2.2. Determinemos los puntos singulares de la curva $C = \{(x, y) \in \mathbb{F}_3^2 : f(x, y) = y^2 - x^3 - x^2 - 2x - 1 = 0\}$ con ayuda de

$$\begin{aligned} \frac{\partial f}{\partial x}(x, y) &= -3x^2 - 2x - 2 = x + 1 = 0, \\ \frac{\partial f}{\partial y}(x, y) &= 2y = 0. \end{aligned}$$

Obtenemos $x = 2$, $y = 0$; como se tiene $(2, 0) \notin C$, no hay puntos singulares.

Ejemplo 2.3. Consideremos la curva afín $\mathcal{C} = \{(x, y) \in \mathbb{F}_5^2 : f(x, y) = y^2 + xy + 3y - x^3 - 4x^2 - 2x - 2 = 0\}$. Calculemos sus puntos de singularidad:

$$\begin{aligned}\frac{\partial f}{\partial x}(x, y) &= y - 3x^2 - 8x - 2 = y + 2x^2 + 2x + 3 = 0,\\ \frac{\partial f}{\partial y}(x, y) &= 2y + x + 3 = 0.\end{aligned}$$

De la segunda ecuación se desprende $y = 2x+1$ que al ser reemplazado en la primera ecuación lleva a $2x^2 + 4x + 4 = 0$, cuyas soluciones son $x = 1$, $x = 2$. De los pares $(1, 3)$ y $(2, 0)$ tenemos que solamente el segundo pertenece a $\mathcal{C}$; y por lo tanto es su único punto singular.

De manera similar, un polinomio homogéneo no constante $F \in \mathbb{K}[x, y, z]$ define una curva proyectiva $\mathcal{D}$ sobre $\mathbb{P}^2_{\mathbb{K}}$ como

$$\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{K}} : F([x : y : z]) = 0\}.$$

En tal caso todo punto $P = [x_0 : y_0 : z_0]$ que satisface

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0$$

se dice **singular** si $P \in \mathcal{D}$; caso contrario decimos que es **no singular** o **regular**.

Ejemplo 2.4. Sea el polinomio $F([x : y : z]) = y^2z + yz^2 + xyz - x^3 - x^2z - xz^2 - z^3$ sobre el cuerpo $\mathbb{F}_2$. Calculemos los puntos singulares de la curva proyectiva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{F}_2} : F([x : y : z]) = 0\}$. Para $[x : y : z]$ un punto singular de la curva proyectiva $\mathcal{D}$, tenemos

$$\frac{\partial F}{\partial x}([x : y : z]) = yz - 3x^2 - 2xz - z^2 = yz - x^2 - z^2 = 0, \tag{2.1}$$

$$\frac{\partial F}{\partial y}([x : y : z]) = 2yz + z^2 + xz = z^2 + xz = 0, \tag{2.2}$$

$$\frac{\partial F}{\partial z}([x : y : z]) = y^2 + 2yz + xy - x^2 - 2xz - 3z^2 = y^2 + xy - x^2 - z^2 = 0. \tag{2.3}$$

De 2.2 se obtiene $z(z + x) = 0$ y se tienen dos casos. Si $z = 0$, de 2.1 obtenemos $-x^2 = 0$ con lo cual $x = 0$ y de 2.3 se desprende $y = 0$ lo cual es absurdo pues en el espacio proyectivo no podemos aceptar el punto $[0 : 0 : 0]$. Por lo tanto, tenemos $z = x$ y al reemplazarlo en 2.1 se cumple $xy = 0$. Luego de 2.3 se desprende $y^2 = 0$ con lo cual nuestro punto es $[x : 0 : x] = [1 : 0 : 1]$, el mismo que está en la curva $\mathcal{D}$ y por lo tanto el único punto singular de la curva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{F}_2} : F([x : y : z]) = 0\}$.

Ejemplo 2.5. Dado el polinomio $F([x : y : z]) = y^2z - x^3 - x^2z - 2xz^2 - z^3$ sobre el cuerpo $\mathbb{F}_3$, calculemos las singularidades de la curva proyectiva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{F}_3} : F([x : y : z]) = 0\}$. Para $[x : y : z]$ un punto singular de la curva $\mathcal{D}$, tenemos

$$\frac{\partial F}{\partial x}([x : y : z]) = -3x^2 - 2xz - 2z^2 = -2xz - 2z^2 = 0, \tag{2.4}$$

$$\frac{\partial F}{\partial y}([x : y : z]) = 2yz = 0, \tag{2.5}$$

$$\frac{\partial F}{\partial z}([x : y : z]) = y^2 - x^2 - 4xz - 3z^2 = y^2 - x^2 - 4xz = 0. \tag{2.6}$$

De 2.5 tenemos dos posibilidades. Si $z = 0$, de 2.6 se desprende $y = x$ con lo cual $[1 : 1 : 0]$ es solución del sistema; pero como no pertenece a la curva $\mathcal{D}$ no lo tomaremos en consideración. Por otro lado, si $y = 0$, de 2.6 tenemos $x(x + 4z) = 0$. Para el caso $x = 0$, observamos de 2.4 que se cumple $z = 0$ y de 2.6 que se cumple $y = 0$, lo cual es absurdo pues $[0 : 0 : 0]$ no pertenece al espacio proyectivo. Ahora para $x = z$, de 2.4 tenemos $x = 0$ lo cual es absurdo pues sobre el espacio proyectivo no se puede tener el punto $[0 : 0 : 0]$. En resumen, no existen puntos singulares en la curva proyectiva $\mathcal{D}$.

Ejemplo 2.6. Sea el polinomio $F([x : y : z]) = y^2z+xyz+3yz^2-x^3-4x^2z-2xz^2-2z^3$ sobre el cuerpo $\mathbb{F}_5$. Si $[x : y : z]$ es un punto singular de la curva proyectiva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{F}_5} : F([x : y : z]) = 0\}$, se tiene

$$\frac{\partial F}{\partial x}([x : y : z]) = yz - 3x^2 - 8xz - 2z^2 = 0, \tag{2.7}$$

$$\frac{\partial F}{\partial y}([x : y : z]) = 2yz + xz + 3z^2 = z(2y + x + 3z) = 0, \tag{2.8}$$

$$\frac{\partial F}{\partial z}([x : y : z]) = y^2 + xy + 6yz - 4x^2 - 4xz - 6z^2 = 0. \tag{2.9}$$

De 2.8, tenemos $z = 0$ ó $2y + x + 3z = 0$. Si $z = 0$, tenemos $x = 0$ de 2.7 y de 2.9 se desprende $y = 0$.

Por otra parte, si $x = 3y+2z$, de 2.7 se obtiene $y(3y+z) = 0$ con lo cual tenemos $y = 0$ ó $y = 3z$. Si $y = 3z$, entonces de 2.9 se tiene $z^2 = 0$ y con ello $z = 0$, lo cual es absurdo. Por lo tanto nos queda el caso $y = 0$ lo cual nos da $x = 2z$ que al reemplazarlo en 2.9 deriva en $-30z^2 \equiv 0$. Es decir, la solución del sistema es el punto $[2z : 0 : z] = [2 : 0 : 1]$ que pertenece a la curva $\mathcal{D}$.

Existe un procedimiento estándar en el cual un polinomio de grado n en dos variables puede asociarse con uno homogéneo en tres variables llamado **homogenización**, el cual se define por $F(x, y, z) = z^n f\left(\frac{x}{z}, \frac{y}{z}\right)$. Para regresar al polinomio original $f(x, y)$ basta tomar $z = 1$.

Dado el polinomio $f(x, y) = y^2 + y + xy - x^3 - x^2 - x - 1$, su homogenización es $F([x : y : z]) = y^2z + yz^2 + xyz - x^3 - x^2z - xz^2 - z^3$. Por los ejemplos 2.1 y 2.4, tenemos que las singularidades de las curvas $\mathcal{C} = \{(x, y) \in \mathbb{K}^2 : f(x, y) = 0\}$ y $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{K}} : F([x : y : z]) = 0\}$ se dan en $(1, 0)$ y $[1 : 0 : 1]$, respectivamente. En el caso de $f(x, y) = y^2 - x^3 - x^2 - 2x - 1$, su homogenización es $F([x : y : z]) = y^2z - x^3 - x^2z - 2xz^2 - z^3$. Por los ejemplos 2.2 y 2.5, en ninguno de los dos casos existen puntos de singularidad. Podríamos decir que si una curva afín no tiene singularidades, tampoco las tendrá su versión homogenizada y viceversa. Lastimosamente, eso no es cierto pues la curva $\mathcal{C} = \{(x, y) \in \mathbb{R}^2 : f(x, y) = y - x^3 = 0\}$ no tiene puntos singulares ($f_y(x, y) = 1 \neq 0$); mientras que su clausura proyectiva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{R}} : F([x : y : z]) = yz^2 - x^3 = 0\}$, cuyas derivadas parciales son $F_x([x : y : z]) = -3x^2$, $F_y([x : y : z]) = -z^2$ y $F_z([x : y : z]) = 2yz$, tiene un punto singular el cual es $[0 : 1 : 0]$.

Dada la curva $\mathcal{C} = \{(x, y) \in \mathbb{K}^2 : f(x, y) = 0\}$ y su clausura proyectiva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{K}} : F([x : y : z]) = 0\}$, diremos que P es un **punto al infinito** de la curva $\mathcal{C}$ cuando interceptamos la recta $z = 0$ con la curva proyectiva.

Ejemplo 2.7. Sea la curva $\mathcal{C} = \{(x, y) \in \mathbb{K}^2 : f(x, y) = x^3 - 3y + x^2 = 0\}$. Tenemos que su clausura proyectiva es $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{K}} : F([x : y : z]) = x^3 - 3yz^2 + x^2z = 0\}$. Si interceptamos la curva proyectiva $\mathcal{D}$ con $z = 0$, se tiene $x^3 = 0$, lo cual nos lleva a que $x = 0$ y por ello nuestro punto al infinito es $[0 : 1 : 0]$.

Ejemplo 2.8. Sea la curva $\mathcal{C} = \{(x, z) \in \mathbb{K}^2 : f(x, z) = x^3 - 3xz + z = 0\}$. Tenemos que su clausura proyectiva es $\mathcal{D} = \{[x : z : y] \in \mathbb{P}^2_{\mathbb{K}} : F([x : z : y]) = x^3 - 3xzy + zy^2 = 0\}$. En este caso vamos a interceptar la curva proyectiva $\mathcal{D}$ con $y = 0$, de donde obtendremos que $x^3 = 0$, lo cual nos lleva a que $x = 0$ y por ello nuestro punto al infinito es $[0 : 0 : 1]$.

Ejemplo 2.9. Ahora consideremos la curva $\mathcal{C} = \{(x, y) \in \mathbb{K}^2 : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\}$, cuya clausura proyectiva es $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{K}} : F([x : y : z]) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0\}$. Al interceptar la curva proyectiva con $z = 0$, se tiene que $x^3 = 0$, es decir $x = 0$ y con ello el punto al infinito es $[0 : 1 : 0]$.

A continuación definiremos el concepto de curva elíptica que será el tema central de este trabajo.

Sean a_1, a_2, a_3, a_4 y a_6 elementos de un cuerpo $\mathbb{K}$. Una **curva elíptica** construida sobre $\mathbb{K}$, denotada por $E(\mathbb{K})$, es una curva no singular determinada por la ecuación

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.10}$$

junto con su punto al infinito $\mathcal{O} = [0 : 1 : 0]$, el cual fue calculado en el ejemplo anterior. Es decir, formalmente estudiaremos objetos del tipo

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}.$$

La curva elíptica $E(\mathbb{K})$ puede ser incrustada en el espacio proyectivo $\mathbb{P}^2_{\mathbb{K}}$ al homogenizar la ecuación (2.10) al agregar el factor z de la siguiente manera

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{2.11}$$

la cual es llamada **forma de Weierstrass**.

Consideremos la función $F([x : y : z]) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3$. En este caso tenemos

$$\begin{aligned}
\frac{\partial F}{\partial x} &= a_1yz - 3x^2 - 2a_2xz - a_4z^2, \\
\frac{\partial F}{\partial y} &= 2yz + a_1xz + a_3z^2, \\
\frac{\partial F}{\partial z} &= y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3a_6z^2.
\end{aligned}$$

Como $\dfrac{\partial F}{\partial z}(\mathcal{O}) = 1 \neq 0$, entonces se tiene que $\mathcal{O}$ es un punto no singular de la curva proyectiva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{K}} : F([x : z : y]) = 0\}$.

Así como la curva elíptica $E(\mathbb{K})$ puede pasar del espacio afín al proyectivo, también podemos llevarla del espacio proyectivo al afín al deshomogenizar la ecuación (2.11), es decir, al poner $z = 1$, para finalmente retomar la ecuación (2.10).

Lema 2.10. *Sea $f \in \mathbb{K}[x, y]$ el polinomio $f(x, y) = y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6$. Consideremos la curva afín $\mathcal{C}$ $\{(x, y) \in \mathbb{K}^2 : f(x, y) = 0\}$, y su correspondiente curva proyectiva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{K}} : F([x : y : z]) = 0\}$, donde $F \in \mathbb{K}[x, y, z]$ es la homogenización de f. Se cumple que el punto en el infinito $\mathcal{O}$ es no singular, y que los puntos singulares de la curva proyectiva se encuentran en la parte afín. Además, si (x, y) es un punto singular de la curva afín, entonces $[x : y : 1]$ es un punto singular de la curva proyectiva.*

Prueba. Líneas atrás hemos visto que el punto en el infinito $\mathcal{O}$ es un punto no singular. Por otro lado, si tenemos un punto singular $[x : y : z]$ de la curva proyectiva, se tiene

$$\begin{aligned}
\frac{\partial F}{\partial x}[x : y : z] &= a_1yz - 3x^2 - 2a_2xz - a_4z^2 = 0,\\
\frac{\partial F}{\partial y}[x : y : z] &= 2yz + a_1xz + a_3z^2 = 0,\\
\frac{\partial F}{\partial z}[x : y : z] &= y^2 + a_1xy + 2a_3yz - a_2x^2 - 2a_4xz - 3a_6z^2 = 0.
\end{aligned}$$

De la segunda ecuación se tiene $z = 0$ o $2y + a_1x + a_3z = 0$. Para el caso $z = 0$ se tiene de la primera ecuación $x = 0$, lo cual al combinarlo con la tercera ecuación se obtiene $y = 0$, es decir tendremos el punto $[0 : 0 : 0]$ quien no pertenece al espacio proyectivo. Por lo tanto tenemos $z \neq 0$, y podemos afirmar que todo punto singular de la curva proyectiva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{K}} : F([x : y : z]) = 0\}$ es de la forma $[x : y : 1]$. Además, obsrevamos que si $[x : y : 1]$ es punto singular de la curva proyectiva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{K}} : F([x : y : z]) = 0\}$, entonces el punto (x, y) es punto singular de la curva $\mathcal{C} = \{(x, y) \in \mathbb{K}^2 : f(x, y) = 0\}$.

Como F es la homogenización de f se tiene $F([x : y : z]) = z^3 f\left(\frac{x}{z}, \frac{y}{z}\right)$, con derivadas

$$\begin{aligned}
\frac{\partial F}{\partial x}([x : y : z]) &= z^2\frac{\partial f}{\partial u}\left(\frac{x}{z}, \frac{y}{z}\right),\\
\frac{\partial F}{\partial y}([x : y : z]) &= z^2\frac{\partial f}{\partial v}\left(\frac{x}{z}, \frac{y}{z}\right),\\
\frac{\partial F}{\partial z}([x : y : z]) &= 3z^2 f\left(\frac{x}{z}, \frac{y}{z}\right) - xz\frac{\partial f}{\partial u}\left(\frac{x}{z}, \frac{y}{z}\right) - yz\frac{\partial f}{\partial v}\left(\frac{x}{z}, \frac{y}{z}\right).
\end{aligned}$$

Se puede observar que si (x, y) es un punto singular de la curva $\mathcal{C} = \{(x, y) \in \mathbb{K}^2 : f(x, y) = 0\}$, entonces $[x : y : 1]$ es un punto singular de la curva proyectiva $\mathcal{D} = \{[x : y : z] \in \mathbb{P}^2_{\mathbb{K}} : F([x : y : z]) = 0\}$. □

A continuación definamos el discriminante, concepto que permitirá en la siguiente sección decidir contundentemente si una curva de tipo

$$E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\},$$

posee algún punto singular o no. Consideremos las expresiones

$$\begin{aligned} d_2 &= a_1^2 + 4a_2, \\ d_4 &= a_1a_3 + 2a_4, \\ d_6 &= a_3^2 + 4a_6, \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ e_4 &= d_2^2 - 24d_4, \\ e_6 &= -d_2^3 + 36d_2d_4 - 216d_6. \end{aligned}$$

El **discriminante** τ de la ecuación de Weierstrass (2.10) se define como

$$\tau(E) = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6.$$

Ejemplo 2.11. La curva $\mathcal{C} = \{(x, y) \in \mathbb{F}_3^2 : f(x, y) = 0\}$, con $f(x, y) = y^2 - x^3 - x^2 - 2x - 1$, es elíptica pues no admite puntos singulares. En este caso su discriminante vale 1.

Ejemplo 2.12. La curva $\mathcal{C} = \{(x, y) \in \mathbb{F}_5^2 : f(x, y) = 0\}$, donde $f(x, y) = y^2 + xy + 3y - x^3 - 4x^2 - 2x - 2$, no es elíptica pues tiene un punto singular $(2, 0)$. Acá su discriminante es 0.

Veamos las distintas formas reducidas (y canónicas) que puedan adoptar las curvas elípticas al tomar en cuenta el valor de la característica del cuerpo $\mathbb{K}$ sobre el cual se trabaja si hacemos cambios lineales reversibles (los mismos que evidentemente preservan el carácter singular o no de una curva). A partir de ahora consideraremos τ como el discriminante de la forma de Weierstrass (2.10).

2.2 Formas canónicas en característica 2

Organizamos nuestro estudio en dos variantes.

Caso $a_1 = 0$**.** En este caso se tiene $d_2 = d_4 = 0$, $d_6 = a_3^2$, $d_8 = a_2a_3^2 - a_4^2$, $e_4 = e_6 = 0$ y $\tau = -27d_6^2 = d_6^2 = a_3^4$.

Primero veamos un ejemplo de curva elíptica, con $a_1 = 0$, que mediante un cambio de variables adoptará una forma más fácil de estudiar. Además, dicho cambio preservará el carácter singular o no de los puntos.

Ejemplo 2.13. La curva $E_1 : y^2 + y = x^3 + x^2 + 1$ definida sobre $\mathbb{F}_2$ es una curva elíptica (acá $\tau = 1 \neq 0$) . Hacemos el cambio de variable $t = x - 1$, $s = y$ para $(x, y) \in E_1$. Como $(t + 1, s) \in E_1$, se tiene

$$\begin{aligned} s^2 + s &= (t + 1)^3 + (t + 1)^2 + 1, \\ s^2 + s &= t^3 + t^2 + t + 1 + t^2 + 1 + 1, \\ s^2 + s &= t^3 + t + 1. \end{aligned}$$

Dada $E_2 : s^2 + s = t^3 + t + 1$, tenemos nuevamente que esta es una curva elíptica (nuevamente con $\tau = 1$). Ahora definamos la función $\psi : E_1 \to E_2$ como $\psi(x, y) =$

$(x-1, y)$, que está bien definida por lo anterior. Observamos que podemos pasar de la curva E_1 a E_2 mediante la función ψ, y con ello la curva E_1 adquiere una forma más manejable (dada por E_2). Obsérvese que en ambos casos el discriminante es simultáneamente distinto de 0.

Lema 2.14. *En un cuerpo algebraicamente cerrado de característica* 2 *una curva cúbica de la forma*

$$y^2 + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

es singular si y solo si $\tau = 0$.

Prueba. En primer lugar tenemos que el discriminante es cero si y solo si $a_3 = 0$, pues $\tau = a_3^4$.

Ahora bien, por el lema 2.10, analizar la singularidad del punto (x_0, y_0) en el espacio afín es lo mismo que analizar el punto $(x_0 : y_0 : 1)$ sobre el espacio proyectivo. Si un punto $P = [x_0 : y_0 : 1] \in E$ es singular, se ha de tener

$$\frac{\partial F}{\partial x}([x_0 : y_0 : 1]) = \frac{\partial F}{\partial y}([x_0 : y_0 : 1]) = \frac{\partial F}{\partial z}([x_0 : y_0 : 1]) = 0,$$

donde $F([x : y : z]) = y^2 z + a_3 y z^2 - x^3 - a_2 x^2 z - a_4 x z^2 - a_6 z^3$. Es decir, con los valores expresados, se debe cumplir

$$\begin{aligned} -3x_0^2 - a_4 &= 0 \\ a_3 &= 0 \\ y_0^2 - a_2 x_0^2 - a_6 &= 0. \end{aligned}$$

Lo anterior tiene solución en $a_3 = 0$ y $(x_0, y_0) = (\sqrt{a_4}, \sqrt{a_2 a_4 + a_6})$. Por lo tanto, podemos concluir que la curva de Weierstrass es singular si y solo si a_3 (y con ello τ) se anula. □

En un cuerpo algebraicamente cerrado, donde la característica del cuerpo es 2 y se tiene $a_1 = 0$, con el cambio $x = x' + a_2$ obtenemos

$$y^2 + a_3 y = x^3 + b_4 x + b_6,$$

donde $b_4 = a_2^2 + a_4$, $b_6 = a_4 a_2 + a_6$, y el discriminante sigue siendo a_3^4.

Si además hacemos el cambio $y = a_3 y'$, $x = \sqrt[3]{a_3^2}\, x'$ obtenemos

$$y^2 + y = x^3 + c_4 x + c_6;$$

donde $c_4 = \dfrac{b_4}{\sqrt[3]{a_3^4}}$ y $c_6 = \dfrac{b_6}{a_3^2}$. Con este cambio, el discriminante es igual a 1. Es decir, mediante dicho cambio de coordenadas la curva de discriminante distinto de 0 se convierte en una curva cuyo discriminante es igual a 1.

Observación 2.15. El cambio de variable anterior tiene sentido si y solo si $\sqrt[3]{a_3^2}$ pertenece al cuerpo donde queremos trabajar, es decir no es indispensable asumir que $\mathbb{K}$ sea algebraicamente cerrado.

Ahora, si adicionalmente realizamos el cambio $x = x' + c_4$ tendremos

$$y^2 + y = x^3 + \alpha_2 x^2 + \alpha_6;$$

donde $\alpha_2 = c_4$ y $\alpha_6 = c_6$, con discriminante igual a 1.

Curiosamente el mismo cambio $x = x' + \alpha_2$ nos regresa a la anterior versión $y^2 + y = x^3 + c_4 x + c_6$ y el discriminante sigue siendo 1.

Caso $a_1 \neq 0$**.** En este caso se tiene $d_2 = a_1^2$, $d_4 = a_1 a_3$, $d_6 = a_3^2$, $d_8 = a_1^2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$ y $\tau = -d_2^2 d_8 - 27 d_6^2 + 9 d_2 d_4 d_6 = d_2^2 d_8 + d_6^2 + d_2 d_4 d_6$.

Si hacemos el cambio de variable $x = a_1^2 x' + \dfrac{a_3}{a_1}$, $y = a_1^3 y' + \dfrac{a_1^2 a_4 + a_3^2}{a_1^3}$ obtenemos la forma

$$y^2 + xy = x^3 + a_2' x^2 + a_6',$$

donde $a_2' = \dfrac{a_3 + a_1 a_2}{a_1^3}$, $a_6' = \dfrac{a_1^6 a_6 + a_1^5 a_3 a_4 + a_1^4 a_2 a_3^2 - a_1^4 a_4^2 - a_3^4 - a_1^3 a_3^3}{a_1^6}$. Tenemos $d_2' = 1$, $d_4' = 0$, $d_6' = 0$, $d_8' = a_6'$ y el nuevo discriminante resulta $\tau' = -a_6'$. Con respecto a los valores originales, este τ' vale $\dfrac{\tau}{a_1^{12}}$.

Ahora veremos una curva con $a_1 \neq 0$ que mediante un cambio de variables toma una forma menos compleja a estudiar. Lo importante de ese cambio es que se preserva la singularidad o no de las mismas.

Ejemplo 2.16. Sobre $\mathbb{F}_2$ definamos la curva $E_3 : y^2 + xy + y = x^3 + x + 1$, con $\tau = 1 \neq 0$. Guiándonos del cambio de coordenadas dado anteriormente, tomaremos $t = x - 1$, $s = y$ para $(x, y) \in E_3$. Como $(t + 1, s) \in E_3$, se tiene

$$\begin{aligned} s^2 + (t+1)s + s &= (t+1)^3 + t + 1 + 1, \\ s^2 + ts + s + s &= t^3 + t^2 + t + 1 + t + 1 + 1, \\ s^2 + ts &= t^3 + t^2 + 1. \end{aligned}$$

Sea $E_4 : s^2 + ts = t^3 + t^2 + 1$, la cual también satisface $\tau = 1$. Definamos la función $\psi : E_3 \to E_4$ como $\psi(x, y) = (x - 1, y)$, que está bien definida por lo anterior. Tenemos que podemos pasar de la curva E_3 a E_4 mediante la función ψ, y con esto la curva E_3 se ve en una forma más fácil dada por E_4, además el discriminante sigue siendo distinto de 0.

Lema 2.17. *En un cuerpo algebraicamente cerrado de característica* 2 *una curva cúbica de la forma*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

con $a_1 \neq 0$*, es singular si y solo si* $\tau = 0$*.*

Prueba. Sabemos que existe un cambio de coordenadas que nos permite pasar de la curva general a la curva $y^2 + xy = x^3 + a_2 x^2 + a_6$. Por ello, la curva general es singular si y solo si la curva $y^2 + xy = x^3 + a_2' x + a_6'$ es singular, y de esta forma podemos limitarnos a trabajar con la segunda ya que el discriminante de uno es

un múltiplo no nulo del discriminante de la otra. En primer lugar notemos que el discriminante vale cero si y sólo si $a_6' = 0$, pues $\tau = -a_6'$.

Por el lema 2.10, analizar la singularidad del punto (x_0, y_0) en el espacio afín es lo mismo que analizar el punto $[x_0 : y_0 : 1]$ sobre el espacio proyectivo.

Si un punto $P = [x_0 : y_0 : 1] \in E$ es singular, se ha de tener

$$\frac{\partial F}{\partial x}([x_0 : y_0 : 1]) = \frac{\partial F}{\partial y}([x_0 : y_0 : 1]) = \frac{\partial F}{\partial z}([x_0 : y_0 : 1]) = 0,$$

donde $F(x : y : z) = y^2z + xyz - x^3 - a_2'x^2z - a_6'z^3$. Es decir, con los valores expresados, se debe cumplir

$$\begin{aligned} y_0 - 3x_0^2 &= 0 \\ x_0 &= 0 \\ y_0^2 + x_0y_0 - a_2'x_0^2 - 3a_6' &= 0. \end{aligned}$$

Lo anterior tiene única solución en $a_6' = 0$ y $(x_0, y_0) = (0, 0)$. Por lo tanto, podemos concluir que la curva en forma de Weierstrass es singular si y solo si su discriminante se anula. □

Ejemplo 2.18. Sea la curva $y^2 + xy = x^3$. En este caso se tiene $a_1 = 1$, $a_3 = 0$, $a_2 = 0$, $a_4 = 0$, $a_6 = 0$, $d_2 = 1$, $d_4 = 0$, $d_6 = 0$, $d_8 = 0$, y concluimos que el discriminante vale $\tau = d_2^2d_8 + d_6^2 + d_2d_4d_6 = 0$. Notemos que la curva es singular en $(0, 0)$.

2.3 Característica distinta de 2

Comenzamos con unos ejemplos típicos que nos permitan simplificar la forma de una curva elíptica mediante un cambio de coordenadas reversible.

Ejemplo 2.19. La curva $E_1 : y^2 + 3xy + y = x^3 + x^2 + 2x + 1$, definida sobre $\mathbb{F}_5$, satisface $\tau = 2$. Hacemos el cambio de variable $t = x$, $s = y + 4x + 3$ para $(x, y) \in E_1$. Como $(t, s - 4t - 3) \in E_1$, tenemos

$$\begin{aligned} (s - 4t - 3)^2 + 3t(s - 4t - 3) + s - 4t - 3 &= t^3 + t^2 + 2t + 1, \\ s^2 &= t^3 + t. \end{aligned}$$

Sea la curva $E_2 : s^2 = t^3 + t$ y consideremos la función $\psi : E_1 \to E_2$ definida por $\psi(x, y) = (x, y + 4x + 3)$ que está bien definida por lo visto anteriormente. La función ψ convierte la curva E_1 en E_2, la cual evidentemente es una forma más sencilla de estudiar; el discriminante de E_2 vale 2.

Ejemplo 2.20. La curva $E_1 : y^2 + 2xy + 2y = x^3 + x^2 + x + 3$, definida sobre $\mathbb{F}_5$, cumple $\tau = 3$. Hacemos el cambio de variable $t = x$, $s = y + x + 1$ para $(x, y) \in E_1$. Como $(t, s - t - 1) \in E_1$, se obtiene

$$\begin{aligned} (s - t - 1)^2 + 2t(s - t - 1) + 2(s - t - 1) &= t^3 + t^2 + 2t + 3, \\ s^2 &= t^3 + 2t^2 + 4t + 3. \end{aligned}$$

La curva $E_2 : s^2 = t^3 + 2t^2 + 4t + 3$ retorna a su forma original con ayuda de la función $\psi : E_1 \to E_2$ definida por $\psi(x, y) = (x, y + x + 1)$. Acá el discriminante de E_2 también vale 3.

Ejemplo 2.21. La curva $E_1 : y^2 + 2xy = x^3 + x^2 + x + 2$, definida sobre $\mathbb{F}_3$, es elíptica pues $\tau = 2$. Hacemos el cambio de variable $t = x$, $s = y+x$ para $(x, y) \in E_1$. Como $(t, s - t) \in E_1$, tenemos

$$\begin{aligned} (s-t)^2 + 2t(s-t) &= t^3 + t^2 + t + 2, \\ s^2 &= t^3 + 2t^2 + t + 2. \end{aligned}$$

Sea la curva elíptica $E_2 : s^2 = t^3 + 2t^2 + t + 2$. La función $\psi : E_1 \to E_2$, donde $E_2 : s^2 = t^3 + 2t^2 + t + 2$, definida por $\psi(x, y) = (x, y + x)$, nos permite facilitar la expresión de E_1 al convertirla en la curva elíptica E_2, cuyo discriminante es 2.

Ejemplo 2.22. La curva $E_1 : y^2 + 2xy + y = x^3 + 2x^2 + x + 1$, definida sobre $\mathbb{F}_3$, es elíptica pues cumple $\tau = 1$. Hacemos el cambio de variable $t = x$, $s = y + x + 2$ para $(x, y) \in E_1$. Como $(t, s - t - 2) \in E_1$, tenemos

$$\begin{aligned} (s-t-2)^2 + 2t(s-t-2) + s - t - 2 &= t^3 + 2t^2 + t + 1, \\ s^2 &= t^3 + 2t + 2. \end{aligned}$$

Sea la curva elíptica $E_2 : s^2 = t^3 + 2t + 1$. La función $\psi : E_1 \to E_2$, definida por $\psi(x, y) = (x, y + x + 2)$, nos permite facilitar la expresión de E_1 al convertirlo en la curva elíptica E_2. El discriminante de E_2 vale 1.

Los cuatro ejemplos anteriores se pueden generalizar de la siguiente manera: cuando la característica no es 2, hacemos el cambio $y = y' - \frac{a_1}{2}x' - \frac{a_3}{2}$ para pasar de $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, con $d_2 = a_1^2 + 4a_2$, $d_4 = a_1a_3 + 2a_4$, $d_6 = a_3^2 + 4a_6$, $d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$ y con discriminante $\tau = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$, a la forma estándar

$$y^2 = x^3 + b_2x^2 + b_4x + b_6;$$

donde $b_2 = \frac{a_1^2 + 4a_2}{4}$, $b_4 = \frac{2a_4 + a_1a_3}{2}$, $b_6 = \frac{a_3^2 + 4a_6}{4}$. Para esta última curva los valores d_i' y e_i' a considerar serán

$$\begin{aligned} d_2' &= 4b_2 &&= d_2, \\ d_4' &= 2b_4 &&= d_4, \\ d_6' &= 4b_6 &&= d_6, \\ d_8' &= 4b_2b_6 - b_4^2 &&= d_8, \\ e_4' &= (d_2')^2 - 24d_4' &&= e_4, \\ e_6' &= -(d_2')^3 + 36d_2'd_4' - 216d_6' &&= e_6. \end{aligned}$$

Por lo tanto, el nuevo discriminante τ' es igual a τ.

Veremos más adelante que las curva es singular si y solo si el discriminante se anula, tal como sucedió en la sección 2.2.

Observación 2.23. Notemos que la forma $y^2 = x^3 + b_2x^2 + b_4x + b_6$ es siempre singular en característica 2.

2.3.1 Característica distinta de 2 y 3

Cuando la característica es distinta de 2 y 3, entonces el cambio $x = x' + \frac{b_2}{3}$ adicional a lo hecho en la página anterior conduce a

$$y^2 = x^3 + c_4 x + c_6;$$

donde $c_4 = -\frac{3b_4 - b_2^2}{3}$, $c_6 = \frac{27b_6 - 9b_2b_4 + 2b_2^3}{27}$. Tenemos $d_2 = 0$, $d_4 = 2c_4$, $d_6 = 4c_6$, $d_8 = -c_4^2$ y un nuevo discriminante $\tau' = -16(4c_4^3 + 27c_6^2) = -16(4b_2^3b_6 + 4b_4^3 + 27b_6^2 - 18b_2b_4b_6)$. Obsérvese la igualdad $\tau' = \tau$.

Procederemos a mostrar que la curva es singular si y solo si el discriminante se anula.

Lema 2.24. *En un cuerpo algebraicamente cerrado de característica distinta de* 2 *y* 3 *una curva cúbica de la forma*

$$y^2 = x^3 + c_4 x + c_6$$

es singular si y solo si $\tau = 0$.

Prueba. Por el lema 2.10, analizar la singularidad del punto (x_0, y_0) en el espacio afín es lo mismo que analizar el punto $[x_0 : y_0 : 1]$ sobre el espacio proyectivo. Si un punto $P = [x_0 : y_0 : 1] \in E$ es singular, se ha de tener

$$\frac{\partial F}{\partial x}([x_0 : y_0 : 1]) = \frac{\partial F}{\partial y}([x_0 : y_0 : 1]) = \frac{\partial F}{\partial z}([x_0 : y_0 : 1]) = 0,$$

donde $F([x : y : z]) = y^2z - x^3 - c_4xz^2 - c_6z^3$. Es decir, con los valores expresados, se debe cumplir

$$\begin{aligned} -3x_0^2 - c_4 &= 0 \\ 2y_0 &= 0 \\ y_0^2 - 2c_4x_0 - 3c_6 &= 0. \end{aligned}$$

Se desprende la igualdad $y_0 = 0$ y obtenemos el sistema

$$\begin{aligned} 3x_0^2 + c_4 &= 0, \\ 2c_4x_0 + 3c_6 &= 0. \end{aligned}$$

Si $c_4 = 0$, entonces $c_6 = 0$. Cuando $c_4 \neq 0$, de la segunda ecuación se tiene $x_0 = -\frac{3c_6}{2c_4}$, que si lo reemplazamos en la primera ecuación lleva a $\frac{27c_6^2 + 4c_4^3}{4c_4^2} = 0$. Por lo tanto, en ambos casos se tiene $\tau = 0$ y concluimos que la curva de Weierstrass es singular si y sólo si su discriminante se anula. □

Ejemplo 2.25. Sobre $\mathbb{F}_5$ las curvas: $E_1 : y^2 = x^3 + x + 1$ y $E_2 : y^2 = x^3 - x + 1$ son no singulares, mientras que: $E_3 : y^2 = x^3 - 3x + 2$, $E_4 : y^2 = x^3 - 3x - 2$, $E_5 : y^2 = x^3$ son singulares.

2.3.2 Característica igual a 3

Como la característica del cuerpo es distinta de 2, toda cúbica es equivalente a una de la forma

$$y^2 = x^3 + b_2x^2 + b_4x + b_6.$$

En este caso tenemos $b_1 = b_3 = 0$, $d_2 = b_2$, $d_4 = 2b_4$, $d_6 = b_6$ y $d_8 = b_2b_6 - b_4^2$. Y el discriminante está dado por $\tau = 2b_2^3b_6 + b_2^2b_4^2 + 2b_4^3$.

Veamos a continuación que nuevamente la curva es singular si y solo si su discriminante vale cero.

Lema 2.26. *En un cuerpo algebraicamente cerrado de característica* 3 *una curva cúbica de la forma*

$$y^2 = x^3 + b_2x^2 + b_4x + b_6$$

es singular si y solo si $\tau = 0$.

Prueba. Por el lema 2.10, analizar la singularidad del punto (x_0, y_0) en el espacio afín es lo mismo que analizar el punto $[x_0 : y_0 : 1]$ sobre el espacio proyectivo. Si un punto $P = [x_0 : y_0 : 1] \in E$ es singular, se ha de tener

$$\frac{\partial F}{\partial x}([x_0 : y_0 : 1]) = \frac{\partial F}{\partial y}([x_0 : y_0 : 1]) = \frac{\partial F}{\partial z}([x_0 : y_0 : 1]) = 0,$$

donde $F([x : y : z]) = y^2z - x^3 - b_2x^2z - b_4xz^2 - b_6z^3$. Es decir, con los valores expresados, se debe cumplir

$$\begin{aligned} -2b_2x_0 - b_4 &= 0 \\ 2y_0 &= 0 \\ y_0^2 - b_2x_0^2 - 2b_4x_0 &= 0. \end{aligned}$$

Se desprende la igualdad $y_0 = 0$ y obtenemos el sistema

$$\begin{aligned} 2b_2x_0 + b_4 &= 0, \\ b_2x_0^2 + 2b_4x_0 &= 0. \end{aligned}$$

Si $b_2 = 0$, entonces $b_4 = 0$ y se tiene discriminante cero. Para $b_2 \neq 0$, de la primera ecuación, se tiene $x_0 = -\dfrac{b_4}{2b_2} = -\dfrac{2b_4}{b_2}$. Como $[x_0 : y_0 : 1]$ pertenece a la curva, obtenemos $2b_4^3 + b_4^2b_2^2 - b_6b_2^3 = 0$, es decir, el discriminante es nulo.

Si el discriminante es nulo, entonces $\tau = 2b_2^3b_6 + b_2^2b_4^2 + 2b_4^3 = 0$. Para $b_2 = 0$, se tiene $b_4 = 0$ y al tomar $x_0 = \sqrt[3]{2b_6}$, se concluye que $[x_0 : 0 : 1]$ es un punto singular. Para $b_2 \neq 0$, tomemos x_0 solución de $-2b_0x - b_4 = 0$. Se obtiene que $[x_0 : 0 : 1]$ es un punto singular. Por lo tanto, podemos concluir que la curva de Weierstrass es singular si y solo si su discriminante se anula. □

Ejemplo 2.27. Sobre $\mathbb{F}_3$ las curvas $E_1 : y^2 = x^3+2x^2+x+1$ y $E_2 : y^2 = x^3+2x^2-x$ son no singulares, mientras que $E_3 : y^2 = x^3 + x^2 + x$ y $E_4 : y^2 = x^3 + x^2 - x - 1$ son singulares.

Veamos unos ejemplos para reducir los términos de una curva elíptica mediante otro cambio de variable.

Ejemplo 2.28. Sobre el cuerpo $\mathbb{F}_3$, definamos la curva elíptica $E_1 : s^2 = t^3 + 2t^2 + t + 2$. A partir de E_1, hagamos el cambio $u = t - 2$, $v = s$. Como $(u + 2, v) \in E_1$, tenemos

$$\begin{aligned} v^2 &= (u+2)^3 + 2(u+2)^2 + u + 2 + 2, \\ v^2 &= u^3 + 2u^2 + 2. \end{aligned}$$

Dada la curva elíptica $E_2 : v^2 = u^3 + 2u^2 + 2$, observamos que $\phi : E_1 \to E_2$, definida por $\phi(t, s) = (t - 2, s)$, elimina el término t de la curva E_1.

Ejemplo 2.29. Dada la curva elíptica $E_1 : y^2 = x^3 + x^2 + x + 1$, sobre $\mathbb{F}_3$, hacemos el cambio $t = x - 1$, $s = y$. Como $(t + 1, s) \in E_1$, tenemos

$$\begin{aligned} s^2 &= (t+1)^3 + (t+1)^2 + t + 1 + 1, \\ s^2 &= t^3 + t^2 + 1. \end{aligned}$$

Dada la curva elíptica $E_2 : s^2 = t^3 + t^2 + 1$, observamos que $\phi : E_1 \to E_2$, definida por $\phi(x, y) = (x - 1, y)$, al igual que en el ejemplo anterior, permite libramos del término x.

En resumen, si la característica del cuerpo $\mathbb{K}$ donde se trabaje es distinto de 2, existe un cambio lineal de coordenadas que nos permite eliminar el término x de una curva elíptica $E : y^2 = x^3 + b_2x^2 + b_4x + b_6$.

Si $b_2 = 0$, tenemos

$$y^2 = x^3 + b_4'x + b_6',$$

la cual es llamada **forma corta de Weierstrass**. En caso se tenga $b_2 \neq 0$, el cambio $x = x' + \dfrac{b_4}{b_2}$ conduce a

$$y^2 = x^3 + \left(\frac{3b_4}{b_2} + b_2\right)x^2 + \left(\frac{3b_4^2}{b_2^2} + 3b_4\right)x + \frac{b_4^3}{b_2^3} + \frac{2b_4^2}{b_2} + b_6.$$

Es decir, que en cuerpos de característica 3 se obtiene la ecuación

$$y^2 = x^3 + b_2'x^2 + b_6',$$

donde $b_2' = b_2$, $b_6' = \dfrac{b_4^3 + 2b_4^2b_2^2 + b_6b_2^3}{b_2^3}$ con discriminante $\tau = 2(b_2')^3b_6'$.

2.4 El grupo definido por una curva elíptica

Las curvas elípticas definen de manera natural una suma, con la cual se obtiene un grupo abeliano sobre el conjunto de sus puntos.

Dados dos puntos $P,\ Q \in E(\mathbb{K})$, el teorema de Bezout garantiza la existencia de un tercer punto de intersección entre la recta L que los une y la curva $E(\mathbb{K})$; ello en el espacio proyectivo, por supuesto. Tomemos $P_1,\ P_2$ puntos en E presentados en alguna de sus formas de Weierstrass, y definamos un nuevo punto P_3 de la siguiente manera. Sea la recta L que pasa por P_1 y P_2. En el espacio proyectivo, L interseca

a E en un tercer punto P_3', en adelante $P_1 * P_2$, que reflejamos con respecto al eje X para obtener P_3; definimos así $P_3 = P_1 + P_2$.

A modo de ejemplo veamos cómo quedan las fórmulas si trabajamos con la curva elíptica $y^2 = x^3 + Ax + B$ sobre un cuerpo $\mathbb{K}$ de característica distinta de 2.

Consideremos primero $P_1 \neq P_2$ con ambos distintos de $\mathcal{O}$. La recta L a través de P_1 y P_2 tiene pendiente igual a $m = \dfrac{y_2 - y_1}{x_2 - x_1}$.

Si $x_1 \neq x_2$, la ecuación de L es $y = m(x - x_1) + y_1$. Para encontrar la intersección con E, sustituimos para obtener $[m(x - x_1) + y_1]^2 = x^3 + Ax + B$. Esto se puede escribir como $x^3 - m^2x^2 + ax + b = 0$. Las tres raíces de esta cúbica corresponden a los tres puntos de intersección de L con E, pero en este caso ya conocemos dos raíces x_1 y x_2, pues P_1 y P_2 son puntos de E y L. Por lo tanto, si $P_3' = (x_3',\ y_3')$, obtenemos

$$\begin{aligned} x_3' &= m^2 - x_1 - x_2 && (2.12)\\ y_3' &= m(x_3' - x_1) + y_1. && (2.13) \end{aligned}$$

A continuación, reflejamos con respecto al eje x para obtener el punto $P_3 = (x_3, y_3)$, donde

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 && (2.14)\\ y_3 &= m(x_1 - x_3) - y_1. && (2.15) \end{aligned}$$

En el caso $x_1 = x_2$, con $y_1 \neq y_2$, la recta a través de P_1 y P_2 es vertical y por lo tanto interseca a E en $\mathcal{O}$. Si reflejamos $\mathcal{O}$ con respecto al eje x obtenemos el mismo punto $\mathcal{O}$ (es por ello que ponemos $\mathcal{O}$). Por lo tanto, en este caso se logra $P_1 + P_2 = \mathcal{O}$.

Ahora consideremos el caso $P_1 = P_2 = (x_1, y_1)$. Como los dos puntos coinciden, tomamos la recta L a través de ellos como la recta tangente. Mediante diferenciación implícita obtenemos la pendiente de L como $m = \dfrac{3x_1^2 + A}{2y_1}$ con $y_1 \neq 0$ (en el caso $y_1 = 0$, estaremos en el caso de una recta vertical y por lo tanto se consigue $P_1 + P_2 = \mathcal{O}$ como en el caso anterior). Por lo tanto, si asumimos $y_1 \neq 0$, la ecuación de L es $y = m(x - x_1) + y_1$ y, como antes, obtenemos la ecuación cúbica $x^3 - m^2x^2 + ax + b = 0$. Esta vez conocemos sólo una raíz x_1, pero ésta es doble pues L es tangente a E en P_1. Si procedemos como arriba obtenemos

$$\begin{aligned} x_3 &= m^2 - 2x_1 && (2.16)\\ y_3 &= m(x_1 - x_3) - y_1. && (2.17) \end{aligned}$$

Finalmente, supongamos $P_2 = \mathcal{O}$. La recta a través de P_1 y $\mathcal{O}$ es una recta vertical que intersecta a E en el punto P_1' que es la reflexión de P_1 con respecto al eje x. Cuando reflejamos P_1' con respecto al eje x para obtener $P_3 = P_1 + P_2$, regresamos a P_1. Luego obtenemos $P_1 + \mathcal{O} = P_1$ para todo $P_1 \in E$.

En resumen, tenemos la siguiente información.

Proposición 2.30. *Sea E una curva elíptica sobre un cuerpo $\mathbb{K}$ de característica distinta de 2 definida por $y^2 = x^3 + Ax + B$. Sean $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ puntos*

en E con $P \neq \mathcal{O}$ y $Q \neq \mathcal{O}$. Entonces $P + Q = (x_3, y_3)$ se obtiene de la siguiente manera.

Si $x_1 \neq x_2$, entonces

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 && (2.18)\\ y_3 &= m(x_1 - x_3) - y_1 && (2.19)\\ m &= \frac{y_2 - y_1}{x_2 - x_1}. && (2.20) \end{aligned}$$

Si $x_1 = x_2$ pero $y_1 \neq y_2$, entonces $P + Q = \mathcal{O}$.
Si $P = Q$ e $y_1 \neq 0$, entonces

$$\begin{aligned} x_3 &= m^2 - 2x_1 && (2.21)\\ y_3 &= m(x_1 - x_3) - y_1 && (2.22)\\ m &= \frac{3x_1^2 + A}{2y_1}. && (2.23) \end{aligned}$$

Si $P = Q$ e $y_1 = 0$, entonces $P + Q = \mathcal{O}$.
Además tenemos $P + \mathcal{O} = P$ para todo $P \in E$.

Para una cúbica de la forma

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

se procede de manera similar y se obtienen fórmulas análogas. Los detalles pueden encontrarse en cualquier texto estándar como [2], [3], [14], o en la tesis de Iván Perez [10].

El siguiente teorema confirma que las curvas elípticas forman un grupo abeliano aditivo con $\mathcal{O}$ como elemento neutro.

Teorema 2.31. *La suma de puntos en cada curva elíptica E, sobre un cuerpo $\mathbb{K}$ de cualquier característica, satisface la siguientes propiedades:*

1. *conmutatividad: $P_1 + P_2 = P_2 + P_1$ para todo $P_1,\ P_2 \in E$;*
2. *existencia del neutro: $P + \mathcal{O} = P$ para todo $P \in E$;*
3. *existencia del inverso: dado $P \in E$, existe $P' \in E$ tal que $P + P' = \mathcal{O}$;*
4. *asociatividad: $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ para todo $P_1,\ P_2,\ P_3 \in E$.*

Los detalles para la demostración del teorema anterior se pueden ver por ejemplo en el tema de tesis de Iván Perez [10].

Observación 2.32. Si P es un punto de inflexión, entonces tendremos $P * P = P$, lo que equivale a escribir $P + P = -P$. En otras palabras, tendremos que P es un punto de inflexión de una curva elíptica si y solo si $3P = \mathcal{O}$. En el caso de $\mathbb{K} = \mathbb{C}$, es consecuencia del teorema de Riemann-Roch que E es un toro topológico, lo cual en este contexto significa que E tiene precisamente nueve puntos de inflexión, hecho conocido desde finales del siglo XIX. Para más detalles se puede ver en [15].

Capítulo 3

Isogenías

En este capítulo se definirán las isogenías entre curvas elípticas, lo cual nos ayudará a identificar los puntos racionales de una curva elíptica. Para el desarrollo de este capítulo se puede consultar también [2], [4], [6], [7], [11], [13], [14], [15].

Antes de pasar a ver la definición de isogenía, veamos el siguiente teorema que se puede ver con más detalle en [15].

Teorema 3.1. *Sean las curvas suaves C_1 y C_2 definidas sobre el cuerpo base $\mathbb{K}$. Si $\phi : C_1 \to C_2$ es un morfismo racional, entonces se satisface lo siguiente:*

- *ϕ se extiende a un morfismo de grupos la cual está definida en todo C_1,*
- *Si el cuerpo base es algebraicamente cerrado, entonces ϕ es constante o sobreyectivo.*

Sean E_1 y E_2 curvas elípticas. Una **isogenía** $\phi : E_1 \to E_2$ es un morfismo racional tal que $\phi(\mathcal{O}) = \mathcal{O}$. Como las curvas E_1 y E_2 son suaves, entonces por el teorema anterior se tiene que ϕ es un homomorfismo de grupos que está definido sobre todo E_1. Además ϕ es sobreyectiva sobre $\overline{\mathbb{K}}$, y podemos usar la isogenía restringiéndonos sobre el cuerpo $\mathbb{K}$. Por otro lado, dos curvas elípticas E_1 y E_2 son **isógenas** si existe una isogenía de E_1 a E_2 con $\phi(E_1) \neq \{\mathcal{O}\}$. Al conjunto de isogenías entre E_1 y E_2 se le denota $Hom(E_1, E_2)$. Si $E_1 = E_2 = E$, entonces $End(E) = Hom(E, E)$ será **el conjunto de endomorfismos de** E o de isogenías de E.

Ejemplo 3.2. Consideremos las curvas elípticas $E_1 : y^2 = x^3 + x + 1$ y $E_2 : y^2 = x^3 + x$ definidas sobre el cuerpo $\mathbb{F}_3$. Sea la aplicación $\phi : E_1 \to E_2$, definida por $\phi(x, y) = (x + 1, y)$, la cual claramente transforma la ecuación E_1 en la otra. Es más, respeta la operación de grupo. En efecto, la recta vertical $x = x_0$ es llevada por la aplicación ϕ en otra recta vertical de ecuación $x = x_0 + 1$. De igual manera, ϕ lleva la recta horizontal $y = y_0$ en sí misma. Finalmente la recta $y = mx + b$ es transformada por ϕ en la recta $y = mx - m + b$. Por lo tanto, la aplicación lleva rectas en rectas y por ello respeta la colinealidad de tres puntos, lo cual es equivalente a que se respete la operación de grupo. Tenemos $\mathcal{O}_{E_1} = \mathcal{O}_{E_2} = [0 : 1 : 0]$ y $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. Por lo tanto ϕ es una isogenía. Claramente esta es reversible.

Ejemplo 3.3. Sobre el cuerpo $\mathbb{F}_2$ definimos la curva elíptica $E : y^2 + xy = x^3 + x^2 + 1$. La aplicación $\phi : E \to E$, dada por $\phi(x, y) = (x, x + y)$, lleva una recta horizontal

$x = x_0$ en sí misma. La recta horizontal $y = y_0$ es llevada en la recta $y = x + y_0$. Por último la recta $y = mx + b$ es llevada en la recta $y = (1 + m)x + b$. Concluimos que ϕ respeta la operación de grupo al respetar la colinealidad. Tenemos $\mathcal{O}_{E_1} = \mathcal{O}_{E_2} = [0 : 1 : 0]$ y $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. Por lo tanto ϕ es una isogenía.

Ejemplo 3.4. Sea la curva elíptica $E : y^2 = x^3 + 1$ sobre el cuerpo $\overline{\mathbb{F}}_3$. La función $\phi : E \to E$ definida por $\phi(x, y) = (\sqrt[3]{y^2}, \sqrt{x^3 + 2})$ está bien definida, pues

$$\begin{aligned} (\sqrt{x^3+2})^2 &= x^3 + 2, \\ (\sqrt[3]{y^2})^3 + 1 &= x^3 + 2. \end{aligned}$$

Dada la recta L de ecuación $y = x + 2$, tomemos $(0, 2)$, $(-1 + \alpha, 1 + \alpha)$, $(-1 + 2\alpha, 1 + 2\alpha)$, con α solución de $t^2 = 2$, los cuales son precisamente los puntos de intersección de la recta con la curva elíptica. Notamos que se cumple $\phi(0, 2) = (1, \alpha)$, $\phi(-1 + \alpha, 1 + \alpha) = (\alpha, \sqrt{1 + 2\alpha})$, $\phi(-1 + 2\alpha, 1 + 2\alpha) = (2\alpha, \sqrt{1 + \alpha})$. La recta que pasa por los puntos $(1, \alpha)$ y $(\alpha, \sqrt{1 + 2\alpha})$ tiene ecuación $y = ((1 + \alpha)\sqrt{1 + 2\alpha} + 1 + 2\alpha)x + 2 + 2\alpha + 2(1 + \alpha)\sqrt{1 + 2\alpha}$. Si suponemos que $(2\alpha, \sqrt{1 + \alpha})$ pertenece a dicha recta, tenemos

$$\begin{aligned} \sqrt{1+\alpha} &= ((1+\alpha)\sqrt{1+2\alpha} + 1 + 2\alpha)2\alpha + 2 + 2\alpha + 2(1+\alpha)\sqrt{1+2\alpha}, \\ \sqrt{1+\alpha} &= \alpha\sqrt{1+2\alpha} + 1 + \alpha, \\ 0 &= 1 + 2\alpha + 2\alpha\sqrt{1+2\alpha}(1+\alpha), \\ 2 + 2\alpha &= \sqrt{1+2\alpha}(1+\alpha), \\ 1 + 2\alpha + \alpha^2 &= (1 + 2\alpha)(1 + 2\alpha + \alpha^2), \\ 1 + 2\alpha &= \alpha + 2\alpha^3, \\ 1 &= 0, \end{aligned}$$

lo cual es contradictorio. Por lo tanto, los puntos $(1, \alpha)$ y $(\alpha, \sqrt{1 + 2\alpha})$ y $(2\alpha, \sqrt{1 + \alpha})$ no son colineales y con ello ϕ no es un homomorfismo de grupos.

Dada una isogenía $\phi : E_1 \to E_2$, su **núcleo**, denotado por $Ker(\phi)$, es definido por $\{P \in E_1 : \phi(P) = \mathcal{O}\}$. Es importante saberlo calcular.

Ejemplo 3.5. Dada la curva elíptica $E : y^2 = x^3 + 3x^2 + 4x$ sobre el cuerpo $\mathbb{F}_{11}$, definimos $\phi : E \to E$ como $\phi(P) = 2P$. Los elementos de su núcleo satisfacen la ecuación $2P = \mathcal{O}$, lo cual es equivalente a $P = -P$. Si $P = (x, y)$, entonces se tiene $-P = (x', -y)$. Como $P = -P$, se tiene entonces $y = 0$. Por simple inspección, los elementos del núcleo de ϕ son $\{\mathcal{O}, (0, 0), (3, 0), (5, 0)\}$.

Ejemplo 3.6. Del ejemplo 3.2 tenemos que la función $\phi : E_1 \to E_2$ con $E_1 : y^2 = x^3 + x + 1$, $E_2 : y^2 = x^3 + x$ definida por $\phi(x, y) = (x + 1, y)$ es una isogenía. Los elementos de E_1 son $(0, 1), (0, 2), (1, 0)$ y al aplicar la isogenía tenemos $\phi(0, 1) = (1, 1), \phi(0, 2) = (1, 2), \phi(1, 0) = (2, 0)$. Luego, como estamos sobre el cuerpo $\mathbb{F}_3$, se tiene que el núcleo de ϕ solo tiene como elemento a $\mathcal{O}$.

Ejemplo 3.7. Sobre el cuerpo $\mathbb{F}_{17}$, sean las curvas elípticas $E_1 : y^2 = x^3 + 7x$, $E_2 : y^2 = x^3 + 6x$ y la isogenía $\phi : E_1 \to E_2$, definida por $\phi(x, y) = \left(\dfrac{y^2}{x^2}, \dfrac{y(7 - x^2)}{x^2}\right)$.

Los elementos de E_1 son $\{(0,0),(1,5),(1,12),(7,1),(7,16),(10,4),(10,13),(16,3),(16,14)\}$.

En particular hagamos los cálculos para obtener la imagen de $(0,0)$ mediante ϕ. Para ello observemos que se cumple

$$\phi(x,y)=\left(\frac{y^2}{x^2}:\frac{y(7-x^2)}{x^2}:1\right)=(y^2:y(7-x^2):x^2)=\left(y:7-x^2:\frac{x^2y}{y^2}\right).$$

Como $(x,y)\in E_1$, entonces $y^2=x(x^2+7)$ y se cumple

$$\phi(x,y)=\left(y:7-x^2:\frac{xy}{x^2+7}\right),$$

y al evaluar en el punto $(0,0)$ se tiene

$$\phi(0,0)=(0:7:0)=(0:1:0)=\mathcal{O}.$$

Tenemos que las imágenes mediante la isogenía ϕ de los elementos de E_1 son, en orden, $\{\mathcal{O},(8,13),(8,4),\ (8,13),(9,16),(9,1),(9,1),(9,16)\}$. Sin embargo, si los comparamos con los elementos de E_2, los cuales son $\{(0,0),(5,6),(5,11),\ (8,4),(8,13),(9,1),(9,16),(12,7),(12,10)\}$, observamos que ϕ no es sobreyectiva.

Ahora veamos un ejemplo de isogenía en la cual siempre que el cuerpo donde esté definida sea algebraicamente cerrado, resulta sobreyectiva.

Ejemplo 3.8. Dadas las curvas elípticas $E_1: y^2=x^3+3x$ y $E_2: y^2=x^3+2x$ sobre $\mathbb{F}_7$, consideremos la isogenía $\phi: E_1\to E_2$ definida por $\phi(x,y)=\left(\frac{y^2}{x^2},\frac{y(3-x^2)}{x^2}\right)$. Los elementos de E_1 son $\{(0,0),(1,2),(1,5),(2,0),(3,1),(3,6),(5,0)\}$

Nuevamente hagamos ciertos cálculos para obtener la imagen de $(0,0)$ mediante ϕ. Para ello observemos que se tiene

$$\phi(x,y)=\left(\frac{y^2}{x^2}:\frac{y(3-x^2)}{x^2}:1\right)=(y^2:y(3-x^2):x^2)=\left(y:3-x^2:\frac{x^2y}{y^2}\right).$$

Como $(x,y)\in E_1$, entonces $y^2=x(x^2+3)$ y se cumple

$$\phi(x,y)=\left(y:3-x^2:\frac{xy}{x^2+3}\right),$$

y al evaluar en el punto $(0,0)$ se tiene

$$\phi(0,0)=(0:3:0)=(0:1:0)=\mathcal{O}.$$

Tenemos que las imágenes vía la isogenía ϕ de los elementos de E_1 son, respectivamente, $\{\mathcal{O},(4,4),(4,3),(0,0),(4,4),(4,3),(0,0)\}$. Además los puntos de E_2 son $\{(0,0),(4,3),(4,4),(5,3),(5,4),(6,2),(6,5)\}$. Observamos que las preimágenes de los elementos de $(5,3)$, $(5,4)$, $(6,2)$ y $(6,5)$ no se encuentran sobre $\mathbb{F}_7$.

A continuación haremos unos cálculos para hallar las preimágenes faltantes: para ello necesitaremos trabajar sobre $\overline{\mathbb{F}}_7$, específicamente debemos considerar $\alpha\notin\mathbb{F}_7$ sujeto a $\alpha^2=5$.

Si $\phi(x,y)=(5,3)$, entonces $\dfrac{y^2}{x^2}=5$ e $\dfrac{y(3-x^2)}{x^2}=3$. Luego $0=y[(y+5)^2+2]$, por lo cual $(y+5)^2=5$. Si α es una solución de $z^2=5$, entonces $z=6\alpha$ es otra solución de dicha ecuación. Por lo tanto, se tendrá $y=2+\alpha$, $y=2+6\alpha$. Como se tiene $y^2=5x^2$, entonces $y=6\alpha x$ o $y=\alpha x$ lo cual es equivalente a $x=4\alpha y$ o $x=3\alpha y$. Con ello, los puntos $(6+\alpha,2+\alpha)$, $(1+\alpha,2+6\alpha)$, $(1+6\alpha,2+\alpha)$, $(6+6\alpha,2+6\alpha)$ satisfacen las ecuaciones $\dfrac{y^2}{x^2}=5$ e $\dfrac{y(3-x^2)}{x^2}=3$, de los cuales los puntos $(6+\alpha,2+\alpha)$ y $(6+6\alpha,2+6\alpha)$ pertenecen a E_1 sobre $\overline{\mathbb{F}}_7$. Por lo tanto las preimágenes de $(5,3)$ son $(6+\alpha,2+\alpha)$ y $(6+6\alpha,2+6\alpha)$.

Para $\phi(x,y)=(5,4)$ tenemos $\dfrac{y^2}{x^2}=5$, $\dfrac{y(3-x^2)}{x^2}=4$. Entonces de $0=y[(y+2)^2+2]$ se tiene $(y+2)^2=5$, de donde $y=5+\alpha$, $y=5+6\alpha$. Como $y^2=5x^2$, se tiene $y=6\alpha x$, $y=2\alpha x$, lo cual es equivalente a $x=4\alpha y$, $x=3\alpha y$, respectivamente. Con ello, los puntos $(6+6\alpha,5+\alpha)$, $(1+6\alpha,5+6\alpha)$, $(1+\alpha,5+\alpha)$, $(6+\alpha,5+6\alpha)$, satisfacen las ecuaciones $\dfrac{y^2}{x^2}=5$ e $\dfrac{y(3-x^2)}{x^2}=4$, donde sólo los puntos $(6+6\alpha,5+\alpha)$ y $(6+\alpha,5+6\alpha)$ pertenecen a E_1 sobre $\overline{\mathbb{F}}_7$. Por lo tanto las preimágenes de $(5,4)$ son $(6+6\alpha,5+\alpha)$ y $(6+\alpha,5+6\alpha)$

Si $\phi(x,y)=(6,2)$, entonces $\dfrac{y^2}{x^2}=6$ e $\dfrac{y(3-x^2)}{x^2}=2$. Luego $0=y[(y+1)^2+2]$, por lo cual $(y+1)^2=5$ y obtenemos $y=6+\alpha$, $y=6+6\alpha$. Como $y^2=6x^2$, entonces $y=5\alpha x$ o $y=2\alpha x$ lo cual es equivalente a $x=2\alpha y$ o $x=5\alpha y$. Con ello, los puntos $(3+5\alpha,6+\alpha)$, $(4+2\alpha,6+\alpha)$, $(4+5\alpha,6+6\alpha)$, $(3+2\alpha,6+6\alpha)$ satisfacen las ecuaciones $\dfrac{y^2}{x^2}=6$ e $\dfrac{y(3-x^2)}{x^2}=2$, de los cuales, los puntos $(3+5\alpha,6+\alpha)$ y $(3+2\alpha,6+6\alpha)$ pertenecen a E_1 sobre $\overline{\mathbb{F}}_7$. Por lo tanto las preimágenes de $(6,2)$ son $(3+5\alpha,6+\alpha)$ y $(3+2\alpha,6+6\alpha)$.

Para $\phi(x,y)=(6,5)$ tenemos $\dfrac{y^2}{x^2}=6$, $\dfrac{y(3-x^2)}{x^2}=5$. Entonces de $0=y[(y+6)^2+2]$ se tiene $(y+6)^2=5$, de donde $y=1+\alpha$, $y=1+6\alpha$. Como $y^2=6x^2$, se tiene $y=2\alpha x$, $y=5\alpha x$, lo cual es equivalente a $x=5\alpha y$, $x=2\alpha y$, respectivamente. Con ello, los puntos $(3+2\alpha,1+\alpha)$, $(4+2\alpha,1+6\alpha)$, $(4+5\alpha,1+\alpha)$, $(3+5\alpha,1+6\alpha)$, satisfacen las ecuaciones $\dfrac{y^2}{x^2}=6$ e $\dfrac{y(3-x^2)}{x^2}=5$, donde sólo los puntos $(3+2\alpha,1+\alpha)$ y $(3+5\alpha,1+6\alpha)$ pertenecen a E_1 sobre $\overline{\mathbb{F}}_7$. Por lo tanto las preimágenes de $(6,5)$ son $(3+2\alpha,1+\alpha)$ y $(3+5\alpha,1+6\alpha)$.

Sabemos del teorema 3.1 que la isogenía es sobreyectiva si el cuerpo base es cerrado. Es por ello que en nuestro ejemplo no hemos encontrado preimágenes de algunos puntos de E_2, pues solo estuvimos trabajando sobre $\mathbb{F}_7$ el cual no es algebraicamente cerrado.

3.1 Aspectos algebraicos de las isogenías

Sean las curvas elípticas E_1, E_2 sobre el espacio afín $\mathbb{A}^2_{\mathbb{K}}$. Por definición una isogenía $\phi : E_1 \to E_2$ queda expresada como

$$\phi(x,y) = \left(\frac{f_x(x,y)}{g_x(x,y)}, \frac{f_y(x,y)}{g_y(x,y)}\right),$$

donde f_x, f_y, g_x y g_y son polinomios. Además, por ser un homomorfismo de grupos, se debe satisfacer

$$\phi((x,y)+(x',y')) = \phi(x,y) + \phi(x',y').$$

De lo anterior tenemos que tanto el numerador como denominador de las componentes de la isogenía son polinomios en dos variables. Dichos polinomios los podemos expresar de una manera más cómoda. Para ello veamos algunos detalles.

Ejemplo 3.9. Consideremos la curva elíptica $E_1 : y^2 + y = x^3 + x + 1$ sobre el cuerpo $\mathbb{F}_2$, y la función polinomial $g(x,y) = x^4 + y^5 - xy^2 + x^3y^3$. Para $(x,y) \in E_1$, observemos que las potencias y^3, y^4, y^5 satisfacen

$$\begin{aligned} y^3 &= y(x^3+x+1-y) = x^3y + xy + y - y^2 = y(x^3+x) - (x^3+x+1), \\ y^4 &= y^2(x^3+x) - y(x^3+x+1) = -y + (x^3+x+1)(x^3+x), \\ y^5 &= (x^3+x+1)(x^3+x)y - y^2 = (x^6+x^3+x^2+x+1)y - (x^3+x+1). \end{aligned}$$

Debido a ello, los valores que toma el polinomio g sobre puntos de la curva elíptica E_1 se expresan como $g(x,y) = (x^4+x^3+x^2+1)y - x^6 - x^4 - x^2 - 1$.

Ejemplo 3.10. Consideremos la curva $E_2 : y^2 + xy = x^3 + x^2 + 1$, sobre el cuerpo $\mathbb{F}_2$, y el polinomio $g(x,y) = x^4 + y^4 - xy^3 + x^3y^2 + y$. Para $(x,y) \in E_2$, observemos que las potencias y^3, y^4 cumplen

$$\begin{aligned} y^3 &= y(x^3+x^2+1-xy) = y(x^3+x^2+1) - x(x^3+x^2+1), \\ y^4 &= y(y(x^3+x^2+1) - x(x^3+x^2+1)) = -(2x^4+2x)y + x^6 + 2x^4 + 2x^3 + 1. \end{aligned}$$

De este modo el polinomio g sobre puntos de la curva elíptica E_2 se reexpresa como $g(x,y) = (-x^4 - x^3 + 1)y + 2x^6 + 2x^5 + x^4 + x^2 + 1$.

Ejemplo 3.11. Sea la curva elíptica $E_3 : y^2 = x^3 + 2x + 1$, sobre el cuerpo $\mathbb{F}_3$, y el polinomio $g(x,y) = x^4y^6 - x + xy^2 + x^3y + y^5$. Para $(x,y) \in E_3$, observemos que las potencias y^3, y^4, y^5, y^6 cumplen

$$\begin{aligned} y^3 &= (x^3+2x+1)y, \\ y^4 &= (x^3+2x+1)^2, \\ y^5 &= (x^3+2x+1)^2y, \\ y^6 &= (x^3+2x+1)^3. \end{aligned}$$

El polinomio g sobre puntos de la curva elíptica E_3 cobra los mismos valores que $g(x,y) = (x^6+x^4+x^2+x+1)y + x^{13} + 2x^7 + 2x^4 + 2x^2$.

Virtud a los ejemplos recién vistos, observamos que para puntos sobre una curva elíptica las potencias de y se expresan en la forma $q(x) + yr(x)$, y con ello los polinomios definidos sobre curvas elípticas también se reducen acordemente. Ello lo precisamos en los siguientes lemas.

Proposición 3.12. *Sea $E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ una curva elíptica definida sobre un cuerpo $\mathbb{K}$. Si $(x, y) \in E$, entonces y^n, para $n \in \mathbb{N}$, se expresa como $p_n(x) + yq_n(x)$, para ciertos polinomios p_n, q_n.*

Prueba. Esto lo probaremos por inducción sobre la potencia de y. Si $n = 1$ tenemos $y = 0 + 1(y)$. Si suponemos válido el resultado para n, es decir $y^n = p(x) + q(x)y$, tendremos

$$\begin{aligned} y^{n+1} &= p(x)y + r(x)y^2, \\ &= p(x)y + q(x)(x^3 + a_2x^2 + a_4x + a_6 - a_1xy + a_4y), \\ &= (p(x) - a_1xq(x) + a_4q(x))y + q(x)(x^3 + a_4x + a_6). \end{aligned}$$

Por lo tanto, para cada $n \in \mathbb{N}$, la potencia y^n se expresa como $p_n(x) + q_n(x)y$. □

Corolario 3.13. *Sea la curva elíptica $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Si $r(x, y)$ es una función regular (polinomial) definida sobre la curva elíptica E, entonces existen polinomios p, $q \in \mathbb{K}[x]$ tales que $r(x, y) = p(x) + q(x)y$.*

Prueba. Por la proposición anterior, para cada $k \in \mathbb{N}$ existen polinomios p_k y q_k de variable x tales que $y^k = p_k(x) + q_k(x)y$. Tenemos entonces $r(x, y) = \sum_{j,k} x^j y^k = \sum_{j,k} x^j p_k + \sum_{j,k} x^j q_k y$. Con $p(x) = \sum_{j,k} x^j p_k(x)$, $q(x) = \sum_{j,k} x^j q_k(x)$ aterrizamos en $r(x, y) = p(x) + q(x)y$. □

Lema 3.14. *Si una función racional $R(x, y)$ está definida sobre la curva elíptica $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, entonces existen polinomios $f(x)$, $g(x)$ y $h(x)$ con los cuales se tiene $R(x, y) = \dfrac{f(x) + g(x)y}{h(x)}$ sobre E.*

Prueba. Como $R(x, y)$ es una función racional, existen polinomios $r_1(x, y)$, $r_2(x, y) \in \mathbb{K}[x, y]$ tales que $R(x, y) = \dfrac{r_1(x, y)}{r_2(x, y)}$. Por el corolario 3.13, para los polinomios $r_1(x, y)$ y $r_2(x, y)$, existen p_1, p_2, q_1, $q_2 \in \mathbb{K}[x]$ que cumplen $r_1(x, y) = p_1(x) + q_1(x)y$ y $r_2(x, y) = p_2(x) + q_2(x)y$. Luego se obtiene $R(x, y) = \dfrac{p_1(x) + q_1(x)y}{p_2(x) + q_2(x)y}$. Si al denominador lo multiplicamos por el factor $p_2(x) - (y + a_1x + a_3)q_2(x)$ se consigue

$$\begin{aligned} &(p_2(x) + q_2(x)y)(p_2(x) - (y + a_1x + a_3)q_2(x)) \\ &\quad = (p_2(x))^2 - (y^2 + a_1xy + a_3y)(q_2(x))^2 - (a_1x + a_3)p_2(x)q_2(x) \\ &\quad = (p_2(x))^2 - (x^3 + a_2x^2 + a_4x + a_6)(q_2(x))^2 - (a_1x + a_3)p_2(x)q_2(x) \\ &\quad = h(x). \end{aligned}$$

Con ello trivialmente llegamos a la expresión deseada. □

Sean las curvas elípticas E y E' y consideremos la isogenía $\phi : E \mapsto E'$ dada por $\phi(x, y) = (R_1(x, y), R_2(x, y))$ donde $R_1,\ R_2$ son racionales en las variables x e y. El lema 3.14 nos permite simplificar esta expresión significativamente.

Lema 3.15. *Sean las curvas elípticas* $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ *y* $E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$. *Una isogenía* $\phi : E \mapsto E'$ *dada por* $\phi(x, y) = (R_1(x, y), R_2(x, y))$ *satisface* $R_1(x, y) = r_1(x)$, *donde* r_1 *es una función racional.*

Prueba. Sabemos que toda isogenía es un homomorfismo y por ello satisface $\phi(-P) = -\phi(P)$. Recordemos que la negación de un punto $(x, y) \in E$ es de la forma $-(x, y) = (x, -y - a_1x - a_3)$. Pero de la igualdad $\phi(x, y) = (R_1(x, y), R_2(x, y))$ se pasa a

$$\begin{aligned} \phi(-P) &= \phi(x, -y - a_1x - a_3) && (3.1)\\ &= (R_1(x, -y - a_1x - a_3), R_2(x, -y - a_1x - a_3)). && (3.2) \end{aligned}$$

Por otro lado, se satisface

$$\begin{aligned} -\phi(P) &= -(R_1(x, y), R_2(x, y)) && (3.3)\\ &= (R_1(x, y), -R_2(x, y) - a'_1R_1(x, y) - a'_3). && (3.4) \end{aligned}$$

Gracias al lema 3.14, tenemos $R_1(x, y) = \dfrac{f_1(x) + g_1(x)y}{h_1(x)}$. De las expresiones (3.2) y (3.4) se obtiene

$$\frac{f_1(x) + g_1(x)y}{h_1(x)} = \frac{f_1(x) - (y + a_1x + a_3)g_1(x)}{h_1(x)},$$

de donde se logra la igualdad $\dfrac{(2y + a_1x + a_3)g_1(x)}{h_1(x)} = 0$. De esto se sigue que $g_1(x)$ es nulo y se concluye $R_1(x, y) = r_1(x)$. □

Hasta ahora hemos visto que las isogenías definidas sobre curvas elípticas en cuerpos de cualquier característica toman la forma

$$\phi(x, y) = \left(\frac{f_1(x)}{h_1(x)}, \frac{f_2(x) + g_2(x)y}{h_2(x)}\right),$$

donde $f_1,\ f_2,\ g_2,\ h_2$ son polinomios en la variable x. Es decir, en su forma general, para la primera componente de la isogenía no influye la característica del cuerpo.

Observación 3.16. La presentación $R_2(x, y) = \dfrac{f_2(x) + g_2(x)y}{h_2(x)}$ del lema 3.15 combinada con las ecuaciones 3.2 y 3.4 deviene en

$$\begin{aligned} R_2(x, -y - a_1x - a_3) &= -R_2(x, y) - a'_1R_1(x, y) - a'_3,\\ \frac{f_2(x) - (y + a_1x + a_3)g_2(x)}{h_2(x)} &= -\frac{f_2(x) + g_2(x)y}{h_2(x)} - (a'_1r_1(x) + a'_3),\\ f_2(x) - (y + a_1x + a_3)g_2(x)h_2(x) &= -f_2(x) - g_2(x)y - (a'_1r_1(x) + a'_3)h_2(x),\\ 2f_2(x) &= (a_1x + a_3)g_2(x) - (a'_1r_1(x) + a'_3)h_2(x), \end{aligned}$$

donde la igualdad $2f_2(x) = (a_1x + a_3)g_2(x) - (a'_1r_1(x) + a'_3)h_2(x)$ se satisface en cualquier característica del cuerpo base.

En el caso que el cuerpo $\mathbb{K}$ sea de característica distinta de 2, tenemos el siguiente lema.

Lema 3.17. *Sean las curvas elípticas* $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $E' : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$ *y consideremos la isogenía* $\phi : E \mapsto E'$ *definida por* $\phi(x, y) = (r_1(x), R_2(x, y))$. *Si la característica del cuerpo* $\mathbb{K}$ *es distinta de 2, entonces se tiene*

$$R_2(x, y) = \left(y + \frac{a_1x + a_3}{2}\right) r_2(x) - \frac{a'_1r_1(x) + a'_3}{2}.$$

Prueba. De la observación 3.16 se cumple

$$2f_2(x) \;=\; (a_1x + a_3)g_2(x) - (a'_1r_1(x) + a'_3)h_2(x).$$

Al aprovechar que la característica del cuerpo es distinta de 2 obtenemos

$$\frac{f_2(x)}{h_2(x)} = \frac{(a_1x + a_3)g_2(x)}{2h_2(x)} - \frac{a'_1r_1(x) + a'_3}{2}.$$

La anterior expresión la reemplazamos en R_2 para obtener

$$R_2(x, y) = \left(y + \frac{a_1x + a_3}{2}\right) r_2(x) - \frac{a'_1r_1(x) + a'_3}{2}.$$

□

Corolario 3.18. *Sean* E_1 *y* E_2 *curvas elípticas sobre el cuerpo* $\mathbb{K}$, *de característica distinta de 2, cuyas ecuaciones son* $E_1 : y^2 = x^3 + a_2x^2 + a_4x + a_6 = f(x)$ *y* $E_2 : y^2 = x^3 + a'_2x^2 + a'_4x + a'_6$. *Sea* $\phi : E_1 \to E_2$ *una isogenía sobre* $\mathbb{K}$. *Entonces* ϕ *queda definida por una función racional de la forma*

$$\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right),$$

donde u, v, s, t *son polinomios en* x. *Por supuesto,* u *y* v *pueden tomarse coprimos al igual que* s *y* t. *Además* v^3 *y* t^2 *dividen a* t^2 *y* v^3f *respectivamente.*

Prueba. Al notar que se tiene $a_1 = a_3 = a'_1 = a'_3 = 0$, el lema 3.17 indica que la isogenía toma la forma $\phi(x, y) = (r_1(x), yr_2(x))$, con $r_1(x)$ y $r_2(x)$ funciones racionales. Es claro además que la isogenía se convierte en $\phi(x, y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right)$ con u, v y s, t parejas de polinomios coprimos.

De $\phi(x, y) \in E_2$ se pasa a

$$\left(\frac{s(x)y}{t(x)}\right)^2 \;=\; \left(\frac{u(x)}{v(x)}\right)^3 + a'_2\left(\frac{u(x)}{v(x)}\right)^2 + a'_4\left(\frac{u(x)}{v(x)}\right) + a'_6, \tag{3.5}$$

$$v^3(x)s^2(x)f(x) \;=\; (u^3(x) + a'_2u^2(x)v(x) + a'_4u(x)v^2(x) + a'_6v^3(x))t^2, \tag{3.6}$$

donde $f(x) = x^3 + a_2x^2 + a_4x + a_6$. Al ser $u(x)$ y $v(x)$ coprimos, se tiene que $v^3(x)$ no puede dividir a $w(x) = u^3(x) + a'_2u^2(x)v(x) + a'_4u(x)v^2(x) + a'_6v^3(x)$ y por ello se cumple que $v^3(x)$ divide a $t^2(x)$. Por otro lado, $t(x)$ y $s(x)$ son coprimos con lo cual $t^2(x)$ divide a $v^3(x)f(x)$. □

3.2 Isogenías duales

Sabemos del lema 3.15 que una isogenía $\phi : E_1 \to E_2$, donde E_1 y E_2 son curvas elípticas, se expresa como $\phi(x,y) = \left(\dfrac{f_1(x)}{h_1(x)}, \dfrac{f_2(x)+g_2(x)y}{h_2(x)}\right)$, donde f_1, f_2, g_2, h_2 son polinomios en la variable x. A partir de ello podemos definir lo que es el **grado de la isogenía ϕ**, lo cual denotaremos por $\boldsymbol{deg(\phi)}$, y se calculará como

$$deg(\phi) = max\{deg(f_1(x)), deg(h_1(x))\}.$$

Observamos que el grado de cada isogenía dada en los ejemplos 3.7 y 3.8 son iguales a 2.

Veamos el siguiente teorema cuya demostración se puede encontrar en [15].

Teorema 3.19. *Si $\phi : E_1 \to E_2$ es una isogenía, con E_1 y E_2 curvas elípticas, de grado m entonces existe una única isogenía $\psi : E_2 \to E_1$ tal que $(\psi \circ \phi)(P) = mP$ y además $(\phi \circ \psi)(Q) = mQ$.*

Del teorema anterior, a la isogenía ψ se le denomina **isogenía dual** de grado m.

En nuestro caso veremos las isogenías duales de grado 2 la cual será importante para la demostración del teorema de Mordell-Weil que se verá en la sección 3.3.

A continuación, sobre un cuerpo $\mathbb{K}$ de característica distinta de 2, consideremos las curvas elípticas $E_1 : y^2 = x^3 + ax^2 + bx$, $E_1^* : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$ y definemos la isogenía $\phi : E_1 \to E_1^*$ como $\phi(x,y) = \left(\dfrac{y^2}{x^2}, \dfrac{y(b-x^2)}{x^2}\right)$.

Si $E_1 : y^2 = x^3 + ax^2 + bx$ es curva elíptica, tenemos $b \neq 0$ y $b' = a^2 - 4b \neq 0$ pues el discriminante vale $\tau(E_1) = 16b^2(a^2 - 4b) \neq 0$. Bajo estas condiciones, también es elíptica la curva

$$E_1^* : y^2 = x^3 - 2ax^2 + b'x,$$

pues su discriminante vale $\tau(E_1^*) = 16(b')^2(4a^2 - 4b') = 16(b')^2(16)b \neq 0$.

Como ya se dijo, definimos $\phi : E_1 \to E_1^*$ como

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

para $(x,y) \neq (0,0)$ y $\phi(0,0) = \phi(\mathcal{O}) = \mathcal{O}$. Veremos que ϕ está bien definida, es decir, para puntos en E_1 la imagen cae en E_1^*.

Primero notemos que se tiene $(0,0) \in E_1$ y $\phi(0,0) = \phi(\mathcal{O}) = \mathcal{O} \in E_1^*$.

Para $(x,y) \in E_1$, con $x \neq 0$, se tiene $y \neq 0$. Probemos que se cumple

$$\frac{y^2(b-x^2)^2}{x^4} = \frac{y^6}{x^6} - 2a\frac{y^4}{x^4} + (a^2 - 4b)\frac{y^2}{x^2},$$

es decir $\phi(x,y) \in E_1^*$. Si multiplicamos por x^6 y dividimos por y^2, la anterior expresión resulta equivalente a

$$b^2x^2 - 2bx^4 + x^6 = y^4 - 2ax^2y^2 + (a^2 - 4b)x^4.$$

Como $(x,y) \in E_1$, reemplazamos $y^2 = x^3 + ax^2 + bx$ e $y^4 = (y^2)^2$ en el lado derecho para confirmar la igualdad deseada.

Veamos ahora que la función ϕ lleva tres puntos colineales de E_1 en tres puntos colineales en E_1^*.

Si tomamos la recta vertical $x = x_0$, entonces se tiene

$$\phi(x_0, y) = \left(\frac{x_0^3 + ax_0^2 + bx_0}{x_0^2}, \frac{y(b - x_0^2)}{x_0^2} \right),$$

con lo cual puntos en la recta $x = x_0$ son llevados en puntos en la recta vertical $x = \dfrac{x_0^3 + ax_0^2 + bx_0}{x_0^2}$; por supuesto $\mathcal{O}$ es llevado en $\mathcal{O}$.

Para la recta $y = 0$ tenemos $\phi(x, 0) = (0, 0)$, cuando $x \neq 0$, y esto significa que la imagen de dicha recta vía ϕ intercepta a E_1^* en el único punto $(0, 0)$. Ahora, para la recta $y = y_0$, con $y_0 \neq 0$, se tiene

$$\phi(x, y_0) = \left(\frac{y_0^2}{x^2}, \frac{by_0}{x^2} - y_0 \right).$$

Al calcular el valor de la pendiente de la recta $L : y = mx + \gamma$ que pasa por $\phi(x_1, y_0)$ y $\phi(x_2, y_0)$, obtenemos

$$m = \frac{\dfrac{by_0}{x_2^2} - y_0 - \dfrac{by_0}{x_1^2} + y_0}{\dfrac{y_0^2}{x_2^2} - \dfrac{y_0^2}{x_1^2}} = \frac{by_0(x_1^2 - x_2^2)}{y_0^2(x_1^2 - x_2^2)} = \frac{b}{y_0}.$$

Y como $\phi(x_2, y_0)$ es un punto de paso, se consigue

$$\gamma \;=\; \frac{by_0}{x_2^2} - y_0 - \frac{b}{y_0}\left(\frac{y_0^2}{x_2^2}\right) = -y_0.$$

Por lo tanto, puntos en esta recta horizontal son llevados por ϕ en puntos en la recta $y = \dfrac{b}{y_0}x - y_0$, la cual depende únicamente de y_0.

Para puntos en la recta $y = mx$, se tiene

$$\phi(x, mx) = \left(m^2, \frac{m(b - x^2)}{x} \right),$$

es decir puntos en $y = mx$ distintos de $(0, 0)$ son llevados mediante ϕ en puntos en la recta vertical $x = m^2$. El tercer punto en discordia es $(0, 0)$ que es llevado en $\mathcal{O}$, el tercer punto de la vertical $x = m^2$ en E_1^*.

Ahora consideremos una recta $y = mx + c$ que no pase por el origen. Si los puntos (x_1, y_1) y (x_2, y_2) pertenecen simultáneamente a la recta y a la curva, tenemos

$$\phi(x_1, y_1) = \left(\frac{y_1^2}{x_1^2}, \frac{y_1(b - x_1^2)}{x_1^2} \right) \text{ y } \; \phi(x_2, y_2) = \left(\frac{y_2^2}{x_2^2}, \frac{y_2(b - x_2^2)}{x_2^2} \right).$$

Además, la pendiente que pasa por los puntos $\phi(x_1, y_1)$ y $\phi(x_2, y_2)$ es

$$\frac{mbx_1x_2 + bc(x_1 + x_2) + x_1^2x_2^2m}{c(2mx_1x_2 + cx_1 + cx_2)}.$$

A continuación intersecamos la recta $y = mx + c$ con la curva elíptica, para obtener la ecuación $0 = x^3 + (a - m^2)x^2 + (b - 2mc)x - c^2$, de lo cual resulta

$$\begin{aligned} x_1 + x_2 + x_3 &= m^2 - a, && (3.7)\\ x_1x_2 + x_1x_3 + x_2x_3 &= b - 2mc, && (3.8)\\ x_1x_2x_3 &= c^2. && (3.9) \end{aligned}$$

También tenemos que la pendiente que atraviesa los puntos $\phi(x_1, y_1)$ y $\phi(x_3, y_3)$ es

$$\frac{mbx_1x_3 + bc(x_1 + x_3) + x_1^2x_3^2m}{c(2mx_1x_3 + cx_1 + cx_3)}.$$

Para que $\phi(x_1, y_1)$, $\phi(x_2, y_2)$ y $\phi(x_3, y_3)$ caigan en una misma recta, se tiene que cumplir que sus pendientes sean iguales, es decir deben quedar sujetos a

$$\frac{mbx_1x_2 + bc(x_1 + x_2) + x_1^2x_2^2m}{c(2mx_1x_2 + cx_1 + cx_2)} = \frac{mbx_1x_3 + bc(x_1 + x_3) + x_1^2x_3^2m}{c(2mx_1x_3 + cx_1 + cx_3)},$$

lo cual es equivalente a la igualdad

$$-bc + 2mx_1x_2x_3 + c(x_1x_2 + x_1x_3 + x_2x_3) = 0,$$

válida por las ecuaciones (3.8) y (3.9). En resumen, la función ϕ lleva tres puntos colineales en tres puntos colineales y ello deriva en que ϕ respete la operación de grupo.

De manera similar E_1^* tiene una curva dual $E_1^{**} : y^2 = x^3 + 4ax^2 + 16bx$ y una correspondiente isogenía $\phi^* : E_1^* \to E_1^{**}$. Sin embargo, la curva elíptica E_1^{**} es isomorfa a E_1 mediante el cambio lineal $(x', y') = l(x, y) = \left(\frac{x}{4}, \frac{y}{8}\right)$ y podemos prestarle más atención a la composición $\psi(x, y) = l(\phi^*(x, y)) = \left(\frac{y^2}{4x^2}, \frac{y(b' - x^2)}{8x^2}\right)$, la cual es evidentemente también una isogenía.

En el siguiente lema veremos que ϕ y ψ, satisfacen $(\phi \circ \psi)(P) = 2P$.

Lema 3.20. *Dadas las curvas elípticas $E_1 : y^2 = x^3 + ax^2 + bx$, $E_1^* : y^2 = x^3 - 2ax^2 + (a^2 - 4b)$ y las isogenías $\phi : E_1 \to E_1^*$, $\psi : E_1^* \to E_1$ definidas como $\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2}\right)$ y $\psi(x, y) = \left(\frac{y^2}{4x^2}, \frac{y(a^2 - 4b - x^2)}{8x^2}\right)$, se tiene $(\phi \circ \psi)(P) = 2P$.*

Prueba. En primer lugar tenemos

$$(\phi \circ \psi)(x, y) = \left(\frac{(a^2 - 4b - x^2)^2}{4y^2}, \frac{(a^2 - 4b - x^2)(16bx^4 - y^4)}{8x^2y^3}\right).$$

Ahora determinemos la duplicación de un punto $P = (x, y)$, denotada por $2P = (x_3, y_3)$, para compararla con la expresión anterior. Para ello tomemos la recta

$L : y = mx + b$, usada para hallar $P * P = (x_3, y_3')$. De lo trabajado en el capítulo 2 tenemos

$$\begin{aligned} m &= \frac{3x^2 - 4ax + a^2 - 4b}{2y}, \\ b &= \frac{-x^3 + (a^2 - 4b)x}{2y} = \frac{x(a^2 - 4b - x^2)}{2y}, \\ x_3 &= m^2 + 2a - 2x = \frac{(x^2 + 4b - a^2)^2}{4y^2}, \\ y_3' &= mx_3 + b = \frac{(16bx^4 - y^4)(a^2 - 4b - x^2)}{-8x^2y^3}, \\ y_3 &= -y_3' = \frac{(16bx^4 - y^4)(a^2 - 4b - x^2)}{8x^2y^3}. \end{aligned}$$

Además, para $x \neq 0$, tenemos $\psi(\phi(x,0)) = \psi(0,0) = \mathcal{O}$ y $\phi(\psi(x,0)) = \phi(0,0) = \mathcal{O}$. Por otro lado se cumple $\psi(\phi(0,0)) = \psi(\mathcal{O}) = \mathcal{O}$ y $\phi(\psi(x,0)) = \phi(\mathcal{O}) = \mathcal{O}$. Obviamente estos cálculos establecen la igualdad $(\phi \circ \psi)(P) = 2P$. □

3.3 Algunos aspectos aritméticos

Para esta sección nos basaremos en [13]. Usaremos a las isogenías y el lema 3.17 para probar que el índice $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ es finito. Esto último es muy importante para concluir que el grupo $E(\mathbb{Q})$ es finito.

En el siguiente lema, encontraremos información sobre la abscisa de los puntos racionales de la curva elíptica $E_1 : y^2 = x^3 + ax^2 + bx$.

Lema 3.21. *Consideremos la curva elíptica $E_1 : y^2 = x^3 + ax^2 + bx$, con $a, b \in \mathbb{Z}$. Sea el punto $(x, y) \in E_1(\mathbb{Q})$, con $x \neq 0$. Entonces x es congruente a $\pm \prod_{i=1}^{\kappa} p_i^{g_i}$ en el grupo cociente $\mathbb{Q}^*/(\mathbb{Q}^*)^2$; acá $p_1, \ldots, p_\kappa$ son los factores primos de b.*

Prueba. Para $(x, y) \in E_1(\mathbb{Q})$ ponemos $(x, y) = \left(\frac{m}{q}, \frac{n}{t}\right)$, con $\text{mcd}(m, q) = \text{mcd}(n, t) = 1$. Por definición tenemos entonces

$$\frac{n^2}{t^2} = \frac{m^3}{q^3} + a\frac{m^2}{q^2} + b\frac{m}{q},$$

o lo que es lo mismo

$$q^3n^2 = t^2m(m^2 + amq + bq^2).$$

Observamos que se tiene $m|n^2$ y $t^2|q^3$. Además se cumple $q^3|t^2$ pues de lo contrario q y m^2 compartirían un divisor, lo cual es absurdo excepto si $q = 1$. Se deduce así $t^2 = q^3$ salvo quizás por el signo. Por otro lado se tiene $q|t$ pues si tomamos la descomposición prima de q, digamos $q = m_1^{\alpha_1} \ldots m_s^{\alpha_s}$, se satisface $t^2 = q^3 = m_1^{3\alpha_1} \ldots m_s^{3\alpha_s}$ y con ello deducimos que α_i es par, digamos $\alpha_i = 2\beta_i$. De $t^2 = m_1^{6\beta_1} \ldots m_s^{6\beta_s}$, obtenemos $t = m_1^{3\beta_1} \ldots m_s^{3\beta_s}$ para concluir $q|t$. Como $q|t$, es decir

$t = qz$, se tiene $t^3 = q^3z^3 = t^2z^3$, y con ello $t = z^3$. Adicionalmente, $q^3 = t^2 = q^2z^2$ implica $q = z^2$. Por lo tanto, un punto racional de la curva elíptica $E_1 : y^2 = x^3 + ax^2 + bx$ es siempre de la forma $\left(\frac{m}{z^2}, \frac{n}{z^3}\right)$, con $\text{mcd}(m, z) = \text{mcd}(n, z) = 1$.

Todo punto racional de la curva elípica $E : y^2 = x^3 + ax^2 + bx$ de la forma $\left(\frac{m}{z^2}, \frac{n}{z^3}\right)$, con $\text{mcd}(m, z) = \text{mcd}(n, z) = 1$, al ser reemplazado en la ecuación $y^2 = x^3 + ax^2 + bx$ obedece

$$\left(\frac{n}{z^3}\right)^2 = \left(\frac{m}{z^2}\right)^3 + a\left(\frac{m}{z^2}\right)^2 + b\left(\frac{m}{z^2}\right),$$

es decir se tiene

$$n^2 = m^3 + am^2z^2 + bmz^4 = m(m^2 + amz^2 + bz^4).$$

Si $d = \text{mcd}(m, n)$, entonces $m = dm_1$ y $n = dn_1$, con $\text{mcd}(m_1, n_1) = 1$. Al reemplazarlo en la ecuación anterior se obtiene

$$\begin{aligned} d^2n_1^2 &= dm_1(m^2 + amz^2 + bz^4), \\ dn_1^2 &= m_1(d^2m_1^2 + adm_1z^2 + bz^4). \end{aligned}$$

Obtenemos $m_1|d$, es decir, $d = m_1d_1$. Si esto lo sustituimos conseguimos

$$\begin{aligned} m_1d_1n_1^2 &= m_1(m_1^4d_1^2 + am_1^2d_1z^2 + bz^4), \\ d_1n_1^2 &= m_1^4d_1^2 + am_1^2d_1z^2 + bz^4, \end{aligned}$$

con lo cual $d_1|bz^4$, y como $\text{mcd}(m, z) = 1$, se desprende $d_1|b$. Si $b = \pm\prod_{i=1}^{\kappa} p_i^{\beta_i}$, con $\beta_i \in \mathbb{N}$ y p_i primos, entonces $d_1 = \pm\prod_{i=1}^{\kappa} p_i^{\gamma_i}$, con $\gamma_i \in \mathbb{N}$, donde los $\gamma_i \in \mathbb{Z}$ satisfacen $0 \leq \gamma_i \leq \beta_i$. Los exponentes γ_i se pueden expresar como $\gamma_i = 2f_i + g_i$, donde $g_i \in \{0, 1\}$. Con ello logramos $d_1 = \pm\left(\prod_{i=1}^{\kappa} p_i^{f_i}\right)^2 \prod_{i=1}^{\kappa} p_i^{g_i}$, de donde se pasa a $\frac{m}{z^2} = \frac{dm_1}{z^2} = \frac{d_1m_1^2}{z^2} = \pm\left(m_1\frac{\prod_{i=1}^{\kappa} p_i^{f_i}}{z}\right)^2 \prod_{i=1}^{\kappa} p_i^{g_i}$. Si consideramos el grupo $(\mathbb{Q}^*)^2$ y el cociente $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, deducimos que $\frac{m}{z^2}$ es congruente a $\pm\prod_{i=1}^{\kappa} p_i^{g_i}$. □

Utilizaremos el lema anterior para encontrar puntos de coordenadas enteras de una curva elíptica en el siguiente ejemplo.

Ejemplo 3.22. En la curva elíptica $E : y^2 = x^3 + 189x^2 + 2310x$ busquemos algunos puntos de coordenadas enteras. Por ejemplo, podemos identificar rápidamente a $(0, 0)$ como uno de ellos. Veamos a continuación si hay otros.

Sea (m, n) un punto de coordenadas enteras con $m \neq 0$. Como vimos antes, pongamos $d = \text{mcd}(m, n)$ (cantidad no nula), de modo que se tenga $m = dm_1$ y $n = dn_1$ con $\text{mcd}(m_1, n_1) = 1$. Al reemplazar en la ecuación de E obtenemos

$$d^2n_1^2 = d^3m_1^3 + 189d^2m_1^2 + 2310dm_1,$$

de donde se logra

$$dn_1^2 = m_1(d^2m_1^2 + 189dm_1 + 2310).$$

Como m_1 y n_1 son relativamente primos resulta que m_1 dividirá a d: por ejemplo $d = d_1 m_1$.

Esto puede ser reemplazado en nuestro despliegue del párrafo anterior para obtener

$$d_1 n_1^2 = d_1^2 m_1^4 + 189 d_1 m_1^2 + 2310.$$

Concluimos que d_1 será un divisor de 2310. (En resumen, un punto entero en E tendrá obligado la forma $(d_1 m_1^2, d_1 m_1 n_1)$, con d_1 divisor de 2310.)

Veamos si podemos encontrar algo con $d_1 = 1$. Si multiplicamos por 4 y agrupamos obtenemos

$$4n_1^2 = (2m_1^2 + 189)^2 - 35721 + 9240,$$

de donde se pasa a

$$26481 = (2m_1^2 + 189)^2 - 4n_1^2 = (2m_1^2 + 2n_1 + 189)(2m_1^2 - 2n_1 + 189).$$

De este modo, el problema se reduce a escrutar factorizaciones enteras tipo $pq = 26481$. Es más, como n_1 siempre puede asumirse positivo, solo nos interesan factores positivos sujetos a $p \geq q$. El listado con el correspondiente análisis está dado a continuación. (La factorización de 26481 es $3 \cdot 7 \cdot 13 \cdot 97$.)

q	p	$2m_1^2 + 189$	$2n_1$	m_1	n_1
1	26481	13241	13240	no es entero	
3	8827	4415	4412	no es entero	
7	3783	1895	1888	no es entero	
13	2037	1025	1012	no es entero	
21	1261	641	620	no es entero	
39	679	359	320	no es entero	
91	291	191	100	1	50
97	273	185	88	no es real	

Figura 3.1: Tabla de factorizaciones enteras y consecuencias

Nuestra primera meta es probar el siguiente teorema.

Teorema 3.23. *Para la curva elíptica $E_1 : y^2 = x^3 + ax^2 + bx$ con $a, b \in \mathbb{Z}$, se satisface que el índice $[E_1(\mathbb{Q}) : 2E_1(\mathbb{Q})]$ es finito.*

El teorema anterior lo probaremos en varias partes. En primer lugar, probaremos que la proyección sobre las abscisas de los puntos racionales de la curva elíptica $E_1 : y^2 = x^3 + ax^2 + bx$ es un homomorfismo. Recordemos que del trabajo efectuado párrafos atrás derivamos información sobre la abscisa del punto de la curva elíptica, lo cual aprovecharemos para la prueba del siguiente lema.

Lema 3.24. *Para la curva elíptica $E_1 : y^2 = x^3 + ax^2 + bx$, definamos $w : E_1 \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ como*

$$w(P) = \begin{cases} 1 \ (mod\ (\mathbb{Q}^*)^2) & si \quad P = \mathcal{O}, \\ b \ (mod\ (\mathbb{Q}^*)^2) & si \quad P = T = (0,0), \\ x \ (mod\ (\mathbb{Q}^*)^2) & si \quad P = (x,y) \ con \ x \neq 0. \end{cases}$$

Resulta que w es un homomorfismo de grupos.

Prueba. La función w está bien definida, pues al tener la curva elíptica E_1 discriminante $\tau = b^2(a^2 - 4b)$ no nulo se obtiene $b \neq 0$.

Ahora probemos que w respeta la operación de grupo. Sean los puntos racionales (x_1, y_1), (x_2, y_2) de la curva elíptica E_1. Consideremos la recta L que pasa por dichos puntos, de ecuación $y = qx + r$, donde $q, r \in \mathbb{Q}$. Si $r = 0$, entonces al interceptar la recta con la curva elíptica se tiene $x(x^2 + (a - q^2)x + b) = 0$, obteniéndose las raíces x_1, x_2 y x_3; notemos que uno de dichos valores es 0. Si tomamos $x_3 = 0$, se tiene $(x_3, y_3) = T$ y con ello $w(T) = b$ y $x_1x_2 = b$, es decir se cumple $w(x_1, y_1)w(x_2, y_2)w(x_3, y_3) = b^2 \equiv 1$. Por lo tanto ϕ respeta la colinealidad y por ende la operación de grupo.

Si la recta no pasa por el origen, es decir si $r \neq 0$, la intersección de la recta con la curva E_1 satisface

$$\begin{aligned} (qx + r)^2 &= x^3 + ax^2 + bx, \\ q^2x^2 + 2qrx + r^2 &= x^3 + ax^2 + bx, \\ 0 &= x^3 + (a - q^2)x^2 + (b - 2qr)x - r^2. \end{aligned}$$

Si x_3 es la abscisa del punto de intersección de la recta L con la curva E_1, entonces tendremos $x_1x_2x_3 = r^2 \equiv 1$. Es decir, si los tres puntos (x_1, y_1), (x_2, y_2), (x_3, y_3) son colineales, se respeta la operación de grupo. □

De la sección 3.2, tenemos que el dual de la curva elíptica $E_1 : y^2 = x^3 + ax^2 + bx$ es la curva elíptica $E_1^* : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Además el lema 3.17 nos dice que las isogenías $\phi : E_1 \to E_1^*$ y $\psi : E_1^* \to E_1$, definidas por $\psi(x, y) = \left(\dfrac{y^2}{x^2}, \dfrac{y(b - x^2)}{x^2}\right)$ y $\psi(x, y) = \left(\dfrac{y^2}{4x^2}, \dfrac{y(a^2 - 4b - x^2)}{8x^2}\right)$ respectivamente, satisfacen $(\phi \circ \psi)(P) = 2P$. En el siguiente lema vamos a establecer una relación entre $Ker(w)$ y $Im(\psi)$.

Lema 3.25. *Sea la curva elíptica $E_1 : y^2 = x^3 + ax^2 + bx$ y su dual $E_1^* : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Se cumple $Ker(w) = Im(\psi)$, donde $\psi : E_1^* \to E_1$ es definida por $\psi(x, y) = \left(\dfrac{y^2}{4x^2}, \dfrac{y(a^2 - 4b - x^2)}{8x^2}\right)$ si $(x, y) \neq (0, 0), \mathcal{O}$, y $\psi(0, 0) = \psi(\mathcal{O}) = \mathcal{O}$.*

Prueba. De la definición de ψ observamos automáticamente la inclusión $Im(\psi) \subset Ker(w)$. Ahora consideremos un punto $P \in Ker(w)$ y verifiquemos que se satisface $P \in Im(\psi)$. Si $P \in E_1$ no es $(0, 0)$, se tiene $P = \left(\dfrac{p^2}{q^2}, k\right)$ y por lo tanto ha de cumplirse

$$k^2 = \frac{p^6}{q^6} + a\frac{p^4}{q^4} + b\frac{p^2}{q^2} \tag{3.10}$$

$$= \frac{p^6 + ap^4q^2 + bp^2q^4}{q^6}. \tag{3.11}$$

Probaremos que bajo tales condiciones existirá $(x, y) \in E_1^*$ sujeto a $\psi(x, y) = \left(\dfrac{p^2}{q^2}, k\right)$,

es decir, que satisface

$$\frac{y^2}{4x^2} = \frac{p^2}{q^2} \qquad \text{e} \tag{3.12}$$

$$\frac{y(a^2-4b-x^2)}{8x^2} = k. \tag{3.13}$$

En efecto, de 3.12 se tiene $x^2 = \dfrac{y^2q^2}{4p^2}$ y al reemplazarlo en 3.13 obtendremos

$$k = \frac{y[4p^2(a^2-4b)-y^2q^2]}{8y^2q^2}, \tag{3.14}$$

$$0 = y^2 + 8ky - \frac{4p^2}{q^2}(a^2-4b) \tag{3.15}$$

$$= (y+4k)^2 - 16k^2 - \frac{4p^2}{q^2}(a^2-4b) \tag{3.16}$$

$$= (y+4k)^2 - \frac{4p^2}{q^2}\left(a^2-4b+\frac{4k^2q^2}{p^2}\right). \tag{3.17}$$

De 3.11, reemplazamos la expresión de k^2 en 3.17 para obtener

$$0 = (y+4k)^2 - \frac{4p^2}{q^2}\left(\frac{4p^4}{q^4}+\frac{4ap^2}{q^2}+a^2\right),$$

$$0 = (y+4k)^2 - \left[\left(\frac{2p}{q}\right)\left(\frac{2p^2}{q^2}+a\right)\right]^2.$$

Luego, las posibles soluciones para y son

$$y_1 = \frac{4p^3}{q^3}+\frac{2ap}{q}-4k,$$

$$y_2 = -\frac{4p^3}{q^3}-\frac{2ap}{q}-4k.$$

De 3.12 se obtiene $x = \pm\dfrac{yq}{2p}$ y con ello los posibles valores para x serán

$$\pm\left[\frac{2p^2}{q^2}+a-\frac{2kq}{p}\right] \quad \text{ó} \quad \pm\left[-\frac{2p^2}{q^2}-a-\frac{2kq}{p}\right].$$

Ahora, como $(x,y) \in E_1^*$, se deberá satisfacer $y^2 = x^3 - 2ax^2 + (a^2-4b)x$, lo cual al combinarlo con $y^2 = \dfrac{4p^2x^2}{q^2}$ lleva a

$$\frac{4p^2x^2}{q^2} = x\left[x^2-2ax+(a^2-4b)\right], \tag{3.18}$$

$$0 = x^2 - \frac{2}{q^2}(aq^2+2p^2)x + a^2 - 4b \tag{3.19}$$

$$= \left[x-\frac{aq^2+2p^2}{q^2}\right]^2 - \frac{(aq^2+2p^2)^2}{q^4} + a^2 - 4b \tag{3.20}$$

$$= \left[x-\frac{aq^2+2p^2}{q^2}\right]^2 - \frac{4(p^4+aq^2p^2+bq^4)}{q^4}. \tag{3.21}$$

Al utilizar 3.11 en la última ecuación se obtiene

$$0 = \left[x - \frac{aq^2 + 2p^2}{q^2}\right]^2 - \frac{4k^2q^2}{p^2},$$

y con ello las soluciones para x son precisamente

$$\begin{aligned} x_1 &= \frac{2kq}{p} + a + \frac{2p^2}{q^2}, \\ x_2 &= -\frac{2kq}{p} + a + \frac{2p^2}{q^2}. \end{aligned}$$

Es decir, los pares (x_1, y_1) y (x_2, y_2) satisfacen $\psi(x_i, y_i) = \left(\frac{p^2}{q^2}, k\right)$

Por otro lado, tener $P = \left(\frac{p^2}{q^2}, 0\right) \in Ker(w)$ equivale a que b sea cuadrado perfecto. Probemos que $(0,0)$ está en la imagen si y solo si b es un cuadrado perfecto. Si $(0,0) \in Im(\psi)$, se satisface $(0,0) \in Ker(w)$, pues $Im(\psi) \subset Ker(w)$. En la otra dirección, asumamos que se tenga $b = \frac{p^2}{q^2}$. Nosotros deberemos encontrar $(x, y) \in E_1^*$ que satisfaga $\psi(x, y) = (0, 0)$. Para ello, se requiere resolver el sistema

$$\begin{aligned} \frac{y^2}{4x^2} &= 0 \qquad \text{e} \\ \frac{y(a^2 - 4b - x^2)}{8x^2} &= 0. \end{aligned}$$

Acá apenas $y = 0$ es posible. Como $(x, 0)$ debe pertenecer a E_1^*, se debe satisfacer

$$x^3 - 2ax^2 + (a^2 - 4b)x = 0,$$

como x no puede ser 0, se pasa a

$$x^2 - 2ax + a^2 - 4b = 0,$$

o de modo equivalente a

$$(x - a)^2 = 4b = \frac{4p^2}{q^2}.$$

Los valores de x serán luego $x_1 = a - \frac{2p}{q}$ y $x_2 = a + \frac{2p}{q}$. Se comprueba así que se verifica $\psi\left(a - \frac{2p}{q}, 0\right) = (0,0)$ y $\psi\left(a + \frac{2p}{q}, 0\right) = (0,0)$, es decir $(0,0) \in Im(\psi)$.

Todo nuestro trabajo se resume en la igualdad $Ker(w) = Im(\psi)$. □

Antes de concluir que el índice $[E_1(\mathbb{Q}) : E_1^*(\mathbb{Q})]$ es finito, probaremos en el siguiente lema que el índice $[E_1(\mathbb{Q}) : \psi(E_1^*(\mathbb{Q}))]$ es finito.

Lema 3.26. *Sea la curva elíptica $E_1 : y^2 = x^3 + ax^2 + bx$ y su dual $E_1^* : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Tenemos que $[E_1(\mathbb{Q}) : \psi(E_1^*(\mathbb{Q}))]$ es finito, donde $\psi : E_1^* \to E_1$ es definida por $\psi(x, y) = \left(\frac{y^2}{4x^2}, \frac{y(a^2 - 4b - x^2)}{8x^2}\right)$ si $(x, y) \neq (0,0), \mathcal{O}$, y $\psi(0,0) = \psi(\mathcal{O}) = \mathcal{O}$.*

Prueba. Definamos $F : \dfrac{E_1^*}{\phi(E_1)} \to \dfrac{\psi(E_1^*)}{(\psi\circ\phi)(E_1)}$ mediante $F(\pi_1(b)) = \pi_2(\psi(b))$, donde $\pi_1 : E_1^* \to \dfrac{E_1^*}{\phi(E_1)}$ y $\pi_2 : E_1^* \to \dfrac{\psi(E_1^*)}{(\psi\circ\phi)(E_1)}$ son las proyecciones canónicas. Dicha función está bien definida, pues si $\pi_1(P) = \pi_1(Q)$, se tiene $P - Q = \phi(R)$ y con ello $\psi(P) - \psi(Q) = (\psi\circ\phi)(R)$, es decir $\pi_2(\psi(P)) = \pi_2(\psi(Q))$. Además F es sobreyectiva puesto que todo elemento de $\dfrac{\psi(E_1^*)}{(\psi\circ\phi(E_1))}$ es de la forma $\pi_2(\psi(D))$, con $D \in E_1^*$. Al ser F sobreyectiva, concluimos la desigualdad de índices $[E_1^* : \phi(E_1)] \geq [\psi(E_1^*) : (\psi\circ\phi)(E_1)]$.

La función $g : \dfrac{E_1}{\psi(E_1^*)} \to \dfrac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$, dada por $g(\overline{P}) = w(P)$, está bien definida, ya que si $\overline{P} = \overline{Q}$, entonces $P - Q \in Im(\psi) = Ker(w)$ y con ello $w(P) = w(Q)$. Además g es inyectiva, pues si $g(\overline{P}) = g(\overline{Q})$, se cumple $w(P) = w(Q)$. Luego se tiene $P - Q \in Ker(w) = Im(\psi)$, es decir $\overline{P} = \overline{Q}$. Como $Im(w)$ es finito y además se tiene $Im(g) = Im(w)$, resulta que el índice $[E_1(\mathbb{Q}) : \psi(E_1^*(\mathbb{Q}))]$ es finito. □

De forma similar se concluye que el índice $[E_1^*(\mathbb{Q}) : \phi(E_1(\mathbb{Q}))]$ es finito. Recordemos que $\psi\circ\phi : E_1 \to E_1$ verifica $(\psi\circ\phi)(P) = 2P$. Sin embargo, acá no siempre hay sobreyectividad así que apenas obtenemos

$$\begin{aligned}[E_1 : 2E_1] &\leq [E_1 : (\psi\circ\phi)(E_1)] = [E_1 : \psi(E_2)][\psi(E_2) : (\psi\circ\phi)(E_1)], \\ &\leq [E_1 : \psi(E_2)][E_2 : \phi(E_1)].\end{aligned}$$

Como $[E_1 : \psi(E_2)]$ y $[E_2 : \phi(E_1)]$ son finitos, concluimos que $[E_1 : 2E_1]$ también lo es, y con ello queda probado el teorema 3.20.

Ahora nuestra segunda meta es probar que $E_1(\mathbb{Q})$ es finitamente generado, el teorema de Mordell-Weil. La siguiente prueba es considerada estándar en el área. (Nuestro desarrollo se basa en [13].)

Teorema 3.27 (Teorema del descenso)**.** *Sean $E_1 : y^2 = x^3 + ax^2 + bx$ una curva elíptica sobre $\mathbb{Q}$, y $h : E_1 \to [0, \infty[$ una función con las siguientes características:*

1. *para cada número M el conjunto $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ es finito;*
2. *para cualquier $P_1 \in E_1(\mathbb{Q})$, existe una constante $r = r(P_1)$ tal que $h(P_2 + P_1) \leq 2h(P_2) + r$, para todo $P_2 \in E(\mathbb{Q})$;*
3. *existe una constante κ tal que $h(2P) \geq 4h(P) - \kappa$ para todo $P \in E(\mathbb{Q})$;*
4. *el índice $[E_1 : 2E_1]$ es finito.*

Entonces $E_1(\mathbb{Q})$ es finitamente generado.

Prueba. Como el índice $[E_1(\mathbb{Q}) : 2E_1(\mathbb{Q})]$ es finito, existen $q_1, q_2, \ldots, q_n \in E_1(\mathbb{Q})$ con los cuales tenemos $\dfrac{E_1(\mathbb{Q})}{2E_1(\mathbb{Q})} = \{\overline{q}_1, \overline{q}_2, \ldots, \overline{q}_n\}$. Para cada $p \in E_1(\mathbb{Q})$, se tiene entonces $\overline{p} = \overline{q}_{i_1}$ con $q_{i_1} \in \{q_1, \ldots, q_n\}$: es decir, existe $p_1 \in E_1(\mathbb{Q})$ tal que $p = q_{i_1} + 2p_1$. De la misma manera, para p_1 podemos encontrar $q_{i_2} \in \{q_1, \ldots, q_n\}$ y

$p_2 \in E_1(\mathbb{Q})$ que cumplen $p_1 = q_{i_2} + 2p_2$. Si continuamos con este proceso obtenemos $q_{i_3}, \ldots, q_{i_m} \in \{q_1, \ldots, q_n\}$ y $p_3 \ldots, p_m \in E_1(\mathbb{Q})$ sujetos a

$$\begin{aligned} p_2 &= q_{i_3} + 2p_3, \\ p_3 &= q_{i_4} + 2p_4, \\ &\vdots \\ p_{m-1} &= q_{i_m} + 2p_m. \end{aligned}$$

Al reemplazar de abajo arriba logramos

$$p = \sum_{j=1}^{m-1} 2^j q_{i_j} + 2^m p_m. \tag{3.22}$$

Nuestra meta es lograr una combinación, como en 3.22, tal que el último elemento, es decir p_m, pertenezca a un conjunto finito conocido de antemano. Para ello, gracias al ítem 2, para cada $j \in \{1, 2, \ldots, n\}$ tomamos k_j sujeto a

$$h(p - q_j) \leq 2h(p) + k_j,$$

para todo $p \in E_1(\mathbb{Q})$. Sea $\kappa' = \max\{k_1, \ldots, k_n\}$ y elijamos κ como en el ítem 3. Probaremos que $E_1(\mathbb{Q})$ es generado por el conjunto finito $\{q_1, \ldots, q_n\} \cup \{p \in E_1(\mathbb{Q}) : h(p) \leq \kappa' + \kappa\}$.

Primero observemos que con la notación introducida se tiene

$$4h(p_j) \leq h(2p_j) + \kappa = h(p_{j-1} - q_{i_j}) + \kappa \leq 2h(p_{j-1}) + \kappa' + \kappa.$$

Debido a ello obtenemos

$$h(p_j) \leq \frac{1}{2}h(p_{j-1}) + \frac{\kappa' + \kappa}{4} = \frac{3}{4}h(p_{j-1}) - \frac{1}{4}(h(p_{j-1}) - (\kappa' + \kappa)).$$

Deducimos que $h(p_{j-1}) \geq \kappa' + \kappa$ implica $h(p_j) \leq \frac{3}{4}h(p_{j-1})$. Si para $m \in \mathbb{N}$ tenemos $p_m \notin \{p \in E_1(\mathbb{Q}) : h(p) \leq \kappa' + \kappa\}$, entonces de lo anterior se obtiene

$$h(p_{m+1}) \leq \left(\frac{3}{4}\right)^m h(p_1).$$

Como $\lim_{n\to\infty} \left(\frac{3}{4}\right)^m = 0$, eventualmente tendremos $h(p_{m+1}) \leq \kappa' + \kappa$ como queríamos probar.

Concluimos que existe m con el que se cumple

$$p = \sum_{j=1}^{m-1} 2^j q_{i_j} + 2^m p_m,$$

donde $\{q_{i_1}, \ldots, q_{i_m}\} \subset \{q_1, \ldots, q_n\}$ y $p_m \in \{p \in E_1(\mathbb{Q}) : h(p) \leq \kappa' + \kappa\}$. □

A continuación, para la demostración del teorema de Mordell-Well, construiremos una función que satisfaga las condiciones del teorema del descenso.

Teorema 3.28 (Teorema de Mordell-Weil)**.** *Sea $E_1 : y^2 = x^3 + ax^2 + bx$ una curva elíptica con $a, b \in \mathbb{Z}$. Si el índice $[E_1(\mathbb{Q}) : 2E_1(\mathbb{Q})]$ es finito, entonces el grupo $E_1(\mathbb{Q})$ es finitamente generado.*

Prueba. Por lo pronto sabemos que $[E_1(\mathbb{Q}) : 2E_1(\mathbb{Q})]$ es finito. Lo que falta es construir la función h para poder usar el teorema del descenso. Para el punto racional $P = \left(\frac{m}{n}, \frac{u}{v}\right) \in E_1(\mathbb{Q})$ escribimos $H(P) = H\left(\frac{m}{n}\right) = \text{máx}\{|m|, |n|\}$, donde $\text{mcd}(m, n) = 1$ si $P \neq \mathcal{O}$, y $H(\mathcal{O}) = 1$. A continuación definimos $h : E_1(\mathbb{Q}) \to [0, \infty[$ como $h(P) = \log(H(P))$. Para $M \geq 0$ tenemos que $h(P) \leq M$ implica $|m| \leq e^M$ y $|n| \leq e^M$, y se concluye que $\{P \in E_1(\mathbb{Q}) : h(P) \leq M\}$ es finito.

Ahora veremos que nuestra función h verifica el segundo ítem del teorema del descenso. Sean los puntos $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ y $P_3 = P_1 + P_2 = (x_3, y_3)$. Si $P_2 = \mathcal{O}$, con tomar $r \geq h(P_1)$ se cumple trivialmente lo deseado. Si $P_1 = \mathcal{O}$, tenemos $h(P_3) = h(P_2) \leq 2h(P_2) + r$, donde r es cualquier constante no negativa. Ahora veamos el caso $P_1 \neq \mathcal{O}$. Si $P_3 = \mathcal{O}$, se tiene $h(P_3) = 0 \leq 2h(P_2) + r$, donde r es cualquier constante no negativa. Cuando $P_3 \neq \mathcal{O}$ tenemos dos subcasos.

Para $x_1 = x_2$, obtenemos $x_3 = \dfrac{(3x_1^2 + 2ax_1 + b)^2}{4y_1^2} - a - 2x_1$, pero al cumplirse $y_1^2 = x_1^3 + ax_1^2 + bx_1$, se logra

$$\begin{aligned} x_3 &= \frac{9x_1^4 + 4a^2x_1^2 + b^2 + 12ax_1^3 + 4abx_1 + 6bx_1^2}{4x_1^3 + 4ax_1^2 + 4bx_1} - a - 2x_1 \\ &= \frac{x_1^4 + b^2 - 2bx_1^2}{4x_1^3 + 4ax_1^2 + 4bx_1} \\ &= \frac{x_1[x_1^3 - 2bx_1] + b^2}{4x_1^3 + 4ax_1^2 + 4bx_1}. \end{aligned}$$

Además P_2 también se expresa cual $P_2 = \left(\frac{m}{l^2}, \frac{n}{l^3}\right)$, con lo cual x_3 se expande tal

$$x_3 = \frac{\frac{m}{l^2}\left[x_1^3 - 2bx_1\right] + b^2}{4x_1^3 + 4ax_1^2 + 4bx_1} = \frac{m[x_1^3 - 2bx_1] + l^2b^2}{l^2(4x_1^3 + 4ax_1^2 + 4bx_1)} = \frac{r}{s}.$$

Por otro lado, se cumple

$$\begin{aligned} |r| &\leq H(P_2)||x_1^3 - 2bx_1| + b^2|, \\ |s| &\leq H(P_2)|4x_1^3 + 4ax_1^2 + 4bx_1|. \end{aligned}$$

Si $M = \text{máx}\{||x_1^3 - 2bx_1| + b^2|, |4x_1^3 + 4ax_1^2 + 4bx_1|\}$, entonces tenemos $H(P_3) \leq MH(P_2)$ y se consigue $h(P_3) \leq h(P_2) + \log(M) \leq 2h(P_2) + \log(M)$.

Para $x_1 \neq x_2$ tenemos

$$\begin{aligned} x_3 &= \frac{y_2^2 - 2y_2y_1 + y_1^2 - x_2^3 + x_2^2x_1 - ax_2^2 + x_2x_1 + 2ax_2x_1 - x_1^3 - ax_1^2}{x_2^2 - 2x_2x_1 + x_1^2}, \\ y_2^2 &= x_2^3 + ax_2^2 + bx_2, \end{aligned}$$

y por tanto $x_3 = \dfrac{-2y_1y_2 + x_1x_2^2 + (b + x_1^2 + 2ax_1)x_2 + y_1^2 - x_1^3 - ax_1^2}{x_2^2 - 2x_1x_2 + x_1^2}$. Además P_2 se expresa como $P_2 = \left(\dfrac{m}{l^2}, \dfrac{n}{l^3}\right)$, con lo cual x_3 queda expresado cual

$$x_3 = \frac{-2y_1nl + x_1m^2 + (b + x_1^2 + 2ax_1)ml^2 + (y_1^2 - x_1^3 - ax_1^2)l^4}{m^2 - 2x_1ml^2 + x_1^2l^4} = \frac{r}{s}.$$

Como $\left(\dfrac{m}{l^2}, \dfrac{n}{l^3}\right) \in E_1$, se tiene $n^2 = m^3 + am^2l^2 + bml^4$ y con ello $|n^2| \leq (1 + |a| + |b|)H(P_2)^3$ de donde se pasa a $|n| \leq \sqrt{1 + |a| + |b|}(H(P_2))^{3/2}$. Por otro lado, se tiene

$$\begin{aligned} |r| &\leq |2y_1||nl| + |x_1||m^2| + |b + x_1^2 + 2ax_1||ml^2| + |y_1^2 - x_1^3 - ax_1^2||l^4| \\ &\leq H(P_2)^2(|2y_1|\sqrt{1 + |a| + |b|} + |x_1| + |b + x_1^2 + 2ax_1| + |y_1^2 - x_1^3 - ax_1^2|), \\ |s| &\leq H(P_2)^2(1 + |2x_1| + x_1^2). \end{aligned}$$

Si $M = \text{máx}\{|2y_1|\sqrt{1 + |a| + |b|} + |x_1| + |b + x_1^2 + 2ax_1| + |y_1^2 - x_1^3 - ax_1^2|, 1 + |2x_1| + x_1^2\}$, se cumple entonces $H(P_1 + P_2) \leq MH(P_2)^2$, obteniéndose $h(P_3) \leq 2h(P_2) + \log(M)$.

En resumen, para $P_1 \in E(\mathbb{Q})$ existe una constante r (que depende de P_1) tal que $h(P_2 + P_1) \leq 2h(P_2) + r$.

Finalmente pasemos a demostrar que existe una constante κ tal que se cumple $h(2P) \geq 4h(P) - \kappa$ para todo $P \in E_1(\mathbb{Q})$. Si tomamos el punto $P = (x_1, y_1)$, entonces la abscisa de $2P = (x_3, y_3)$ es $x_3 = \dfrac{x_1^4 + b^2 - 2bx_1^2}{4x_1^3 + 4ax_1^2 + 4bx_1}$. Pongamos $\phi(x) = x^4 + b^2 - 2bx^2$ y $\psi(x) = 4x^3 + 4ax^2 + 4bx$. Definamos $p(m, n) = n^4\phi\left(\dfrac{m}{n}\right) = m^4 + n^4b^2 - 2bm^2n^2$ y $q(m, n) = n^4\psi\left(\dfrac{m}{n}\right) = 4m^3n + 4am^2n^2 + 4bmn^3$. Recordemos que la curva elíptica tiene ecuación $E_1 : y^2 = x^3 + ax^2 + bx$. Si $f(x) = x^3 + ax^2 + bx$, entonces $\phi(x) = (f'(x))^2 - 4(a + 2x)f(x)$ y $\psi(x) = 4f(x)$. Al ser E_1 una curva elíptica, los polinomios f y f' no tienen raíces en común, y con ello tampoco ϕ y ψ. Por lo tanto se tiene $\text{mcd}(\phi, \psi) = 1$ en $\mathbb{Q}[x]$ y por ende existen polinomios $F, G \in \mathbb{Q}[x]$ sujetos a

$$F(x)\phi(x) + G(x)\psi(x) = 1. \tag{3.23}$$

Lógicamente existe un entero A con el cual se tiene $AF, AG \in \mathbb{Z}[x]$. Definimos $D = \text{máx}\{grad(F), grad(G)\}$ y multiplicamos ambos lados de 3.23 por An^{4+D} para obtener

$$\begin{aligned} An^{4+D}F\left(\frac{m}{n}\right)\phi\left(\frac{m}{n}\right) + An^{4+D}G\left(\frac{m}{n}\right)\psi\left(\frac{m}{n}\right) &= An^{4+D}, \\ An^DF\left(\frac{m}{n}\right)p(m, n) + An^DG\left(\frac{m}{n}\right)q(m, n) &= An^{4+D}. \end{aligned}$$

Si $k = \text{mcd}\{p(m, n), q(m, n)\}$, se tiene $k|An^{4+D}$. Como $k|p(m, n)$ y $An^{3+D}p(m, n) = An^{3+D}m^4 + b^2An^{7+D} - 2Abm^2n^{5+D}$, se tiene $k|An^{3+D}m^4$. Por lo tanto, se cumple $k|\text{mcd}(An^{4+D}, An^{3+D}m^4) = An^{3+D}$. Al aplicar el proceso anterior $(3 + D)$ veces conseguimos $k|A$, es decir, $\text{mcd}\{p(m, n), q(m, n)\}$ divide a A.

De

$$x_3 = \frac{x_1^4 + b^2 - 2bx_1^2}{4x_1^3 + 4ax_1^2 + 4bx_1} = \frac{m^4 + n^4b^2 - 2bm^2n^2}{4m^3n + 4am^2n^2 + 4bmn^3} = \frac{p(m,n)}{q(m,n)},$$

se pasa a

$$\begin{aligned} H(2P) &= \text{máx}\left\{\frac{|p(m,n)|}{k}, \frac{|q(m,n)|}{k}\right\}, \\ &= \frac{1}{k}\text{máx}\{|p(m,n)|, |q(m,n)|\}, \\ &\geq \frac{1}{A}\text{máx}\{|p(m,n)|, |q(m,n)|\}, \\ &\geq \frac{1}{A}\text{máx}\left\{\left|n^4\phi\left(\frac{m}{n}\right)\right|, \left|n^4\psi\left(\frac{m}{n}\right)\right|\right\}, \\ &\geq \frac{1}{2A}\left(\left|n^4\phi\left(\frac{m}{n}\right)\right| + \left|n^4\psi\left(\frac{m}{n}\right)\right|\right), \end{aligned}$$

Ahora definimos $z(t) = \dfrac{|\phi(t)| + |\psi(t)|}{2A \cdot \text{máx}\{|t^4|, 1\}}$, cantidad positiva pues si $z(t_0) = 0$ para algún valor t_0, se tendrá $\phi(t_0) = \psi(t_0) = 0$, con lo cual ϕ y ψ compartirán raíces, lo cual es imposible. Asimismo se tiene

$$\begin{aligned} \lim_{t\to\infty} z(t) &= \lim_{t\to\infty} \frac{|\phi(t)| + |\psi(t)|}{2A \cdot \text{máx}\{|t^4|, 1\}}, \\ &= \lim_{t\to\infty} \frac{|\phi(t)| + |\psi(t)|}{2A \cdot |t^4|}, \\ &= \frac{1}{2A} > 0. \end{aligned}$$

A partir de ello, al aprovechar la continuidad de z, se deduce $z(t) > C$ para cierto $C > 0$ y para todo $t \in \mathbb{R}$. Luego tendremos

$$\begin{aligned} z\left(\frac{m}{n}\right) &= \frac{\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|}{2A \cdot \text{máx}\left\{\left|\frac{m}{n}\right|^4, 1\right\}}, \\ &= \frac{\left|n^4\phi\left(\frac{m}{n}\right)\right| + \left|n^4\psi\left(\frac{m}{n}\right)\right|}{2A \cdot \text{máx}\{|m|^4, |n|^4\}}. \end{aligned}$$

De $z\left(\dfrac{m}{n}\right) > C$, $H(2P) \geq \dfrac{1}{2A}\left(\left|n^4\phi\left(\dfrac{m}{n}\right)\right| + \left|n^4\psi\left(\dfrac{m}{n}\right)\right|\right)$ y $H\left(\dfrac{m}{n}\right) = \text{máx}\{|m|, |n|\}$, se pasa a

$$H(2P) \geq CH^4\left(\frac{m}{n}\right),$$

y con ello tenemos

$$h(2P) \geq 4h\left(\frac{m}{n}\right) - \log\left(\frac{2A}{C}\right).$$

Por lo tanto h cumple los ítemes del teorema del descenso y con ello concluimos que $E_1(\mathbb{Q})$ es finitamente generado. □

Capítulo 4

Isomorfismos de curvas elípticas

Ahora veremos la importancia del invariante j, lo cual se podrá notar de mejor manera al estudiarlo según sea la característica del cuerpo donde se trabaje. Las referencias básicas para este capítulo son [1], [3], [7], [11], [15], [16].

Las curvas elípticas

$$\begin{array}{rcccl} E_1(\mathbb{K}) & : & y^2 + a_1xy + a_3y & = & x^3 + a_2x^2 + a_4x + a_6 \\ E_2(\mathbb{K}) & : & s^2 + a_1'ts + a_3's & = & t^3 + a_2't^2 + a_4't + a_6', \end{array}$$

son **isomorfas** sobre $\mathbb{K}$ cuando existe una isogenía $\phi : E_1 \to E_2$ invertible.

Comenzaremos analizando la forma de las isogenías invertibles entre dos curvas elípticas sobre cuerpos de cualquier característica.

Lema 4.1. *Sean las curvas elípticas*

$$\begin{array}{rcccl} E_1(\mathbb{K}) & : & y^2 + a_1xy + a_3y & = & x^3 + a_2x^2 + a_4x + a_6 \\ E_2(\mathbb{K}) & : & s^2 + a_1'ts + a_3's & = & t^3 + a_2't^2 + a_4't + a_6' \end{array}$$

y consideremos un isomorfismo $\phi : E_1 \to E_2$. Entonces la isogenía toma la forma $\phi(x, y) = (r(x), p(x) + q(x)y)$, donde $r \in \mathbb{K}[x]$ es de grado 1 y q, $r \in \mathbb{K}[x]$ son polinomios.

Prueba. Dado que ϕ es un isomorfismo, existe $\psi : E_2 \to E_1$ tal que $(\phi \circ \psi)(P) = P$ y $(\psi \circ \phi)(Q) = Q$ para todo $P \in E_1$ y $Q \in E_2$. Observamos que tanto ϕ como ψ son isogenías de grado 1.

Si la característica del cuerpo $\mathbb{K}$ es distinta de 2, entonces podemos suponer sin pérdida de generalidad que las curvas elípticas son de la forma $E_1 : y^2 = x^3 + a_2x^2 + a_4x + a_6$ y $E_2 : y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$. Por el corolario 3.18, la isogenía ϕ queda definida como $\phi(x, y) = \left(\dfrac{u(x)}{v(x)}, \dfrac{s(x)}{t(x)}y\right)$. Además $v^3(x)$ divide a $t^2(x)$ y $t^2(x)$ divide a $v^3(x)f(x)$, donde $f(x) = x^3 + a_2x^2 + a_4x + a_6$. Como el grado de la isogenía ϕ es 1, entonces máx$\{deg(u(x)), deg(v(x))\} = 1$. Supongamos que el polinomio $v(x)$ no es constante. Si t es un polinomio no constante, como $t^2(x)$ divide a $v^3(x)f(x)$ y $f(x)$ no tiene raíces dobles, entonces existe un factor primo de $t(x)$ que divide a $v^3(x)$ y por ende divide a $v(x)$. Dado que $deg(v(x)) = 1$, se observa que $v(x)$ divide a $t(x)$ y por ello se tiene $t(x) = v(x)v_1(x)$. Como $v^3(x)$ divide a $t^2(x) = v^2(x)v_1^2(x)$, entonces

$v(x)$ divide a $v_1(x)$ y por ello $v_1(x) = v(x)v_2(x)$. De la expresión $t(x) = v(x)v_1(x)$ se deduce $t(x) = v^2(x)v_2(x)$, y como $t^2(x)$ divide a $v^3(x)f(x)$ se obtiene que $v(x)v_2^2(x)$ divide a $f(x)$. Dado que $f(x)$ no tiene raíces dobles, $v_2(x)$ resulta constante y puede tomarse igual a 1. Gracias a ello se concluye que v_1 y v coinciden y se satisface $t(x) = v^2(x)$. Lo anterior implica que v divide a f y por tanto se tiene $f(x) = v(x)f_1(x)$. Del corolario 3.18 se tiene la ecuación $v^3(x)s^2(x)f(x) = g(x)t^2(x)$, donde $g(x) = u^3(x)+a_2'u^2(x)v(x)+a_4'u(x)v^2(x)+a_6'v^3(x)$, y al reemplazar en dicha ecuación las expresiones $t(x) = v^2(x)$ y $f(x) = v(x)f_1(x)$ se obtiene $s^2(x)f_1(x) = g(x)$. Como $deg(f_1(x)) = 2$ y $deg(g(x)) \leq 3$, entonces $deg(s^2(x)) \leq 1$ lo cual obliga a decir que s es constante. Asumiendo que $s(x) = 1$, se tiene que $f_1(x) = g(x)$. Debido a esto, la isogenía queda expresada como $\phi(x, y) = \left(\dfrac{u(x)}{v(x)}, \dfrac{y}{v^2(x)}\right)$. Si tomamos x_0 raíz de v, entonces $f(x_0) = 0$ y $f_1(x_0) \neq 0$ pues f no admite raíces dobles. Como $\phi(x : y : 1) = \left(u(x) : \dfrac{y}{v(x)} : v(x)\right) = \left(u(x) : \dfrac{y}{v(x)} : v(x)\right) = (yu(x) : f_1(x) : yv(x))$, entonces $\phi(x_0 : 0 : 1) = (0 : f_1(x_0) : 0) = \mathcal{O}$, lo cual es imposible. Por lo tanto, $t(x)$ es un polinomio constante y al cumplirse $v^3(x)s^2(x)f(x) = g(x)t^2(x)$ se desprende que $v(x)$ también es constante lo cual contradice a lo supuesto. Entonces v es constante, y como $t^2(x)$ divide a $v^3(x)f(x)$, se deduce que t es constante. En este caso tomamos $r(x) = u(x)$, $q(x) = 0$ y $q(x) = s(x)$.

Veamos ahora el caso cuando la característica del cuerpo base es 2. Tenemos que el isomorfismo está definido como $\phi(x, y) = \left(\dfrac{u(x)}{v(x)}, \dfrac{s(x) + w(x)y}{t(x)}\right)$.
De la sección 2.2, cuando $a_1 = a_1' = 0$, podemos tomar las curvas elípticas como $E_1 : y^2 + y = x^3 + a_4x + a_6$ y $E_2 : y^2 + y = x^3 + a_4'x + a_6$. Sabemos de la observación 3.16, que se satisface

$$2s(x) = (a_1x + a_3)w(x) - \left(a_1'\frac{u(x)}{v(x)} + a_3'\right)t(x). \tag{4.1}$$

Como $a_1 = a_1' = 0$ y $a_3 = a_3' = 1$, de la ecuación 4.1, tenemos $w(x) = t(x)$ y con ello la isogenía queda expresada como $\phi(x, y) = \left(\dfrac{u(x)}{v(x)}, \dfrac{s(x) + t(x)y}{t(x)}\right)$, que en esta ocasión lo podemos elegir de tal manera que $t(x)$ y $s(x)$ sean coprimos. Dado que $\phi(x, y) \in E_2$, tenemos

$$\left(\frac{s + ty}{t}\right)^2 + \frac{s + ty}{t} = \left(\frac{u}{v}\right)^3 + a_4'\frac{u}{v} + a_6', \tag{4.2}$$

$$\frac{s^2 + t^2y^2 + st + t^2y}{t^2} = \frac{u^3 + a_4'uv^2 + a_6'v^3}{v^3}, \tag{4.3}$$

$$v^3(s^2 + t^2y^2 + st + t^2y) = t^2(u^3 + a_4'uv^2 + a_6'v^3), \tag{4.4}$$

$$v^3(s^2 + st + t^2(y^2 + y)) = t^2(u^3 + a_4'uv^2 + a_6'v^3), \tag{4.5}$$

$$v^3(s^2 + st + t^2(x^3 + a_4x + a_6)) = t^2(u^3 + a_4'uv^2 + a_6'v^3). \tag{4.6}$$

Por otro lado, si v no es constante, nos damos cuenta de la última ecuación que v^3 divide a $t^2(u^3 + a_4'uv^2 + a_6'v^3)$ y como v no divide a $u^3 + a_4'uv^2 + a_6'v^3$, entonces v^3 divide a t^2 con lo cual podemos decir que $t = v^nw_1$ donde v no divide a w_1 y $n \geq 2$.

De la ecuación 4.6 tenemos $v^3 s(s+t) = t^2[u^3 + a_4' uv^2 + a_6' v^3 - v^3(x^3 + a_4 x + a_6)]$. Observamos que $t^2 = v^{2n} w_1^2$ divide a $v^3 s(s+t)$ y como v no divide a s ni a $s+t$ se deduce que $2n \leq 3$ lo cual es absurdo pues $n \geq 2$. Por lo tanto v debe ser un polinomio constante. De la ecuación 4.6 se tiene que t también es constante pues de lo contrario t^2 divide a $s^2 + st + t^2(x^3 + a_4 x + a_6)$ lo que implica que t divida a s y ello contradice el hecho que s y t sean coprimos. En este caso tomamos $r(x) = u(x)$, $p(x) = s(x)$ y $r(x) = w(x)$.
Para $a_1, a_1' \neq 0$, podemos suponer que las curvas elípticas son de la forma E_1 : $y^2 + xy = x^3 + a_2 x^2 + a_6$ y $E_2 : y^2 + xy = x^3 + a_2' x^2 + a_6'$. Sabemos que en general se cumple

$$2s(x) = (a_1 x + a_3) w(x) - \left(a_1' \frac{u(x)}{v(x)} + a_3' \right) t(x). \tag{4.7}$$

De las curvas elípticas E_1 y E_2 nos damos cuenta que $a_1 = a_1' = 1$ y $a_3 = a_3' = 0$, y con ello, de la ecuación 4.7, $xw(x)v(x) = u(x)t(x)$. Como $\phi(x,y) = \left(\frac{u}{v}, \frac{s+wy}{t} \right) \in E_2$, tenemos

$$\left(\frac{s+wy}{t} \right)^2 + \left(\frac{u}{v} \right) \left(\frac{s+wy}{t} \right) = \left(\frac{u}{v} \right)^3 + a_2' \left(\frac{u}{v} \right)^2 + a_6', \tag{4.8}$$

$$\left(\frac{s+wy}{t} \right) \left[\frac{s+wy}{t} + \frac{xw}{t} \right] = \frac{u^3 + a_2' u^2 v + a_6' v^3}{v^3}, \tag{4.9}$$

$$(s+wy)[s+wy+xw] = \frac{(u^3 + a_2' u^2 v + a_6' v^3) t^2}{v^3}, \tag{4.10}$$

$$s^2 + w^2 y^2 + swx + w^2 xy = \frac{(u^3 + a_2' u^2 v + a_6' v^3) t^2}{v^3}, \tag{4.11}$$

$$s^2 + swx + w^2(y^2 + xy) = \frac{(u^3 + a_2' u^2 v + a_6' v^3) t^2}{v^3}, \tag{4.12}$$

$$s^2 + swx + w^2(x^3 + a_2 x^2 + a_6) = \frac{(u^3 + a_2' u^2 v + a_6' v^3) t^2}{v^3}, \tag{4.13}$$

$$s^2 + swx + w^2(x^3 + a_2 x^2 + a_6) = \frac{(u^3 + a_2' u^2 v + a_6' v^3) t^2}{v^3}, \tag{4.14}$$

Supongamos que v no es constante. Dado que v no divide a $u^3 + a_2' u^2 v + a_6' v^3$, entonces v^3 divide a t^2 y de esa forma $t = v^\alpha t_1$ donde v no divide a t_1 con $\alpha \geq 2$. De la igualdad $xwv = ut$, se obtiene $w = \dfrac{v^{\alpha-1} u t_1}{x}$ que al reemplazarlo en la ecuación 4.14 se cumple

$$s(s+wx) + \frac{v^{2\alpha-2} u^2 t_1^2 (x^3 + a_2 x^2 + a_6)}{x^2} = g v^{2\alpha-3} t_1^2, \tag{4.15}$$

donde $g = u^3 + a_2' u^2 v + a_6' v^3$.
Si $v = mx$, con m escalar, entonces de la ecuación 4.15 se cumple

$$s(s+wx) = g v^{2\alpha-3} t_1^2 - v^{2\alpha-4} m^2 u^2 t_1^2 (x^3 + a_2 x^2 + a_6), \tag{4.16}$$

$$s(s+wx) = v^{2\alpha-4} t_1^2 [gv - m^2 u^2 (x^3 + a_2 x^2 + a_6)]. \tag{4.17}$$

Si suponemos que $\alpha = 2$, a partir de la ecuación 4.10 y de la igualdad $t = v^2 t_1$, se tiene

$$(s + wy)(s + wy + xw) \;=\; gvt_1^2.$$

Para $x = 0$, tomando y_0 tal que $(0, y_0) \in E_1$, se tiene $s(0) + w(0)y_0 = 0$. Volviendo al isomorfismo, podemos observar lo siguiente

$$\begin{aligned}
\phi(x : y : 1) &= \left(\frac{u}{v} : \frac{s + wy}{t} : 1\right), \\
\phi(x : y : 1) &= \left(\frac{u}{v} : \frac{s + wy}{v^2 t_1} : 1\right), \\
\phi(x : y : 1) &= \left(\frac{u(s + wy + wx)}{v} : \frac{(s + wy)(s + wy + wx)}{v^2 t_1} : (s + wy + wx)\right), \\
\phi(x : y : 1) &= \left(\frac{u(s + wy + wx)}{v} : \frac{gvt_1^2}{v^2 t_1} : (s + wy + wx)\right), \\
\phi(x : y : 1) &= \left(u(s + wy + wx) : gt_1 : (s + wy + wx)v\right).
\end{aligned}$$

Dado que $g(0), t_1(0) \neq 0$, se tiene $\phi(0 : y_0 : 1) = (0 : g(0)t_1(0) : 0) = (0 : 1 : 0)$, lo cual no puede ocurrir pues ϕ es un isomorfismo y además concluimos que $\alpha > 2$. De la ecuación 4.17, se desprende que v divide a s y por ello lo podemos expresar como $s = v^k s_1$ donde v no divide a s_1. Volviendo a la ecuación 4.17 y reemplazando $s = v^k s_1$ tenemos

$$v^k s_1(v^k s_1 + ut_1 v^{\alpha-1}) \;=\; v^{2\alpha-4} t_1^2 [gv - m^2 u^2 (x^3 + a_2 x^2 + a_6)].$$

De la última ecuación se puede apreciar que $k < 2\alpha - 4$ y además

$$s_1(v^k s_1 + ut_1 v^{\alpha-1}) \;=\; v^{2\alpha-4-k} t_1^2 [gv - m^2 u^2 (x^3 + a_2 x^2 + a_6)]. \tag{4.18}$$

Como $2\alpha - 4 - k > 0$, entonces del lado izquierdo de la ecuación 4.18 deducimos que $min\{k, \alpha - 1\} \leq 2\alpha - 4 - k$ y de ello se concluye que $k \leq \alpha - 3$. Ahora del isomorfismo ϕ se tiene

$$\begin{aligned}
\phi(x : y : 1) &= \left(\frac{u}{v} : \frac{s + wy}{t} : 1\right), \\
\phi(x : y : 1) &= \left(\frac{ut}{v} : s + wy : t\right), \\
\phi(x : y : 1) &= \left(ut_1 v^{\alpha-1} : v^k s_1 + mut_1 v^{\alpha-2} y : v^\alpha t_1\right), \\
\phi(x : y : 1) &= \left(ut_1 v^{\alpha-1-k} : s_1 + mut_1 v^{\alpha-2-k} y : v^{\alpha-k} t_1\right),
\end{aligned}$$

Nuevamente, para $(0, y_0) \in E_1$, tenemos que $\phi(0 : y_0 : 1) = (0 : 1 : 0)$ lo cual no puede suceder y podemos decir entonces que v es coprimo con x.
Dado que v es coprimo con x y $\alpha \geq 2$, de la ecuación 4.15, se deduce que v divide a s y por ello $s = v^k s_1$ tal que v es coprimo con s_1. Si $k < \alpha - 1$, del isomorfismo ϕ

tenemos

$$\begin{aligned}
\phi(x:y:1) &= \left(\frac{u}{v} : \frac{s+wy}{t} : 1\right), \\
\phi(x:y:1) &= \left(\frac{ut}{v} : s+wy : t\right), \\
\phi(x:y:1) &= \left(uv^{\alpha-1}t_1 : v^k s_1 + \frac{ut_1 v^{\alpha-1}y}{x} : v^\alpha t_1\right), \\
\phi(x:y:1) &= \left(uv^{\alpha-1-k}t_1 : s_1 + \frac{ut_1 v^{\alpha-1-k}y}{x} : v^{\alpha-k} t_1\right),
\end{aligned}$$

Nos damos cuenta que $\phi(x_0 : y_0 : 1) = (0 : s_1 : 0) = (0 : 1 : 0)$, para $(x_0, y_0) \in E_1$ con $v(x_0) = 0$, lo cual no puede suceder. Por otro lado, cuando $k \geq \alpha - 1$ y de la ecuación 4.10, el isomorfismo ϕ queda como

$$\begin{aligned}
\phi(x:y:1) &= \left(\frac{u}{v} : \frac{s+wy}{t} : 1\right), \\
\phi(x:y:1) &= \left(\frac{u(s+wy+wx)}{v} : \frac{(s+wy)(s+wy+wx)}{t} : s+wy+wx\right), \\
\phi(x:y:1) &= \left(\frac{u(s+wy+wx)}{v} : \frac{gt}{v^3} : s+wy+wx\right), \\
\phi(x:y:1) &= \left(\frac{uv^2(s+wy+wx)}{t} : g : \frac{(s+wy+wx)v^3}{t}\right), \\
\phi(x:y:1) &= \left(uv^{2-\alpha}(s+wy+wx) : gt_1 : (s+wy+wx)v^{3-\alpha}\right), \\
\phi(x:y:1) &= \left(uv^{2-\alpha+k}s_1 + \frac{u^2 t_1 v}{x}(y+x) : gt_1 : v^{3-\alpha+k}s_1 + \frac{ut_1 v^2}{x}(y+x)\right).
\end{aligned}$$

Observamos que $\phi(x_0 : y_0 : 1) = (0 : w(x_0)t_1(x_0) : 0) = (0 : 1 : 0)$, para $(x_0, y_0) \in E_1$ con $v(x_0) = 0$, lo cual tampoco puede ocurrir. Por lo tanto, se tiene que v es constante. De la igualdad $ut = xwv$ y la ecuación 4.14 nos damos cuenta que si x divide a u, entonces t divide a s y w. Si x no divide a u, entonces $t = x^n t_2$ donde x no divide a t_2 y además $w = ut_2 v^{-1} x^{n-1}$. Por la ecuación 4.14 se tiene que t_2 divide a s, con ello $s = t_2 s_1$ y se cumple

$$\begin{aligned}
s_1(s_1 + uv^{-1}x^n) + u^2 v^{-2} x^{2n-2}(x^3 + a_2 x^2 + a_6) &= gv^{-3}x^{2n}, \qquad (4.19) \\
s_1^2 + a_6 u^2 v^{-2} x^{2n-2} + uv^{-1}x^n(s_1 + uv^{-1}x^n(x + a_2)) &= gv^{-3}x^{2n}. \qquad (4.20)
\end{aligned}$$

Si $n = 1$, la ecuación 4.20 se reduce a

$$s_1^2 + a_6 u^2 v^{-2} + uv^{-1}x(s_1 + uv^{-1}x(x + a_2)) = gv^{-3}x^2,$$

y observamos que x divide a $s_1^2 + u^2 v^{-2} a_6 = (s_1 + uv^{-1}\sqrt{a_6})^2$, es decir x^2 divide a $s_1^2 + u^2 v^{-2} a_6$, y con ello se tiene que x divide a s_1. Por lo tanto, deducimos que x^2 divide a $u^2 v^{-2} a_6$ lo cual es contradictorio pues x es coprimo con u.

Si $n > 1$, entonces de la ecuación 4.20 se tiene que x divide a s_1 y con ello $s_1 = x^m s_2$ donde x no divide a s_2. Luego el isomorfismo queda de la siguiente manera

$$\begin{aligned}
\phi(x : y : 1) &= \left(\frac{u}{v} : \frac{t_2 x^m s_2 + u t_2 v^{-1} x^{n-1} y}{x^n t_2} : 1\right), \\
\phi(x : y : 1) &= (u x^n t_2 : t_2 x^m s_2 v + u t_2 x^{n-1} y : x^n t_2 v), \\
\phi(x : y : 1) &= (u x^n : x^m s_2 v + u x^{n-1} y : x^n v).
\end{aligned}$$

Dado que $\mathcal{O}$ solo se corresponde con $\mathcal{O}$, se tiene que $m = n - 1$, y entonces ϕ queda expresado como

$$\phi(x : y : 1) = (ux : s_2 v + uy : xv).$$

En la ecuación 4.20 reemplazamos $m = n - 1$ y obtenemos

$$\begin{aligned}
x^{2n-2}(s_2^2 + a_6 u^2 v^{-2}) + u v^{-1} x^{2n-1} s_2 + u^2 v^{-2} x^{2n}(x + a_2) &= g v^{-3} x^{2n}, \quad (4.21) \\
s_2^2 + a_6 u^2 v^{-2} + u v^{-1} x s_2 + u^2 v^{-2} x^2 (x + a_2) &= g v^{-3} x^2. \quad (4.22)
\end{aligned}$$

Observamos que x divide a $s_2^2 + a_6 u^2 v^{-2} = (s_2 + a_6 u v^{-1})^2$, y por ello deducimos que x^2 divide a $s_2^2 + a_6 u^2 v^{-2}$. Luego de la ecuación 4.22, vemos que x divide a $u v^{-1} s_2$ lo cual es imposible pues x es coprimo con u y s_2.
Finalmente, llegamos a que x divide a u y con ello t divide a s y w. En este caso tomemos $r(x) = u(x)$, $p(x) = \dfrac{s(x)}{t(x)}$ y $q(x) = \dfrac{w(x)}{t(x)}$. □

Del teorema anterior, podemos ser un poco más precisos con respecto a los polinomios r y q tal como se muestra en el siguiente corolario.

Corolario 4.2. *Sean las curvas elípticas*

$$\begin{aligned}
E_1(\mathbb{K}) &: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \\
E_2(\mathbb{K}) &: s^2 + a_1' ts + a_3' s = t^3 + a_2' t^2 + a_4' t + a_6'
\end{aligned}$$

y consideremos un isomorfismo $\phi : E_1 \to E_2$. Entonces la isogenía toma la forma $\phi(x, y) = (u(x), v(x) + \lambda y)$, donde u, $v \in \mathbb{K}[x]$ son polinomios de grado 1 y λ es una constante.

Prueba. Del lema 4.1 tenemos $\phi(x, y) = (r(x), p(x) + q(x)y)$ con inversa, digamos ψ, de la forma $\psi(t, s) = (R(t), P(t) + Q(t)s)$, y además que los polinomios r, R son de grado 1. Al ser ψ la inversa de ϕ se cumple

$$\begin{aligned}
R(r(x)) &= x, && (4.23) \\
r(R(t)) &= t, && (4.24) \\
P(r(x)) + Q(r(x))(p(x) + q(x)y) &= y, && (4.25) \\
p(R(t)) + q(R(t))(P(t) + Q(t)s) &= s. && (4.26)
\end{aligned}$$

De la ecuación 4.25, tenemos $P(r(x)) + Q(r(x))p(x) + Q(r(x))q(x)y = y$. De ello obtenemos las igualdades

$$\begin{aligned}
P(r(x)) + Q(r(x))p(x) &= 0, && (4.27) \\
Q(r(x))q(x) &= 1. && (4.28)
\end{aligned}$$

De la ecuación 4.28 se concluye que Q y q son constantes, es decir son de la forma $q(x) = m_1$ y $Q(t) = m_2$. De 4.27 se tiene $P(r(x)) + Q(r(x))p(x) = 0$. Y al ser Q constante, se deduce $P(r(x)) = -m_2 p(x)$. Al reemplazar $t = r(x)$ y $s = p(x) + m_1 y$ en la ecuación de E_2 tenemos

$$\begin{aligned} & m_1^2 y^2 + a_1' \delta m_1 xy + y(2m_1 p(x) + a_1' \gamma m_1 + a_3' m_1) \quad = \\ & \delta^3 x^3 + x^2(3\delta^2\gamma + a_2'\delta^2) + x(3\delta\gamma^2 + 2a_2'\delta\gamma + a_4'\delta) + \gamma^3 + a_2'\gamma^2 + a_4'\gamma + a_6' - p^2(x) \\ & -a_1'\delta x p(x) - a_1'\gamma p(x) - a_3' p(x). \end{aligned}$$

Luego el grado de p es a lo más 1 pues la relación entre x e y debe ser precisamente aquella que define a E_1. De la misma manera obtenemos $deg(P) \leq 1$ y se concluye la igualdad $deg(P) = deg(p) = 1$. □

Ahora veremos más de cerca la forma de las isogenías si tomamos en consideración la característica del cuerpo $\mathbb{K}$.

Si el cuerpo $\mathbb{K}$ tiene característica distinta de 2, entonces dos curvas elípticas E_1 y E_2 pueden reducirse a través de transformaciones elementales a $E_1 : \ y^2 = x^3 + a_2 x^2 + a_4 x + a_6$ y $E_2 : \ s^2 = t^3 + a_2' t^2 + a_4' t + a_6'$.

Corolario 4.3. *Sean las curvas elípticas $E_1 : \ y^2 = x^3 + a_2 x^2 + a_4 x + a_6$ y $E_2 : \ s^2 = t^3 + a_2' t^2 + a_4' t + a_6'$ en un cuerpo de característica distinta de 2 y tomemos una isogenía $\phi : E_1 \to E_2$ entre ellas. Si ϕ es un isomorfismo, entonces la isogenía ϕ es de la forma $\phi(x, y) = (u(x), \lambda y)$, con inversa, digamos ψ, de la forma $\psi(t, s) = (U(t), \sigma s)$, acá u y U son de grado uno.*

Prueba. Si las curvas elípticas son isomorfas, por el corolario 4.2 existe una isogenía invertible $\phi : E_1 \to E_2$ de la forma $\phi(x, y) = (u(x), v(x) + \lambda y)$ con u de grado exactamente 1 y v a lo sumo de grado 1. Por el corolario 3.18 resulta que v es nulo y por lo tanto queda $\phi(x, y) = (u(x), \lambda y)$. De igual manera la inversa de ϕ, digamos $\psi : E' \to E$, toma la forma $\psi(t, s) = (U(t), \sigma s)$, donde U es polinomio de primer grado. □

A continuación estudiaremos la forma particular que deberán asumir las partes lineales en la isogenía del corolario anterior.

Teorema 4.4. *Sean las curvas elípticas $E_1 : \ y^2 = x^3 + a_2 x^2 + a_4 x + a_6$ y $E_2 : \ s^2 = t^3 + a_2' t^2 + a_4' t + a_6'$ y la isogenía $\phi : E_1 \to E_2$. La isogenía ϕ es un isomorfismo si y solo si está definido como $\phi(x, y) = (u^2 x + \beta, u^3 y)$, para algún $u \in \overline{\mathbb{K}}$.*

Prueba. Sean las curvas elípticas $E_1 : \ y^2 = x^3 + a_2 x^2 + a_4 x + a_6$ y $E_2 : \ s^2 = t^3 + a_2' t^2 + a_4' t + a_6'$ isomorfas mediante la isogenía $\phi : E_1 \to E_2$. Por el corolario anterior se tiene $t = \alpha x + \beta$ y $s = \lambda y$, expresión que reemplazaremos en la curva elíptica E_2 para obtener

$$\begin{aligned} \lambda^2 y^2 &= (\alpha x + \beta)^3 + a_2'(\alpha x + \beta)^2 + a_4'(\alpha x + \beta) + a_6' \\ &= \alpha^3 + 3\alpha^2\beta x^2 + 3\alpha\beta^2 x + \beta^3 + a_2'(\alpha^2 x^2 + 2\alpha\beta x + \beta^2) + a_4'(\alpha x + \beta) + a_6' \\ &= \alpha^3 x^3 + (3\alpha^2\beta + a_2'\alpha^2)x^2 + (3\alpha\beta + 2a_2'\alpha\beta + a_4'\alpha)x + a_2'\beta^2 + a_4'\beta + a_6'. \end{aligned}$$

De la curva $E_1:\ y^2 = x^3 + a_2x^2 + a_4x + a_6$ tenemos la relación

$$\lambda^2y^2 = \lambda^2x^3 + \lambda^2a_2x^2 + \lambda^2a_4x + \lambda^2a_6,$$

lo cual conduce a

$$\begin{aligned}
\lambda^2 &= \alpha^3 && (4.29)\\
a_2\lambda^2 &= 3\alpha^2\beta + a_2'\alpha^2 && (4.30)\\
a_4\lambda^2 &= 3\alpha\beta + 2a_2'\alpha\beta + a_4'\alpha && (4.31)\\
a_6\lambda^2 &= a_2'\beta^2 + a_4'\beta + a_6'. && (4.32)
\end{aligned}$$

De la ecuación 4.29 se tiene $w = \lambda^2 = \alpha^3$; luego, para $u = \dfrac{\lambda}{\alpha}$ se obtiene $w = u^6$, valor con el que se consigue $\lambda = u^3$ y $\alpha = u^2$. Así la isogenía ϕ toma la forma indicada. □

En el caso que las curvas elípticas tengan la presentación $E:\ y^2 = x^3 + a_4x + a_6$ y $E':\ s^2 = t^3 + a_4't + a_6'$, directamente de la ecuación 4.30 se deduce $3\alpha^2\beta = 0$ y ello implica que la isogenía ϕ toma la forma $\phi(x, y) = (u^2x, u^3y)$ para algún $u \in \overline{\mathbb{K}}$.

Ahora veamos la forma de las isogenías invertibles entre curvas elípticas definidas sobre un cuerpo de característica 2.

Teorema 4.5. *Sea $\mathbb{K}$ de característica 2 y las curvas elípticas*

$$\begin{aligned}
E_1(\mathbb{K}) &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\\
E_2(\mathbb{K}) &: s^2 + a_1'ts + a_3's = t^3 + a_2't^2 + a_4't + a_6'.
\end{aligned}$$

Si la isogenía $\phi : E_1 \to E_2$ es un isomorfismo, entonces necesariamente $\phi(x, y) = (u^2x + \delta, u^2\nu x + u^3y + \beta)$, para algún $u \in \overline{\mathbb{K}}$.

Prueba. Sea $\phi : E_1 \to E_2$ definida por $\phi(x, y) = (R_1(x, y), R_2(x, y))$, una isogenía con $R_1(x, y) = u(x)$ y $R_2(x, y) = v(x) + \lambda y$ como en el corolario 4.2, con inversa $\psi(s, t) = (U(t), V(t) + \tau s)$. Como $\phi[-(x, y)] = -\phi(x, y)$, observando la segunda componente, se tiene

$$\begin{aligned}
R_2(x, -y - a_1x - a_3) &= -R_2(x, y) - a_1'R_1(x, y) - a_3',\\
v(x) + \lambda(-y - a_1x - a_3) &= -(v(x) + \lambda y) - a_1'u(x) - a_3',\\
2v(x) + \lambda(-y - a_1x - a_3) &= -\lambda y - a_1'u(x) - a_3',\\
\lambda(y + a_1x + a_3) &= \lambda y + a_1'u(x) + a_3'.
\end{aligned}$$

Utilizamos $\lambda(y + a_1x + a_3) = \lambda y + a_1'u(x) + a_3'$, para expresar $s(s + a_1't + a_3')$ en términos de las variables x e y como sigue:

$$\begin{aligned}
s(s + a_1't + a_3') &= (v(x) + \lambda y)(v(x) + \lambda y + a_1't + a_3'),\\
&= (v(x) + \lambda y)(v(x) + \lambda(y + a_1x + a_3)),\\
&= (v(x) + \lambda y)(v(x) + \lambda y + \lambda a_1x + \lambda a_3),\\
&= v^2(x) + \lambda^2y^2 + \lambda v(x)(a_1x + a_3) + \lambda^2y(a_1x + a_3),\\
&= v^2(x) + \lambda v(x)(a_1x + a_3) + \lambda^2(y^2 + a_1xy + a_3y).
\end{aligned}$$

Al reemplazar $v(x) = \alpha x + \beta$ y tener en cuenta que se satisface $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, podemos representar $s(s + a_1't + a_3')$ como función de la variable x cual

$$\lambda^2x^3 + (\alpha^2 + \lambda\alpha a_1 + \lambda^2a_2)x^2 + (\lambda\alpha a_3 + \lambda\beta a_1 + \lambda^2a_4)x + (\beta^2 + \lambda a_3\beta + \lambda^2a_6).$$

Para expresar $t^3 + a_2't^2 + a_4't + a_6'$ en términos de la variable x, reemplazamos $t = r(x) = \gamma x + \delta$ para obtener

$$t^3 + a_2't^2 + a_4't + a_6' = \gamma^3x^3 + (\gamma^2\delta + a_2'\gamma^2)x^2 + (\gamma\delta^2 + a_4'\gamma)x + (\delta^3 + a_2'\delta^2 + a_4'\delta + a_6').$$

Como para la curva elíptica E_2 se tiene $s(s + a_1't + a_3') = t^3 + a_2't^2 + a_4't + a_6'$, las relaciones entre los coeficientes de las potencias de la variable x satisfacen

$$\begin{aligned}
\lambda^2 &= \gamma^3, && (4.33)\\
\alpha^2 + \lambda\alpha a_1 + \lambda^2a_2 &= \gamma^2(\delta + a_2'), && (4.34)\\
\lambda\alpha a_3 + \lambda\beta a_1 + \lambda^2a_4 &= \gamma\delta^2 + a_4'\delta, && (4.35)\\
\beta^2 + \lambda a_3\beta + \lambda^2a_6 &= \delta^3 + a_2'\delta^2 + a_4'\delta + a_6'. && (4.36)
\end{aligned}$$

De 4.33 se tiene $\lambda = u^3$ y $\gamma = u^2$ con $u = \dfrac{\lambda}{\gamma}$. Luego al reemplazar $\lambda = u^3$ y $\gamma = u^2$ en la expresión 4.34 concluimos $\alpha = u^2\nu$. En resumen, la isogenía queda expresada cual $\phi(x, y) = (u^2x + \delta, u^2\nu x + u^3y + \beta)$. □

Del teorema 4.4 y el teorema 4.5 podemos finiquitar la labor de obtener las isogenías de curvas elípticas sobre cuerpos de cualquier característica. La forma general de todas ellas es $\phi(x, y) = (u^2x + \delta, u^2\nu x + u^3y + \beta)$, donde ν, δ ó β pueden en algunos casos anularse.

Ejemplo 4.6. Consideremos las curvas elípticas $E_1 :\ y^2 = x^3 + 3x + 1$ y $E_2 :\ y^2 = x^3 + 243x + 729$. Estas son isomorfas sobre $\mathbb{Q}$, pues la función $\phi(x, y) : E_1 \mapsto E_2$ definida por $\phi(x, y) = (9x, 27y)$ es un isomorfimo.

Veamos ahora un atajo para determinar si dos curvas elípticas son isomorfas. Anteriormente habíamos definido el discriminante τ. Cuando se tenga $\tau \neq 0$, el **invariante j de la curva**, que denotamos por $j(E)$, viene dado por

$$j(E) = \frac{e_4^3}{\tau}.$$

Proposición 4.7. *Si las curvas elípticas*

$$\begin{aligned}
E_1(\mathbb{K}) &: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\\
E_2(\mathbb{K}) &: y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6'
\end{aligned}$$

son isomorfas mediante $\phi : E_2 \to E_1$ definido como $\phi(x', y') = (u^2x' + \delta, u^2\nu x' + u^3y' + \beta)$, entonces la relación que hay entre los coeficientes asociados de las curvas

E_1 y E_2 es la siguiente (para la definición ver capítulo 2):

$$\begin{aligned}
ua_1' &= a_1 + 2\nu,\\
u^2a_2' &= a_2 - \nu a_1 + 3\delta - \nu^2,\\
u^3a_3' &= a_3 + \delta a_1 + 2\beta,\\
u^4a_4' &= a_4 - \nu a_3 + 2\delta a_2 - (\beta + \delta\nu)a_1 + 3\delta^2 - 2\nu\beta,\\
u^6a_6' &= a_6 + \delta a_4 + \delta^2 a_2 + \delta^3 - \beta a_3 - \beta^2 - \delta\beta a_1,\\
u^2d_2' &= d_2 + 12\delta,\\
u^4d_4' &= d_4 + \delta d_2 + 6\delta^2,\\
u^6d_6' &= d_6 + 2\delta d_4 + \delta^2 d_2 + 4\delta^3,\\
u^8d_8' &= d_8 + 3\delta d_6 + 3\delta^2 d_2 + 3\delta^4,\\
u^4e_4' &= e_4,\\
u^6e_6' &= e_6,\\
u^{12}\tau' &= \tau.
\end{aligned}$$

Prueba. Como $(u^2x' + \delta, u^2\nu x' + u^3y' + \beta) \in E_1$ se tiene

$$\begin{aligned}
&(u^2\nu x' + u^3y' + \beta)^2 + a_1(u^2x' + \delta)(u^2\nu x' + u^3y' + \beta) + a_3(u^2\nu x' + u^3y' + \beta) \quad =\\
&(u^2x' + \delta)^3 + a_2(u^2x' + \delta)^2 + a_4(u^2x' + \delta) + a_6,\\
&u^4\nu^2(x')^2 + u^6(y')^2 + \beta^2 + 2u^5\nu x'y' + 2u^3\beta y' + 2u^2\nu\beta x' + a_1(u^4\nu(x')^2 + u^5x'y' +\\
&u^2\beta x' + u^2\delta\nu x' + u^3\delta y' + \delta\beta) + a_3u^2\nu x' + a_3u^3y' + a_3\beta \quad =\\
&u^6(x')^3 + 3u^4(x')^2\delta + 3u^2\delta^2x' + \delta^3 + a_2(u^4(x')^2 + 2u^2\delta x' + \delta^2) + a_4u^2x' + a_4\delta + a_6,\\
&u^6(y')^2 + (2u^5\nu + a_1u^5)x'y' + (2u^3\beta + a_1u^3\delta + a_3u^3)y' \quad =\\
&u^6(x')^3 - (u^4\nu^2 + a_1u^4\nu - 3u^4\delta - a_2u^4)(x')^2 + (3u^2\delta^2 + 2u^2\delta a_2 + a_4u^2 - 2u^2\nu\beta -\\
&a_1u^2\beta - a_1u^2\delta\nu - a_3u^2\nu)x' + \delta^3 + a_2\delta^2 + a_4\delta + a_6 - \beta^2 - a_1\delta\beta - a_3\beta.
\end{aligned}$$

Además $(x', y') \in E_2$ y con ello

$$\begin{aligned}
(y')^2 + a_1'x'y' + a_3'y' &= (x')^3 + a_2'(x')^2 + a_4' + a_6',\\
u^6(y')^2 + u^6a_1'x'y' + u^6a_3'y' &= u^6(x')^3 + u^6a_2'(x')^2 + u^6a_4' + u^6a_6'.
\end{aligned}$$

Deducimos las igualdades

$$\begin{aligned}
u^6a_1' &= 2u^5\nu + a_1u^5,\\
u^6a_2' &= -u^4\nu^2 - a_1u^4\nu + 3u^4\delta + a_2u^4,\\
u^6a_3' &= 2u^3\beta + a_1u^3\delta + a_3u^3,\\
u^6a_4' &= 3u^2\delta^2 + 2u^2\delta a_2 + a_4u^2 - 2u^2\nu\beta - a_1u^2\beta - a_1u^2\delta\nu - a_3u^2\nu,
\end{aligned}$$

y con ello

$$\begin{aligned}
ua_1' &= a_1 + 2\nu,\\
u^2a_2' &= a_2 - \nu a_1 + 3\delta - \nu^2,\\
u^3a_3' &= a_3 + \delta a_1 + 2\beta,\\
u^4a_4' &= a_4 - \nu a_3 + 2\delta a_2 - (\beta + \delta\nu)a_1 + 3\delta^2 - 2\nu\beta,\\
u^6a_6' &= a_6 + \delta a_4 + \delta^2 a_2 + \delta^3 - \beta a_3 - \beta^2 - \delta\beta a_1.
\end{aligned}$$

Mediante cálculos similares obtenemos

$$\begin{aligned} u^2 d_2' &= d_2 + 12\delta, \\ u^4 d_4' &= d_4 + \delta d_2 + 6\delta^2, \\ u^6 d_6' &= d_6 + 2\delta d_4 + \delta^2 d_2 + 4\delta^3, \\ u^8 d_8' &= d_8 + 3\delta d_6 + 3\delta^2 d_2 + 3\delta^4, \\ u^4 e_4' &= e_4, \\ u^6 e_6' &= e_6, \\ u^{12}\tau' &= \tau. \end{aligned}$$

□

De la proposición 4.7 tenemos entonces

$$j(E) = \frac{e_4^3}{\tau} = \frac{u^{12}(e_4')^3}{u^{12}\tau'} = \frac{(e_4')^3}{\tau'} = j(E').$$

Es decir, el invariante j no se modifica al ejecutar un cambio de variables; razón por la que lleva tal nombre.

Dos curvas elípticas pueden ser isomorfas sobre $\overline{\mathbb{K}}$, pero no se sabe a priori si pueden serlo sobre $\mathbb{K}$ o si solo son isomorfas sobre $\overline{\mathbb{K}}$ y no sobre $\mathbb{K}$. Para ello introduciremos el concepto de **twist de curvas elípticas**.

Sean las curvas elípticas $E_1(\mathbb{K})$ y $E_2(\mathbb{K})$. Decimos que son **twist** una de la otra si son $\overline{\mathbb{K}}$-isomorfas mas no $\mathbb{K}$-isomorfas.

Ejemplo 4.8. Sea la curva

$$E : y^2 = x^3 + 3x + 2$$

sobre $\mathbb{F}_5$. Ahora definamos la curva

$$E' : y^2 = x^3 + x + 4$$

La asignación $\psi(x, y) = (3x, \alpha y)$ es un isomorfismo de E sobre E', donde α es solución de $\alpha^2 = 2$. Se observa $\alpha \in \overline{\mathbb{F}}_5$, pero $\alpha \notin \mathbb{F}_5$.

Si E es una curva elíptica, pondremos $Aut(E)$ para referirnos al grupo de los automorfismos de E, es decir, los isomorfismos de E en E.

Ejemplo 4.9. Consideremos la curva elíptica $E : y^2 = x^3 + 2$ sobre el cuerpo $\mathbb{F}_7$. La asignación $\rho(x, y) = (u^2 x, 6y)$ es un automorfismo, donde $u^3 = 6$. Se observa $u \in \overline{\mathbb{F}}_7$, pero $u \notin \mathbb{F}_7$.

Observación 4.10. Si las curvas elípticas E_1 y E_2 son isomorfas sobre $\overline{\mathbb{K}}$, entonces tendremos $Aut(E_1) \equiv Aut(E_2)$. Más adelante se verá que $j(E_1) = j(E_2)$ implica que E_1 y E_2 son isomorfas, con lo cual podemos concluir que $j(E_1) = j(E_2)$ implica $Aut(E_1) \equiv Aut(E_2)$.

Veremos a continuación algunas propiedades del invariante j, de los twist y de los automorfismos de las curvas elípticas $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ al tener en consideración la característica del cuerpo $\mathbb{K}$.

4.1 Curvas elípticas en característica 2

Por lo visto en la sección 2.2, si $a_1 = 0$, la curva elíptica E es isomorfa a

$$E' : y^2 + a_3 y = x^3 + b_4 x + b_6.$$

En este caso, tenemos $d_2' = d_4' = 0$, $d_6' = a_3^2$, $e_4' = 0$, $\tau' = a_3^4$ y además $j' = 0$.

Si $a_1 \neq 0$, tenemos que la curva E es isomorfa a

$$E' : y^2 + xy = x^3 + a_2' x^2 + a_6';$$

acá se tiene $d_2' = 1$, $d_4' = d_6' = 0$, $e_4' = 1$, $\tau' = -a_6' = \dfrac{\tau}{a_1^{12}}$ y además $j' = \dfrac{a_1^{12}}{\tau}$.

Ejemplo 4.11. Las curvas elípticas $E_1 : y^2 + y = x^3 + x$, $E_2 : y^2 + y = x^3 + 1$, $E_3 : y^2 + y = x^3 + x + 1$, definidas sobre el cuerpo $\mathbb{F}_2$, cumplen $j(E_1) = j(E_2) = j(E_3) = 0$.

Ejemplo 4.12. Las curvas elípticas $E_4 : y^2 + xy = x^3 + x^2 + 1$, $E_5 : y^2 + xy = x^3 + \alpha$, $E_6 : y^2 + xy = x^3 + \alpha x^2 + 1 + \alpha$, sobre el cuerpo $\mathbb{F}_4 = \{0, 1, \alpha, 1 + \alpha\}$, cumplen $j(E_4) = 1$, $j(E_5) = 1 + \alpha$, $j(E_6) = \alpha$; acá $\alpha^2 + \alpha + 1 = 0$

Si el invariante j es cero, entonces $a_1 = 0$, pues de lo contrario se tendría $j = \dfrac{a_1^{12}}{\tau}$, lo cual es absurdo. Es decir, $j = 0$ es equivalente a $a_1 = 0$

En los ejemplos 4.11 y 4.12, se comprobó que para cualquier elemento del cuerpo $\mathbb{F}_4$ existen curvas elípticas cuyos invariantes son dichos valores. Esto se generaliza en la siguiente proposición a cualquier cuerpo de característica 2.

Proposición 4.13. *Para todo $j \in \mathbb{K}$, existe una curva elíptica E con $j(E) = j$.*

Prueba. Para el caso $j = 0$, consideramos la curva elíptica $E : y^2 + y = x^3 + x + 1$, la cual cumple $j(E) = 0 = j$. Si $j \neq 0$ la curva elíptica $E : y^2 + xy = x^3 + x^2 - \dfrac{1}{j}$ satisface $j(E) = j$. □

Ejemplo 4.14. Sean las curvas elípticas $E_1 : y^2 + y = x^3 + x$, $E_3 : y^2 + y = x^3 + x + 1$ sobre $\mathbb{F}_2$. Definamos $\phi : E_3 \to E_1$ como $\phi(x, y) = (x, y + \alpha)$, donde $\alpha \in \overline{\mathbb{F}}_2$ es solución de $\alpha^2 + \alpha = 1$. Para $(x, y) \in E_3 \cap L$, donde L es una recta de ecuación $y = mx + b$, tenemos $y + \alpha = mx + b + \alpha$, es decir ϕ respeta la operación de grupo. Como la homogenización de ϕ es $\phi[x : y : z] = [x : y + \alpha z : z]$, se tiene $\phi(\mathcal{O}) = [0 : 1 : 0] = \mathcal{O}$. Además ϕ está bien definida, pues $(x, y) \in E_3$ equivale a cualquiera de las identidades

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

es decir, tendremos $(x, y + \alpha) \in E_1$. Concluimos que ϕ es un isomorfismo con inversa $\phi^{-1}(x, y) = (x, y - \alpha x)$.

Ejemplo 4.15. Sea la curva elíptica $E_2 : y^2 + y = x^3 + 1$, definida sobre el cuerpo $\mathbb{F}_2$. Definamos $\phi : E_2 \to E_2$ como $\phi(x, y) = (x + 1, x + y + \alpha)$, $\alpha \in \overline{\mathbb{F}}_2$ solución de $\alpha^2+\alpha = 1$. Para $(x, y) \in E \cap L$, donde L es una recta de ecuación $y = mx+b$, tenemos $y+\alpha = mx+b+\alpha$, es decir ϕ respeta la operación de grupo. Como la homogenización de ϕ es $\phi[x : y : z] = [x+z : x+y+\alpha z : z]$, se tiene $\phi(\mathcal{O}) = [0 : 1 : 0] = \mathcal{O}$. Además, está bien definida pues $(x, y) \in E_2$ es equivalente a cualquiera de las siguientes identidades

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

es decir, a $(x + 1, x + y + \alpha) \in E_2$. Concluimos que ϕ es un isomorfismo con inversa $\phi^{-1}(x, y) = (x - 1, y - x - \alpha x + 1)$.

En los ejemplos anteriores hemos manipulado curvas elípticas isomorfas de la forma $E : y^2+a_3y = x^3+b_4x+b_6$. El siguiente paso es clasificar dichos isomorfismos. Ello lo haremos en el siguiente teorema.

Teorema 4.16. *Sean las curvas elípticas $E : y^2 + b_3y = x^3 + b_4x + b_6$, $E' : y^2 + u^{-3}b_3y = x^3+u^{-4}(\nu^4+b_4-b_3\nu)x+u^{-6}(b_4\nu^2+\nu^6+b_6-\beta^2-b_3\beta)$, con $u \in \overline{\mathbb{K}}^*$ y $\beta, \delta \in \overline{\mathbb{K}}$. La función $\phi : E'(\overline{\mathbb{K}}) \to E(\overline{\mathbb{K}})$, definida por $\phi(x, y) = (u^2x + \nu^2, u^2\nu x + u^3y + \beta)$, es un isomorfismo de grupos.*

Prueba. Sean $u \in \overline{\mathbb{K}}^*$ y $\beta, \delta \in \overline{\mathbb{K}}$. Tenemos que $(x, y) \in E'$ es equivalente a cualquiera de las siguiente identidades

$$y^2 + b_3u^{-3}y = x^3 + u^{-4}(\nu^4 + b_4 - b_3\nu)x + u^{-6}(b_4\nu^2 + \nu^6 + b_6 - \beta^2 - b_3\beta),$$

$$u^6y^2 + b_3u^3y = u^6x^3 + u^2(\nu^4 + b_4 - b_3\nu)x + b_4\nu^2 + \nu^6 + b_6 - \beta^2 - b_3\beta,$$

$$u^4\nu^2x^2+u^6y^2+\beta^2+b_3u^2\nu x+b_3u^3y+b_3\beta = u^6x^3+u^4\nu^2x^2+u^2\nu^4x+\nu^6+b_4u^2x+b_4\nu^2+b_6,$$

$$(u^2\nu x + u^3y + \beta)^2 + b_3(u^2\nu x + u^3y + \beta) = (u^2x + \nu^2)^3 + b_4(u^2x + \nu^2) + b_6,$$

es decir, a $(u^2x + \nu^2, u^2\nu x + u^3y + \beta) \in E$. Además la función inversa está definida por $\phi(x, y) = (u^{-2}(x - \nu^2), u^{-3}(y - \nu x + \nu^3 - \beta))$. En coordenadas proyectivas tenemos

$$\begin{array}{rccl} \phi : & E'(\overline{K}) & \to & E(\overline{K}) \\ & [x : y : z] & \mapsto & [u^2x + \nu^2z : u^2\nu x + u^3y + \beta z : z] \end{array}$$

Por ejemplo se tiene

$$\phi(\mathcal{O}) = \phi([0 : 1 : 0]) = [0 : u^3 : 0] = [0 : 1 : 0] = \mathcal{O}.$$

Por último, tenemos la recta L de ecuación $y = mx + b$. Si $(x, y) \in L \cap E'$ y $\phi(x, y) = (\overline{x}, \overline{y})$, tenemos $y = mx + b$, $\overline{x} = u^2x + \nu^2$, $\overline{y} = u^2\nu x + u^3y + \beta$. Además se cumple $\overline{y} = (\nu + um)\overline{x} - \nu^2(\nu + um) + u^3b + \beta$. Por lo tanto, ϕ lleva rectas en rectas y por ende respeta la operación de grupo. En conclusión, ϕ es un isomorfismo. □

Teorema 4.17. *Sean las curvas elípticas $E' : y^2 + b'_3y = x^3 + b'_4x + b'_6$, $E : y^2 + b_3y = x^3 + b_4x + b_6$. Si $\phi : E' \to E$ es un isomorfismo definido por $\phi(x, y) = (u^2x + \nu^2, u^2\nu x + u^3y + \beta)$ para algún $u \in \overline{\mathbb{K}}^*$, $\beta, \nu \in \overline{\mathbb{K}}$, entonces $b'_3 = u^{-3}b_3$, $b'_4 = u^{-4}(\nu^4 + b_4 - b_3 + \nu)$ y $b'_4 = u^{-6}(b_4\nu^2 + \nu^6 + b_6 - \beta^2 - b_3\beta)$.*

Prueba. De la proposición 4.7, con $\delta = \nu^2$, tenemos $b_3' = u^{-3}b_3$, $b_4' = u^{-4}(\nu^4 + b_4 - b_3 + \nu)$ y $b_4' = u^{-6}(b_4\nu^2 + \nu^6 + b_6 - \beta^2 - b_3\beta)$. □

Ejemplo 4.18. Sea la curva elíptica $E_7 : y^2 + xy = x^3 + (1+\alpha)x^2 + 1 + \alpha$ sobre el cuerpo $\mathbb{F}_4$; acá $\alpha^2 + \alpha + 1 = 0$. Definamos $\phi : E_7 \to E_6$ como $\phi(x, y) = (x, y + \alpha x)$. Para $(x, y) \in E_7 \cap L$, donde L es una recta de ecuación $y = mx + b$, tenemos $\alpha x + y = (m + \alpha)x + b$, es decir ϕ respeta la operación de grupo. Como la homogenización de ϕ es $\phi[x : y : z] = [x : \alpha x + y : z]$, se tiene $\phi(\mathcal{O}) = [0 : 1 : 0] = \mathcal{O}$. Además, ϕ está bien definida, pues tener $(x, y) \in E_7$ es equivalente a

$$\begin{aligned} y^2 + xy &= x^3 + (1+\alpha)x^2 + 1 + \alpha, \\ \alpha^2x^2 + y^2 + \alpha x^2 + xy &= x^3 + \alpha x^2 + 1 + \alpha, \\ (y + \alpha x)^2 + x(y + \alpha x) &= x^3 + \alpha x^2 + 1 + \alpha, \end{aligned}$$

es decir, a $(x, y + \alpha x) \in E_6$. Concluimos que ϕ es un isomorfismo con inversa $\phi^{-1}(x, y) = (x, y - \alpha x)$.

Ejemplo 4.19. Sea la curva elíptica $E_8 : y^2 + xy = x^3 + x^2 + \alpha$ sobre el cuerpo $\mathbb{F}_4$; acá $\alpha^2 + \alpha + 1 = 0$. Definamos $\phi : E_8 \to E_5$ como $\phi(x, y) = (x, (1+\alpha)x + y)$. Para $(x, y) \in E_7 \cap L$, donde L es una recta de ecuación $y = mx + b$, tenemos $\alpha x + y = (m + \alpha)x + b$, es decir ϕ respeta la operación de grupo. Como la homogenización de ϕ es $\phi[x : y : z] = [x : (1+\alpha)x + y : z]$, se tiene $\phi(\mathcal{O}) = [0 : 1 : 0] = \mathcal{O}$. Además, está bien definida, pues tener $(x, y) \in E_8$ es equivalente a

$$\begin{aligned} y^2 + xy &= x^3 + \alpha, \\ (1+\alpha)^2x^2 + y^2 + (1+\alpha)x^2 + xy &= x^3 + x^2 + \alpha, \\ ((1+\alpha)x + y)^2 + x((1+\alpha)x + y) &= x^3 + x^2 + \alpha, \end{aligned}$$

es decir, a $(x, (1+\alpha)x + y) \in E_5$. Concluimos que ϕ es un isomorfismo con inversa ϕ^{-1} definida por $\phi^{-1}(x, y) = (x, y - \alpha x)$.

De los ejemplos anteriores observamos que las curvas elípticas E_6 y E_7 son isomorfas mediante $\phi : E_7 \to E_6$ dada por $\phi(x, y) = (x, y + \alpha x)$. Un caso similar sucede entre las curvas elípticas E_8 y E_5 gracias al isomorfismo $\phi : E_8 \to E_5$ definido por $\phi(x, y) = (x, (1+\alpha)x + y)$. En el siguiente teorema estableceremos condiciones rápidas para reconocer cuándo dos curvas elípticas del tipo $E : y^2 + xy = x^3 + b_2x^2 + b_6$, definidas sobre un cuerpo de característica 2, son isomorfas.

Teorema 4.20. *Sean las curvas elípticas $E : y^2 + xy = x^3 + b_2x^2 + b_6$, $E' : y^2 + xy = x^3 + (b_2 - \nu - \nu^2)x^2 + b_6$, con $\nu \in \overline{\mathbb{K}}$. La función $\phi : E'(\overline{\mathbb{K}}) \to E(\overline{\mathbb{K}})$, definida por $\phi(x, y) = (x, \nu x + y)$, es un isomorfismo de grupos.*

Prueba. Tenemos que $(x, y) \in E'$ es equivalente a

$$\begin{aligned} y^2 + xy &= x^3 + (b_2 - \nu - \nu^2)x^2 + b_6, \\ \nu^2x^2 + y^2 + \nu x^2 + xy &= x^3 + b_2x^2 + b_6, \\ (\nu x + y)^2 + x(\nu x + y) &= x^3 + b_2x^2 + b_6, \end{aligned}$$

es decir, a $(x, \nu x + y) \in E$. Además, la función inversa está definida por $\phi(x, y) = (x, y - \nu x)$. En coordenadas proyectivas tenemos

$$\begin{array}{rccc} \phi: & E'(\overline{K}) & \to & E[\overline{K}] \\ & [x:y:z] & \mapsto & [x:\nu x+y:z] \end{array}$$

Para $\mathcal{O} = [0:1:0]$, se tiene

$$\phi(\mathcal{O}) = \phi([0:1:0]) = [0:1:0] = \mathcal{O}.$$

Por último, sea la recta L de ecuación $y = mx+b$. Si $(x, y) \in L \cap E'$ y $\phi(x, y) = (\overline{x}, \overline{y})$, tenemos $y = mx + b$, $\overline{x} = x$, $\overline{y} = \nu x + y$. Además $\overline{y} = (\nu + m)\overline{x} + b$. Por lo tanto, ϕ lleva rectas en rectas y por ello respeta la operación de grupo. En conclusión, ϕ es un isomorfismo. □

Teorema 4.21. *Sean las curvas elípticas $E' : y^2 + xy = x^3 + b_2'x^2 + b_6'$, $E : y^2 + xy = x^3 + b_2x^2 + b_6$. Si $\phi : E' \to E$ es un isomorfismo definido por $\phi(x, y) = (x, \nu x + y)$ para algún $\nu \in \overline{\mathbb{K}}$, entonces $b_2' = b_2 + \nu + \nu^2$ y $b_6' = b_6$.*

Prueba. De la proposición 4.7, para $u = 1$, $\delta = 0$, $\beta = 0$, tenemos $b_2' = b_2 - \nu - \nu^2$ y $b_6' = b_6$. □

Los lemas que se enuncian a continuación permitirán a la postre demostrar que dos curvas elípticas son isomorfas cuando tienen el mismo invariante j.

Lema 4.22. *Toda curva elíptica $E' : y^2 + c_3y = x^3 + c_4x + c_6$ es isomorfa a $E : y^2 + y = x^3 + x + 1$.*

Prueba. Como E' es una curva elíptica y $\tau = c_3^4$, tenemos $c_3 \neq 0$. Sean $u, \nu, \beta \in \overline{\mathbb{K}}$ valores que satisfacen $c_3 = u^{-3}$, $c_4 = u^{-4}(\nu^4 + \nu)$, $c_6 = u^{-6}(v^2 + v^6 + 1 - \beta^2 - \beta)$. Por los teoremas 4.16 y 4.17, la función $\phi : E' \to E$, definida por $\phi(x, y) = (u^2x + \nu^2, u^2\nu x + u^3y + \beta)$, es un isomorfismo. □

Lema 4.23. *Toda curva elíptica $E' : y^2 + xy = x^3 + c_2x^2 + c_6$ con invariante j es isomorfa a $E : y^2 + xy = x^3 + x^2 - \dfrac{1}{j}$.*

Prueba. Observamos que las curvas elípticas E' y E tiene el mismo invariante j. La isogenía $\phi : E' \to E$ definida por $\phi(x, y) = (x, \nu x + y)$, donde $\nu \in \overline{\mathbb{K}}$ es una solución de $c_2 = 1 + \nu + \nu^2$, es un isomorfismo por los teoremas 4.20 y 4.21. □

Del ejemplo 4.14 concluimos que E_1 es isomorfa a E_3. Y del ejemplo 4.15, se tiene un automorfismo de E_2. Lo coincidente es que tienen el mismo invariante igual a 0.

Ahora bien, las curvas elípticas $E_7 : y^2+xy = x^3+(1+\alpha)x^2+1+\alpha$ y $E_6 : y^2+xy = x^3 + \alpha x^2 + 1 + \alpha$ cumplen $j(E_7) = j(E_6) = \alpha$ y por el ejemplo 4.18 son isomorfas. Además las curvas elípticas $E_8 : y^2 + xy = x^3 + x^2 + \alpha$ y $E_5 : y^2 + xy = x^3 + \alpha$ tienen el mismo invariante j, dado por $j(E_8) = j(E_5) = 1 + \alpha$, y por el ejemplo 4.19 también son isomorfas.

A partir de las observaciones anteriores, podemos vislumbrar el siguiente resultado que establece que dos curvas elípticas son isomorfas si y solo si tienen el mismo invariante j.

Teorema 4.24. *Dos curvas elípticas de característica* 2 *son isomorfas sobre* $\overline{\mathbb{K}}$ *si y solo si tienen el mismo invariante* j*.*

Prueba. Tomamos dos curvas elípticas E y E' con invariantes $j(E)$ y $j(E')$ respectivamente. Si E y E' son isomorfas, entonces por la proposición 4.7 tienen el mismo invariante j.

Ahora supongamos $j(E) = j(E')$. Tenemos dos casos. Si las curvas elípticas son de la forma $E : y^2 + a_3y = x^3 + b_4x + b_6$, $E' : y^2 + a_3'y = x^3 + b_4'x + b_6'$, entonces por el lema 4.22 dichas curvas son isomorfas a $H : y^2 + y = x^3 + x + 1$. En el caso que tengan la forma $E : y^2 + xy = x^3 + c_2x^2 + c_6$, $E' : y^2 + xy = x^3 + c_2'x^2 + c_6'$, por el lema 4.23 las curvas son isomorfas a cierto $F : y^2 + xy = x^3 + x^2 - \dfrac{1}{j}$. En ambos casos, concluimos que E y E' son isomorfas. □

Ejemplo 4.25. Sean las curvas elípticas $E : y^2 + xy = x^3 + x^2 + 1$ y $E' : y^2 + xy = x^3 + 1$, definidas sobre $\mathbb{F}_2$. Como $j(E) = j(E') = 1$, por el teorema 4.24, son isomorfas y por los teoremas 4.20 y 4.21, el isomorfismo $\phi : E' \to E$ está definido por $\phi(x, y) = (x, \nu x + y)$ donde $0 = 1 - \nu - \nu^2$, $\nu \in \overline{\mathbb{F}}_2$. Notemos que el isomorfismo se define apenas sobre $\overline{\mathbb{F}}_2$, pues $\nu \notin \mathbb{F}_2$.

Ejemplo 4.26. Las curvas elípticas $E : y^2 + xy = x^3 + x^2 + \alpha$ y $E' : y^2 + xy = x^3 + (1+\alpha)x^2 + \alpha$, definidas sobre $\mathbb{F}_4$ son isomorfas, pues $j(E) = j(E') = 1 + \alpha$. Por el teorema 4.24, estas son isomorfas y por los teoremas 4.20 y 4.21, el isomorfismo $\phi : E' \to E$ está definido por $\phi(x, y) = (x, \nu x + y)$ cuando $1 + \alpha = 1 - \nu - \nu^2$, y $\alpha \neq 0$, pues E es curva elíptica. Luego el isomorfismo es sobre $\overline{\mathbb{F}}_4$, pues $\nu \notin \mathbb{F}_4$.

De los ejemplos anteriores, podemos adelantar la siguiente observación.

Observación 4.27. Todo twist de la curva elíptica $E : y^2 + xy = x^3 + b_2x^2 + b_6$ es de la forma $E' : y^2 + xy = x^3 + (b_2 - \nu - \nu^2)x^2 + b_6$, con $\nu + \nu^2 \in \mathbb{K}$ siempre que $\nu \notin \mathbb{K}$.

Finalmente vamos a determinar el orden del grupo de los automorfismos cuando la curva elíptica adopta la forma $E : y^2 + b_3y = x^3 + b_4x + b_6$ ó $E : y^2 + xy = x^3 + b_2x^2 + b_6$.

Teorema 4.28. *El grupo de automorfismo* $Aut(E)$ *para la curva elíptica* $E : y^2 + b_3y = x^3 + b_4x + b_6$ *tiene* 24 *elementos.*

Prueba. Sea $\phi : E \to E$ un automorfismo que por los teoremas 4.16 y 4.17 está definido por $\phi(x, y) = (u^2x + \nu^2, u^2\nu x + u^3y + \beta)$. De la proposición 4.7, para $\delta = \nu^2$, se tiene

$$\begin{aligned} b_3 &= u^{-3}b_3, \\ b_4 &= u^{-4}(\nu^4 + b_4 - b_3 + \nu), \\ b_6 &= u^{-6}(b_4\nu^2 + \nu^6 + b_6 - \beta^2 - b_3\beta). \end{aligned}$$

Observamos de la primera ecuación que u puede tomar tres valores. Para cada uno de estos tres valores que tome u se tiene de la segunda ecuación que ν puede tomar cuatro valores. Y a partir de los valores que tomen u y ν, β toma dos valores. Es decir, en total existen 24 automorfismos. □

Ejemplo 4.29. Los automorfismos de la curva elíptica $E : y^2 + y = x^3 + x + 1$, están dados por $\phi(x, y) = (u^2x + \nu^2, u^2\nu x + u^3y + \beta)$ con las constantes sujetas a $1 = u^{-3}$, $1 = u^{-4}(\nu^4 + \nu)$, $1 = u^{-6}(\nu^2 + \nu^6 + 1 - \beta^2 - \beta)$. Consideremos las raíces de $x^3 = 1$, digamos 1, α y α^2, con α solución de $x^2 + x = 1$, una raíz de $x^4 + x = 1$ digamos κ, y una raíz de $x^4 + x = \kappa^3$ digamos λ. Con ello tenemos los isomorfismos

$$\begin{aligned}
\phi_1(x,y) &= (x+\kappa^2, \kappa x + y + \lambda),\\
\phi_2(x,y) &= (x+\kappa^2, \kappa x + y + 1 + \lambda),\\
\phi_3(x,y) &= (x+1+\kappa^2, (1+\kappa)x + y + \lambda^4),\\
\phi_4(x,y) &= (x+1+\kappa^2, (1+\kappa)x + y + 1 + \lambda^4),\\
\phi_5(x,y) &= (x+\kappa^4, \kappa^2 x + y + \lambda^2),\\
\phi_6(x,y) &= (x+\kappa^4, \kappa^2 x + y + 1 + \lambda^2),\\
\phi_7(x,y) &= (x+1+\kappa^4, (1+\kappa^2)x + y + \kappa),\\
\phi_8(x,y) &= (x+1+\kappa^4, (1+\kappa^2)x + y + 1 + \kappa),\\
\phi_9(x,y) &= (\alpha^2 x + \alpha^2\kappa^2, \kappa x + y + \alpha^2\kappa^3),\\
\phi_{10}(x,y) &= (\alpha^2 x + \alpha^2\kappa^2, \kappa x + y + 1 + \alpha^2\kappa^3),\\
\phi_{11}(x,y) &= (\alpha^2 x + \alpha^2(1+\kappa^2), (1+\kappa)x + y + \alpha^2(1+\kappa)^3),\\
\phi_{12}(x,y) &= (\alpha^2 x + \alpha^2(1+\kappa^2), (1+\kappa)x + y + 1 + \alpha^2(1+\kappa)^3),\\
\phi_{13}(x,y) &= (\alpha^2 x + \alpha^2\kappa^4, \kappa^2 x + y + \alpha^2\kappa^6),\\
\phi_{14}(x,y) &= (\alpha^2 x + \alpha^2\kappa^4, \kappa^2 x + y + 1 + \alpha^2\kappa^6),\\
\phi_{15}(x,y) &= (\alpha^2 x + \alpha^2(1+\kappa^4), (1+\kappa^2)x + y + \kappa + \alpha\kappa^2 + \alpha^2(1+\alpha)^3),\\
\phi_{16}(x,y) &= (\alpha^2 x + \alpha^2(1+\kappa^4), (1+\kappa^2)x + y + 1 + \kappa + \alpha\kappa^2 + \alpha^2(1+\alpha)^3),\\
\phi_{17}(x,y) &= (\alpha x + \alpha\kappa^2, \kappa x + y + \alpha\kappa^3),\\
\phi_{18}(x,y) &= (\alpha x + \alpha\kappa^2, \kappa x + y + 1 + \alpha\kappa^3),\\
\phi_{19}(x,y) &= (\alpha x + \alpha(1+\kappa^2), (1+\kappa)x + y + \alpha\kappa^3 + \alpha^2\kappa^2 + \alpha^2\kappa),\\
\phi_{20}(x,y) &= (\alpha x + \alpha(1+\kappa^2), (1+\kappa)x + y + 1 + \alpha\kappa^3 + \alpha^2\kappa^2 + \alpha^2\kappa),\\
\phi_{21}(x,y) &= (\alpha x + \alpha\kappa^4, \kappa^2 x + y + \alpha\kappa^2 + \alpha\kappa^3),\\
\phi_{22}(x,y) &= (\alpha x + \alpha\kappa^4, \kappa^2 x + y + 1 + \alpha\kappa^2 + \alpha\kappa^3),\\
\phi_{23}(x,y) &= (\alpha x + \alpha(1+\kappa^4), (1+\kappa^2)x + y + \alpha^2\kappa^6 + \kappa),\\
\phi_{24}(x,y) &= (\alpha x + \alpha(1+\kappa^4), (1+\kappa^2)x + y + 1 + \alpha^2\kappa^6 + \kappa).
\end{aligned}$$

Teorema 4.30. *El grupo de automorfismo $Aut(E)$ para la curva elíptica $E : y^2 + xy = x^3 + b_2x^2 + b_6$ tiene 2 elementos.*

Prueba. Sea $\phi : E \to E$ un automorfismo que por los teoremas 4.20 y 4.21 está dado por $\phi(x, y) = (x, \nu x + y)$. De la observación 4.6, para $u = 1$, $\delta = 0$, $\beta = 0$, se tiene

$$\begin{aligned}
b_2 &= b_2 + \nu + \nu^2,\\
b_6 &= b_6.
\end{aligned}$$

Observamos que ν solo puede tomar valores 0 o 1, es decir, existen apenas 2 automorfismos. □

A modo de ejemplo analicemos los automorfismos de la curva elíptica $E : y^2 + xy = x^3 + x^2 + 1$, para lo cual debemos tener en cuenta los teoremas 4.20 y 4.21. Sea $\phi : E \to E$ definido por $\phi(x, y) = (x, \nu x + y)$ sujeto a $1 = 1 + \nu + \nu^2$. Tenemos que los automorfismos de la curva elíptica $E : y^2 + xy = x^3 + x^2 + 1$ son precisamente

$$\begin{aligned} \phi_1(x, y) &= (x, y), \\ \phi_2(x, y) &= (x, x + y). \end{aligned}$$

4.2 Curvas elípticas en característica 3

Toda curva elíptica definida sobre un cuerpo $\mathbb{K}$ de característica 3 es reducida a la forma $E : y^2 = x^3 + b_2x^2 + b_4x + b_6$.

Si $b_2 \neq 0$, mediante el cambio $x = x' + \dfrac{b_4}{b_2}$ se tiene

$$E : y^2 = (x')^3 + b_2'(x')^2 + b_6',$$

donde $b_2' = b_2$, $b_6' = \dfrac{b_4^3 + 2b_4^2b_2^2 + b_6b_2^3}{b_2^3}$, $d_2' = 4b_2' = b_2'$, $d_6' = 4b_6' = b_6'$, $d_8' = 4b_2'b_6' = b_2'b_6'$, $e_4' = (b_2')^2$, $\tau' = -(b_2')^3b_6'$ y $j = -\dfrac{(b_2')^3}{b_6'}$.

Si $b_2 = 0$, tenemos

$$E : y^2 = x^3 + b_4x + b_6,$$

donde $d_2 = 0$, $d_4 = 2b_4$, $d_6 = 4b_6$, $e_4 = 0$, $\tau = -8(2b_4)^3 = -b_4$ y $j = 0$.

Ejemplo 4.31. Para las curvas elípticas $E_1 : y^2 = x^3 + x^2 + 1$, $E_2 : y^2 = x^3 + x^2 + 2$, $E_3 : y^2 = x^3 + 2x^2 + 1$, $E_4 : y^2 = x^3 + 2x^2 + 2$, definidas sobre $\mathbb{F}_3$, se tiene $j(E_1) = 2$, $j(E_2) = 1$, $j(E_3) = 1$, $j(E_4) = 2$.

Ejemplo 4.32. Las curvas elípticas $E_5 : y^2 = x^3 + x$, $E_6 : y^2 = x^3 + x + 1$, $E_7 : y^2 = x^3 + x + 2$, $E_8 : y^2 = x^3 + 2x$, $E_9 : y^2 = x^3 + 2x + 1$, $E_{10} : y^2 = x^3 + 2x + 2$, definidas sobre $\mathbb{F}_3$, tienen todos invariante j igual a 0.

Observación 4.33. Si el invariante j es cero, tenemos $b_2 = 0$. Para el caso cuando $j \neq 0$, este se expresa como $-\dfrac{b_2^3}{b_6}$, con lo cual $b_2 \neq 0$.

Ejemplo 4.34. Las curvas elípticas $E_{11} : y^2 = x^3 - \alpha x^2 + 1$, $E_{12} : y^2 = x^3 - (1 + \alpha)x^2 + 1$, $E_{13} : y^2 = x^3 - (2 + \alpha)x^2 + 1$, $E_{14} : y^2 = x^3 + \alpha^2x^2 - 1$, $E_{15} : y^2 = x^3 + (1 + \alpha)^2x^2 - 1$, $E_{16} : y^2 = x^3 + (2 + \alpha)^2x^2 - 1$, definidas sobre $\mathbb{F}_9$, con α solución de $\alpha^3 - \alpha = 1$, satisfacen $j(E_{11}) = 1 + \alpha$, $j(E_{12}) = 2 + \alpha$, $j(E_{13}) = \alpha$, $j(E_{14}) = (1 + \alpha)^2$, $j(E_{15}) = (2 + \alpha)^2$, $j(E_{16}) = \alpha^2$.

Gracias a los ejemplos anteriores, observamos que para cada elemento de $\mathbb{F}_9$, existen curvas elípticas cuyo invariante j toma el valor correspondiente. Esto es un caso particular de la siguiente propiedad.

Proposición 4.35. *Si $j \in \mathbb{K}$, entonces existe una curva elíptica E tal que $j(E) = j$.*

Prueba. Para el caso $j = 0$, tomamos la curva elíptica $E : y^2 = x^3 + x + 1$ que cumple $j(E) = 0 = j$. Para $j \neq 0$ la curva elíptica $E : y^2 = x^3 + x^2 - \frac{1}{j}$ cumple $j(E) = j$. □

Ejemplo 4.36. Sean las curvas elípticas $E_5 : y^2 = x^3 + x$, $E_6 : y^2 = x^3 + x + 1$ sobre el cuerpo $\mathbb{F}_3$. Definamos $\phi : E_6 \to E_5$ como $\phi(x, y) = (x+2, y)$. Para $(x, y) \in E_6 \cap L$, donde L es una recta de ecuación $y = mx + b$, tenemos $y = m(x + 2) + b - 2m$, es decir ϕ respeta la operación de grupo. Con la homogenización de ϕ dada por $\phi([x : y : z]) = [x + 2z : y : z]$, se tiene $\phi([\mathcal{O}]) = [0 : 1 : 0] = \mathcal{O}$. Además, está bien definida, pues $(x, y) \in E_6$ es equivalente a tener

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

es decir, a $(x + 2, y) \in E_5$. Concluimos que ϕ es un isomorfismo, con inversa $\phi^{-1}(x, y) = (x + 1, y)$.

Ejemplo 4.37. Sean las curvas elípticas $E_1 : y^2 = x^3+x^2+1$, $E_4 : y^2 = x^3+2x^2+x$, sobre el cuerpo $\mathbb{F}_3$. Definamos $\phi : E_4 \to E_1$, como $\phi(x, y) = (u^2x, u^3y)$ con $u \in \overline{\mathbb{F}}_3$ raíz de $x^2 = 2$. Para $(x, y) \in E_4 \cap L$, donde L es una recta de ecuación $y = mx + b$, tenemos $u^3y = um(u^2x) + u^3b$, es decir ϕ respeta la operación de grupo. Como la homogenización de ϕ es dada por $\phi([x : y : z]) = [u^2x : u^3y : z]$, se tiene $\phi(\mathcal{O}) = [0 : u^3 : 0] = [0 : 1 : 0] = \mathcal{O}$. Además está bien definida, pues $(x, y) \in E_4$ es equivalente a

$$\begin{aligned} y^2 &= x^3 + 2x^2 + 1, \\ y^2 &= x^3 + u^{-2}x^2 + 1, \\ u^6y^2 &= u^6x^3 + u^4x^2 + 1, \\ (u^3y)^2 &= (u^2x)^3 + (u^2x)^2 + 1, \end{aligned}$$

es decir, a $(u^2x, u^3y) \in E_1$. Por lo tanto, ϕ es un isomorfismo con inversa $\phi^{-1}(x, y) = (u^{-2}x, u^{-3}y)$.

En el siguiente teorema veremos que las curvas elípticas $E : y^2 = x^3 + b_2x^2 + b_4x + b_6$ y $E' : y^2 = x^3 + u^{-2}b_2x^2 + u^{-4}(2\delta b_2 + b_4)x + u^{-6}(b_2\delta^2 + b_4\delta + b_6 + \delta^3)$ son isomorfas, algo que ya se pudo apreciar en los ejemplos anteriores.

Teorema 4.38. *Sean las curvas elípticas $E' : y^2 = x^3 + u^{-2}b_2x^2 + u^{-4}(2\delta b_2 + b_4)x + u^{-6}(b_2\delta^2 + b_4\delta + b_6 + \delta^3)$, $E : y^2 = x^3 + b_2x^2 + b_4x + b_6$, con $u \in \overline{\mathbb{K}}^*$ y $\delta \in \overline{\mathbb{K}}$. La función $\phi : E'(\overline{\mathbb{K}}) \to E(\overline{\mathbb{K}})$, definida por $\phi(x, y) = (u^2x + \delta, u^3y)$, es un isomorfismo de grupos.*

Prueba. Sean $u \in \overline{\mathbb{K}}^*$ y $\delta \in \overline{\mathbb{K}}$. Decir $(x, y) \in E'$ es equivalente a las siguientes identidades

$$\begin{aligned} y^2 &= x^3 + u^{-2}b_2x^2 + u^{-4}(2\delta b_2 + b_4)x + u^{-6}(b_2\delta^2 + b_4\delta + b_6 + \delta^3), \\ u^6y^2 &= u^6x^3 + u^4b_2x^2 + u^2(2\delta b_2 + b_4)x + (b_2\delta^2 + b_4\delta + b_6 + \delta^3), \\ u^6y^2 &= u^6x^3 + \delta^3 + b_2(u^4x^2 + 2u^2\delta x + \delta^2) + b_4u^2x + b_4\delta + b_6, \\ (u^3y)^2 &= (u^2x + \delta)^3 + b_2(u^2x + \delta)^2 + b_4(u^2x + \delta) + b_6, \end{aligned}$$

es decir, a $(u^2x+\delta, u^3y) \in E$. Además la función inversa, $\phi^{-1} : E \to E'$, está definida por $\phi^{-1}(x,y) = (u^{-3}x, u{-}2(x-\delta))$. En coordenadas proyectivas tenemos

$$\begin{array}{rccc} \phi: & E'(\overline{K}) & \to & E(\overline{K}) \\ & [x:y:z] & \mapsto & [u^2x+\delta z : u^3y : z] \end{array}$$

Para $\mathcal{O} = [0:1:0]$, se tiene

$$\phi(\mathcal{O}) = \phi([0:1:0]) = [0:u^3:0] = [0:1:0] = \mathcal{O}.$$

Por último, sea la recta L de ecuación $y = mx{+}b$. Si $(x,y) \in L \cap E'$ y $\phi(x,y) = (\overline{x}, \overline{y})$, tenemos $y = mx+b$, $\overline{x} = u^2x+\delta$ y $\overline{y} = u^3y$. Además $\overline{y} = um\overline{x} + u^3b - um\delta$. Por lo tanto, ϕ lleva rectas en rectas y por ello respeta la operación de grupo. En conclusión, ϕ es un isomorfismo. □

Teorema 4.39. *Sean las curvas elípticas $E' : y^2 = x^3 + b'_2x^2 + b'_4x + b'_6$, $E : y^2 = x^3 + b_2x^2 + b_4x + b_6$. Si $\phi : E' \to E$ es un isomorfismo definido como $\phi(x,y) = (u^2x+\delta, u^3y)$ para algún $u \in \overline{\mathbb{K}}^*$ y $\delta \in \overline{\mathbb{K}}$, se tiene $b'_2 = u^{-2}b_2$, $b'_4 = u^{-4}(2\delta b_2 + b_4)$ y $b'_6 = u^{-6}(b_2\delta^2 + b_4\delta + b_6 + \delta^3)$.*

Prueba. De la proposición 4.7, para $\nu = 0$, $\beta = 0$, tenemos $b'_2 = u^{-2}b_2$, $b'_4 = u^{-4}(2\delta b_2 + b_4)$ y $b'_6 = u^{-6}(b_2\delta^2 + b_4\delta + b_6 + \delta^3)$. □

El siguiente lema confirma que dos curvas elípticas son isomorfas precisamente cuando tienen el mismo invariante j.

Lema 4.40. *Para la curva elíptica $E' : y^2 = x^3 + b_2x + b_4x + b_6$ con invariante j, se tiene lo siguiente:*

1. *si $j = 0$, entonces E' es isomorfa a $E : y^2 = x^3 + x + 1$;*
2. *si $j \neq 0$, entonces E' es isomorfa a $E : y^2 = x^3 + x^2 - \dfrac{1}{j}$.*

Prueba. Veamos la demostración para cada valor que tome el invariante j.

Si $j = 0$, por lo visto en la observación 4.33 se tiene $b_2 = 0$ y al verificarse $\tau = -b_4$, se cumple $b_4 \neq 0$, pues E' es una curva elíptica. Se comprueba por los teoremas 4.38 y 4.39 que el isomorfismo $\phi : E' \to E$ está definido por $\phi(x,y) = (u^2x+\delta, u^3y)$, donde $b_4 = u^{-4}$ y $b_6 = u^{-6}(\delta + 1 + \delta^3)$, con $u \in \overline{\mathbb{K}}^*$.

Si $j \neq 0$, se tiene $b_2 \neq 0$ y por ello, después de un cambio lineal de variable toma la forma $y^2 = x^3 + b'_2x^2 + b'_6$. Además se cumple $b'_6 \neq 0$ por ser una curva elíptica y $\tau' = -b'^3_2 b'_6$. Se verifica por los teoremas 4.38 y 4.39 que el isomorfismo $\phi : E' \to E$ está definido por $\phi(x,y) = (u^2x, u^3y)$, donde $b'_2 = u^{-2}$, $b'_6 = -\dfrac{u^{-6}}{j}$. □

Del ejemplo 4.36 obtenemos que las curvas elípticas $E_5 : y^2 = x^3 + x$ y $E_6 : y^2 = x^3 + x + 1$ son isomorfas y además tienen invariante $j = 0$. En el caso de las curvas elípticas $E_1 : y^2 = x^3 + x^2 + 1$ y $E_4 : y^2 = x^3 + 2x^2 + 1$, se tiene que son isomorfas por el ejemplo 4.37 y también tienen el mismo invariante j, específicamente $j(E_1) = j(E_2) = 2$.

Teorema 4.41. *Dos curvas elípticas son isomorfas sobre $\overline{\mathbb{K}}$ si y solo si tienen el mismo invariante j.*

Prueba. Sean las curvas elípticas E y E' con sus respectivos invariantes $j(E)$ y $j(E')$. Si dichas curvas son isomorfas, por la proposición 4.6 tenemos $j(E) = j(E')$. Ahora supongamos $j(E) = j(E')$. Si $j(E) = 0$, entonces $j(E') = 0$ y por el lema 4.40 se tiene que las curvas elípticas E y E' son isomorfas a $E : y^2 = x^3 + 1$. Luego E y E' son isomorfas. Si $j(E) \neq 0$, entonces $j(E') \neq 0$ y por el lema 4.40 se tiene que las curvas elípticas E y E' son isomorfas a $E : y^2 = x^3 + x^2 - \dfrac{1}{j}$. Luego E y E' son isomorfas. □

Ejemplo 4.42. Las curvas elípticas $E : y^2 = x^3 + x^2 + 2$ y $E' : y^2 = x^3 + 2x^2 + 1$ son isomorfas, pues $j(E) = j(E') = 1$. Por los teoremas 4.38 y 4.39, el isomorfismo $\phi : E' \to E$ está definido por $\phi(x, y) = (u^2x + \delta, u^3y)$ donde $2 = u^{-2}$, $0 = u^{-4}(2\delta)$, $1 = u^{-6}(\delta^2 + 2 + \delta)$. Como $u \in \overline{\mathbb{F}}_3 \setminus \mathbb{F}_3$, se tiene que E' es twist de E.

Ejemplo 4.43. Dadas las curvas elípticas $E' : y^2 = x^3 + 2x^2 + 1$ y $F : 2y^2 = x^3 + 2x^2 + 1$ sobre $\mathbb{F}_3$, definimos $\phi : F \to E'$ como $\phi(x, y) = (x, 2u^{-1}y)$; acá $u^2 = 2$. Notamos que ϕ está bien definida pues

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

Además ϕ respeta la operación de grupo, ya que para $(x, y) \in F \cap L$, con L una recta de ecuación $y = mx + b$, se tiene $2u^{-1}y = 2mu^{-1}x + 2u^{-1}b$. En coordenadas proyectivas tenemos $\phi([x : y : z]) = [ux : 2y : uz]$ y con ello $\phi(\mathcal{O}) = \phi([0 : 1 : 0]) = [0 : 2 : 0] = \mathcal{O}$. Por lo tanto ϕ es un isomorfismo cuya inversa está definida por $\phi^{-1}(x, y) = (x, 2uy)$.

A continuación probaremos un lema que nos ayudará a demostrar que toda curva elíptica que sea un twist de E es de la forma $E_v : vy^2 = x^3 + b_2x^2 + b_6$.

Lema 4.44. *Las curvas elípticas $E : w^6y^2 = x^3 + b_2x^2 + b_6$ y $E' : y^2 = x^3 + \dfrac{b_2}{w^2}x^2 + \dfrac{b_6}{w^6}$, con $b_2, b_6 \in \mathbb{K}^*$, $w \in \overline{\mathbb{K}}$, son isomorfas.*

Prueba. Para $(x, y) \in E$ se tiene

$$\begin{aligned} w^6y^2 &= x^3 + b_2x^2 + b_6, \\ y^2 &= \frac{x^3}{w^6} + \frac{b_2}{w^6}x^2 + \frac{b_6}{w^6}, \\ y^2 &= \left(\frac{x}{w^2}\right)^3 + \frac{b_2}{w^2}\left(\frac{x}{w^2}\right)^2 + \frac{b_6}{w^6}. \end{aligned}$$

Definamos $\phi : E \to E'$ como $\phi(x, y) = \left(\dfrac{x}{w^2}, y\right)$, que está bien definida gracias a la fórmula desplegada. Sea la recta L de ecuación $y = mx + b$. Si $(x, y) \in E \cap L$ y $(\overline{x}, \overline{y}) = \phi(x, y)$, entonces $y = mx + b$, $\overline{x} = \dfrac{x}{w^2}$, $\overline{y} = y$. Al verificarse $\overline{y} = mw^2\overline{x} + b$, es decir ϕ concluimos que ϕ preserva la operación de grupo. Además ϕ tiene inversa definida por $\phi^{-1}(x, y) = (w^2x, y)$. Por lo tanto ϕ es un isomorfismo. □

Teorema 4.45. *Sea $E : y^2 = x^3 + b_2x^2 + b_6$ una curva elíptica, con $b_2, b_6 \in \mathbb{K}^*$. Todo curva elíptica E' twist de E es isomorfa a algún $E_v : vy^2 = x^3 + b_2x^2 + b_6$.*

Prueba. Sea E' una curva elíptica twist a E. Por los teoremas 4.38 y 4.39 se tiene que el isomorfismo $\phi_1 : E \to E'$ está definido por $\phi_1(x, y) = (u^{-2}x, u^{-3}y)$ con la curva E' de la forma $E' : y^2 = x^3 + u^{-2}b_2x^2 + u^{-6}b_6$, donde $u \in \overline{\mathbb{K}}^*$ es tal que $u \notin \mathbb{K}$. Con el lema 4.44 aparece el isomorfismo $\phi_2 : E' \to E_{u^6}$ definido por $\phi_2(x, y) = (u^2x, y)$ Por lo tanto E_{u^6} es isomorfo a E mediante el isomorfismo $\phi : E \to E_{u^6}$ definido por $\phi(x, y) = (x, u^{-3}y)$. Como $u \notin \mathbb{K}$, entonces E_{u^6} es twist de E. □

Finalmente determinaremos el orden del grupo de automorfismos para curvas elípticas del tipo $E : y^2 = x^3 + b_2x^2 + b_4x + b_6$.

Teorema 4.46. *El grupo de automorfismos $Aut(E)$ para la curva elíptica $E : y^2 = x^3 + b_2x^2 + b_4x + b_6$, con invariante j, tiene dos elementos si $j \neq 0$ y doce si $j = 0$.*

Prueba. Por los teoremas 4.38 y 4.39, el automorfismo $\phi : E \to E$ está definido por $\phi(x, y) = (u^2x + \delta, u^3y)$.

Para $j = 0$ se tiene $b_2 = 0$ y por la proposición 4.7, ha de tenerse $\nu = 0$ y $\beta = 0$, y se debe cumplir

$$b_4 = u^{-4}b_4, \tag{4.37}$$
$$b_6 = u^{-6}(b_4\delta + b_6 + \delta^3). \tag{4.38}$$

Observamos que u puede tomar cuatro valores y por cada valor que tome u se obtiene tres valores para δ. En resumen existen 12 automorfismos.

Para el caso $j \neq 0$, se tiene $b_2 \neq 0$. Luego, la curva elíptica adopta la forma $E : y^2 = x^3 + b_2x^2 + b_6$. Por la proposición 4.7, con $\nu = 0$, $\beta = 0$, $\delta = 0$, se cumple

$$\begin{aligned} b_2 &= b_2u^{-2}, \\ b_6 &= u^{-6}b_6. \end{aligned}$$

Notamos que u solo puede tomar dos valores y por ello existen apenas dos automorfismos. □

Los automorfismos de la curva elíptica $E_1 : y^2 = x^3 + x^2 + 1$ sobre el cuerpo $\mathbb{F}_3$, están definidos por $\phi(x, y) = (u^2x + \delta, u^3y)$ sujetos a $1 = u^{-2}$ y $1 = u^{-6}$. Y gracias a estas restricciones tenemos los automorfismos

$$\begin{aligned} \phi_1(x, y) &= (x, y), \\ \phi_2(x, y) &= (x, 2y), \end{aligned}$$

Ejemplo 4.47. Los automorfismos $\phi : E_6 \to E_6$ para la curva elíptica $E_6 : y^2 = x^3 + x + 2$ definida sobre $\mathbb{F}_3$, están dados por $\phi(x, y) = (u^2x + \delta, u^3y)$ con $1 = u^{-4}$, $2 = u^{-6}(\delta + 2 + \delta^3)$. Si $\alpha \in \overline{\mathbb{F}}_3$ es solución de $\alpha^2 + 1 = 0$, aparecen los siguientes

automorfismos

$$\begin{aligned}
\phi_1(x,y) &= (x,y),\\
\phi_2(x,y) &= (x+\alpha,y),\\
\phi_3(x,y) &= (x+2\alpha,y),\\
\phi_4(x,y) &= (x,2y),\\
\phi_5(x,y) &= (x+\alpha,2y),\\
\phi_6(x,y) &= (x+2\alpha,2y),\\
\phi_7(x,y) &= (2x+1,2\alpha y),\\
\phi_8(x,y) &= (2x+1+\alpha,2\alpha y),\\
\phi_9(x,y) &= (2x+1-\alpha,2\alpha y),\\
\phi_{10}(x,y) &= (2x+1,\alpha y),\\
\phi_{11}(x,y) &= (2x+1+\alpha,\alpha y),\\
\phi_{12}(x,y) &= (2x+1-\alpha,\alpha y),
\end{aligned}$$

4.3 Curvas elípticas en cuerpos de característica distinta de 2 y 3

En este caso toda curva elíptica toma la forma $E : y^2 = x^3 + c_4x + c_6$, donde $d_2 = 0$, $d_4 = 2c_4$, $d_6 = 4c_6$, $e_4 = -48c_4$, $\tau = -64c_4^3 - 432c_6^2$ y $j = \dfrac{(1728)(4)c_4^3}{4c_4^3 + 27c_6^2}$.

Ejemplo 4.48. Las curvas elípticas sobre $\mathbb{F}_5$ dadas por $E_1 : y^2 = x^3 + 1$, $E_2 : y^2 = x^3 + 2$, $E_3 : y^2 = x^3 + 3$, $E_4 : y^2 = x^3 + 4$, tienen invariante j iguales, específicamente $j(E_1) = j(E_2) = j(E_3) = j(E_4) = 0$.

Ejemplo 4.49. Las curvas elípticas sobre $\mathbb{F}_5$ dadas por $E_5 : y^2 = x^3 + x$, $E_6 : y^2 = x^3 + 2x$, $E_7 : y^2 = x^3 + 3x$, $E_8 : y^2 = x^3 + 4x$, tienen invariante j iguales, para todos vale $1728 \equiv 3$.

Ejemplo 4.50. Las curvas elípticas sobre $\mathbb{F}_5$ dadas por $E_9 : y^2 = x^3 + x + 2$, $E_{10} : y^2 = x^3 + x + 3$, $E_{11} : y^2 = x^3 + x + 4$, $E_{12} : y^2 = x^3 + 4x + 2$, $E_{13} : y^2 = x^3 + 2x + 4$, $E_{14} : y^2 = x^3 + 3x + 2$, cumplen $j(E_9) = j(E_{10}) = 1$, $j(E_{11}) = j(E_{12}) = 2$, $j(E_{13}) = j(E_{14}) = 4$.

Observación 4.51. Notemos que de la igualdad $j = \dfrac{6912c_4^3}{4c_4^3 + 27c_6^2}$ se obtiene $j = 0$ si y solo si $c_4 = 0$. Además,

$$j = 1728 = \frac{6912c_4^3}{4c_4^3 + 27c_6^2} \text{ equivale a } 1 = \frac{4c_4^3}{4c_4^3 + 27c_6^2} \text{ es decir, a } c_6 = 0.$$

En otras palabras se tiene $j = 1728$ si y solo si $c_6 = 0$.

De los ejemplos 4.48, 4.49 y 4.50 tenemos que las curvas elípticas $E_1 : y^2 = x^3 + 1$, $E_5 : y^2 = x^3 + x$, $E_9 : y^2 = x^3 + x + 2$, $E_{11} : y^2 = x^3 + x + 4$, $E_{14} : y^2 = x^3 + 3x + 2$,

definidas sobre el cuerpo $\mathbb{F}_5$, tienen invariante j iguales a $j(E_1) = 0$, $j(E_5) = 3$, $j(E_9) = 1$, $j(E_{11}) = 2$, $j(E_{14}) = 4$, respectivamente, es decir para cada elemento de $\mathbb{F}_5$ existe una curva elíptica cuyo invariante j es dicho elemento. La proposición que sigue a continuación generaliza este resultado para cualquier cuerpo de característica distinta de 2 y 3.

Proposición 4.52. *Si $j \in \mathbb{K}$, entonces existe una curva elíptica E tal que $j(E) = j$.*

Prueba. Para el caso $j = 0$, consideramos la curva elíptica $E : y^2 = x^3 + 1$ que satisface $j(E) = 0$. Si $j = 1728$, la curva elíptica $E : y^2 = x^3 + x$, satisface $j(E) = 1728$. Si $j \neq 0, 1728$, la curva elíptica $E : y^2 = x^3 + \dfrac{3j}{1728 - j}x + \dfrac{2j}{1728 - j}$, satisface $j(E) = j$. □

Ejemplo 4.53. Sean las curvas elípticas $E_1 : y^2 = x^3+1$ y $E_2 : y^2 = x^3+2$ definidas sobre el cuerpo $\mathbb{F}_5$. Definamos $\phi : E_1 \to E_2$ como $\phi(x, y) = (u^2x, u^3y)$, donde $u \in \overline{\mathbb{F}}_5$ satisface $u^6 = 2$. Para $(x, y) \in L \cap E_1$, donde L es una recta de ecuación $y = mx+b$, tenemos $u^3y = um(u^2x) + u^3b$, es decir ϕ respeta la operación de grupo. Como la homogenización de ϕ está definida por $\phi([x : y : z]) = [4x : 2y : z]$, se tiene $\phi(\mathcal{O}) = \phi([0 : 1 : 0]) = [0 : 2 : 0] = [0 : 1 : 0] = \mathcal{O}$. Además, ϕ está bien definida pues $(x, y) \in E_1$ es equivalente a cada una de las siguientes identidades

$$\begin{aligned} y^2 &= x^3 + 1, \\ u^6y^2 &= u^6x^3 + 2, \\ (u^3y)^2 &= (u^2x)^3 + 2, \end{aligned}$$

es decir, a $(u^2x, u^3y) \in E_2$. Concluimos que ϕ es un isomorfismo, con inversa $\phi^{-1}(x, y) = (u^{-2}x, u^{-3}y)$.

Ejemplo 4.54. Sean las curvas elípticas $E_9 : y^2 = x^3 + x + 2$ y $E_{10} : y^2 = x^3 + x + 3$ definidas sobre el cuerpo $\mathbb{F}_5$. Definamos $\phi : E_9 \to E_{10}$ como $\phi(x, y) = (4x, 2y)$. Para $(x, y) \in L \cap E_1$, donde L es una recta de ecuación $y = mx + b$, tenemos $2y = 3m(4x)+2b$, es decir ϕ respeta la operación de grupo. Como la homogenización de ϕ está definida por $\phi([x : y : z]) = [4x : 3y : z]$, se tiene $\phi(\mathcal{O}) = \phi([0 : 1 : 0]) = [0 : 2 : 0] = [0 : 1 : 0] = \mathcal{O}$. Además, ϕ está bien definida pues $(x, y) \in E_9$ es equivalente a

$$\begin{aligned} y^2 &= x^3 + x + 2, \\ 4y^2 &= 4x^3 + 4x + 3, \\ (2y)^2 &= (4x)^3 + 4x + 3, \end{aligned}$$

es decir, a $(4x, 2y) \in E_{10}$. Concluimos que ϕ es un isomorfismo, con inversa $\phi^{-1}(x, y) = (4x, 3y)$.

Ejemplo 4.55. Sean las curvas elípticas $E_7 : y^2 = x^3 + 3x$ y $E_8 : y^2 = x^3 + 4x$ definidas sobre el cuerpo $\mathbb{F}_5$. Definamos $\phi : E_7 \to E_8$ como $\phi(x, y) = (u^2x, u^3y)$, con $u \in \overline{\mathbb{F}}_5$ tal que $u^4 = 3$. Para $(x, y) \in L \cap E_1$, donde L es una recta de ecuación $y = mx+b$, tenemos $u^3y = um(u^2x)+u^3b$, es decir ϕ respeta la operación de grupo.

Como la homogenización de ϕ está definida por $\phi([x:y:z]) = [u^2x : u^3y : z]$, se tiene $\phi(\mathcal{O}) = \phi([0:1:0]) = [0:u^3:0] = [0:1:0] = \mathcal{O}$. Además, ϕ está bien definida pues decir que se satisface $(x,y) \in E_7$ es equivalente a cada una de las siguientes identidades

$$\begin{aligned} y^2 &= x^3 + 3u^{-4}x, \\ y^2 &= x^3 + 3u^{-4}x, \\ u^6y^2 &= u^6x^3 + 3u^2x, \\ (u^3y)^2 &= (u^2x)^3 + 3u^2x, \end{aligned}$$

es decir, a $(u^2x, u^3y) \in E_8$. Concluimos que ϕ es un isomorfismo, con inversa $\phi^{-1}(x,y) = (u^{-2}x, u^{-3}y)$.

Acabamos de escribir ejemplos en los cuales las curvas elípticas son isomorfas. Los siguientes teoremas nos muestran en que casos dos curvas elípticas son isomorfas y cómo está definido el isomorfismo que lo lleva a cabo.

Teorema 4.56. *Sean las curvas elípticas $E : y^2 = x^3 + b_4x + b_6$, $E' : y^2 = x^3 + u^{-4}b_4x + u^{-6}b_6$, con $u \in \overline{\mathbb{K}}^*$. La función $\phi : E'(\overline{\mathbb{K}}) \to E(\overline{\mathbb{K}})$, definida por $\phi(x,y) = (u^2x, u^3y)$, es un isomorfismo de grupos.*

Prueba. Sea $u \in \overline{\mathbb{K}}^*$. Tenemos que $(x,y) \in E'$ es equivalente a cada una de las siguientes identidades

$$\begin{aligned} y^2 &= x^3 + u^{-4}b_4x + u^{-6}b_6, \\ u^6y^2 &= u^6x^3 + u^2b_4x + b_6, \\ (u^3y)^2 &= (u^2x)^3 + b_4(u^2x) + b_6, \end{aligned}$$

es decir, a $(u^2x, u^3y) \in E$ y por ello ϕ está bien definida. Además, se tiene $(x,y) \in E$ si y solo si $(u^{-2}x, u^{-3}y) \in E'$. Luego la función ϕ tiene inversa definida por $\phi^{-1}(x,y) = (u^{-2}x, u^{-3}y)$.

En coordenadas proyectivas tenemos

$$\begin{array}{rccc} \phi: & E(\overline{K}) & \to & E'(\overline{K}) \\ & [x:y:z] & \mapsto & [u^2x : u^3y : z] \end{array}$$

Como $\mathcal{O} = [0:1:0]$, se tiene

$$\phi(\mathcal{O}) = \phi([0:1:0]) = [0:u^3:0] = [0:1:0] = \mathcal{O}.$$

Por último, sea la recta L de ecuación $y = mx+b$. Si $(x,y) \in L \cap E$ y $\phi(x,y) = (\overline{x}, \overline{y})$, tenemos $y = mx + b$, $\overline{x} = u^2x$ y $\overline{y} = u^3y$. Además $\overline{y} = um\overline{x} + u^3b$. Por lo tanto, ϕ lleva rectas en rectas y por ello respeta la operación de grupo. En conclusión, ϕ es un isomorfismo. □

Teorema 4.57. *Sean las curvas elípticas $E : y^2 = x^3 + b_4x + b_6$ y $E' : y^2 = x^3 + b'_4x + b'_6$. Si $\phi : E \to E'$ es un isomorfismo definido como $\phi(x,y) = (u^2x, u^3y)$ para algún $u \in \mathbb{K}^*$, entonces $b'_4 = u^{-4}b_4$ y $b'_6 = u^6b_6$.*

Prueba. De la proposición 4.7, para $\delta = 0$, $\nu = 0$, $\beta = 0$, tenemos $b_4' = u^{-4}b_4$ y $b_6 = u^{-6}b_6$. □

El siguiente lema nos permitirá concluir que dos curvas elípticas son isomorfas cuando tienen el mismo invariante j.

Lema 4.58. *Para la curva elíptica $E' : y^2 = x^3 + b_4x + b_6$ con invariante j, se tiene lo siguiente:*

1. *si $j = 0$, entonces E' es isomorfa a $E : y^2 = x^3 + 1$;*
2. *si $j = 1728$, entonces E' es isomorfa a $E : y^2 = x^3 + x$;*
3. *si $j \neq 0, 1728$, entonces E' es isomorfa a $E : y^2 = x^3 + \dfrac{3j}{1728 - j}x + \dfrac{2j}{1728 - j}$.*

Prueba. Veamos la demostración para cada valor que tome el invariante j.

Si $j = 0$, por lo visto en la observación 4.51 se tiene $b_4 = 0$ y como $\tau = -64b_4^3 - 432b_6^2$ se sigue $b_6 \neq 0$, pues E' es una curva elíptica. Se verifica por los teoremas 4.56 y 4.57 que el isomorfismo $\phi : E' \to E$ está definido por $\phi(x, y) = (u^2x, u^3y)$, donde $u \in \overline{\mathbb{K}}^*$ satisface $u^6 = b_6$.

Si $j = 1728$, por lo visto en la observación 4.51 se tiene $b_6 = 0$ y como $\tau = -64b_4^3 - 432b_6^2$ se sigue $b_4 \neq 0$, pues E' es una curva elíptica. Se verifica por los teoremas 4.56 y 4.57 que el isomorfismo $\phi : E' \to E$ está definido por $\phi(x, y) = (u^2x, u^3y)$, donde $u^4 = b_4$ en $\overline{\mathbb{K}}^*$.

Si $j \neq 0, 1728$, por lo visto en la observación 4.51 se tiene $b_4 \neq 0$ y $b_6 \neq 0$. Se verifica por los teoremas 4.56 y 4.57 que el isomorfismo $\phi : E' \to E$ está definido por $\phi(x, y) = (u^2x, u^3y)$, donde $\dfrac{3j}{u^4b_4} = u^4b_4$ y $\dfrac{2j}{1728 - j} = u^6b_6$. Si resolvemos el sistema para determinar el valor u, obtenemos

$$\frac{2j}{1728 - j} = \frac{3j}{(1728 - j)b_4}u^2b_6,$$

lo cual equivale a $\dfrac{2b_4}{3b_6} = u^2$. Es decir, con $u = \dfrac{2b_4}{3b_6}$, se verifica que $\phi : E' \to E$ es el isomorfismo buscado. □

Para las curvas elípticas $E_1 : y^2 = x^3 + 1$ y $E_2 : y^2 = x^3 + 2$ se satisface $j(E_1) = j(E_2) = 0$ y por el ejemplo 4.53 se tiene que son isomorfas. Un caso similar ocurre para los pares de curvas $E_9 : y^2 = x^3 + x + 2$ y $E_{10} : y^2 = x^3 + x + 3$, $E_7 : y^2 = x^3 + 3x$ y $E_8 : y^2 = x^3 + 4x$, las cuales satisfacen $j(E_9) = j(E_{10}) = 1$ y $j(E_7) = j(E_8) = 3$.

Teorema 4.59. *Dos curvas elípticas son isomorfas sobre $\overline{\mathbb{K}}$ si y solo si tienen el mismo invariante j.*

Prueba. Sean las curvas elípticas E y E' con sus respectivos invariantes $j(E)$ y $j(E')$.

Si dichas curvas son isomorfas, por la proposición 4.6 tenemos $j(E) = j(E')$.

Ahora supongamos $j(E) = j(E')$. Si $j(E) = 0$, por el lema 4.58 se tiene que las curvas elípticas E y E' son isomorfas a $E : y^2 = x^3 + 1$. Si $j(E) = 1728$, por el

lema 4.58 se tiene que las curvas elípticas E y E' son isomorfas a $E : y^2 = x^3 + x$. Si $j(E) \neq 0, 1728$, entonces por el lema 4.58 se tiene que las curvas elípticas E y E' son isomorfas a $E : y^2 = x^3 + \dfrac{3j}{1728 - j}x + \dfrac{2j}{1728 - j}$. □

A continuación veremos unos ejemplos en los cuales las curvas twist de $E_1 : y^2 = x^3+1$ y de $E_7 : y^2 = x^3+3x$ son isomorfas a curvas de la forma $E_v : vy^2 = x^3+b_4x+b_6$, con $v \in \mathbb{F}_5$ libre de cuadrados.

Ejemplo 4.60. Del ejemplo 4.53, las curvas elípticas $E_1 : y^2 = x^3 + 1$ y $E_2 : y^2 = x^3 + 2$ son isomorfas mediante $\phi : E_1 \to E_2$ definida por $\phi(x, y) = (u^2x, u^3y)$, con $u \in \overline{\mathbb{F}}_5$ tal que $u^6 = 2$. Además la curva elíptica E_2 es un twist de E_1, pues $u \notin \mathbb{F}_5$. Definamos $\psi : F \to E_2$ como $\psi(x, y) = (u^2x, y)$, donde $F : u^{-6}y^2 = x^3 + 1$. La función ψ está bien definida pues se tiene

$$\begin{aligned} u^{-6}y^2 &= x^3 + 1, \\ y^2 &= u^6x^3 + u^6, \\ y^2 &= (u^2x)^3 + 2. \end{aligned}$$

Sea $(x, y) \in F \cap L$, con L una recta de ecuación $y = xm+b$. Se tiene $y = u^{-2}m(u^2x)+b$ y por ello ψ respeta la operación de grupo. Además la forma homogenizada de ψ está dada por $\psi([x : y : z]) = [u^2x : y : z]$ y satisface $\psi(\mathcal{O}) = \psi([0 : 1 : 0]) = [0 : 1 : 0] = \mathcal{O}$, con $\mathcal{O} = [0 : 1 : 0]$. Por lo tanto ψ es un isomorfismo con inversa $\psi^{-1}(x, y) = (u^{-2}x, y)$, es decir E_2 es isomorfo a la curva elíptica F, acá u^{-6} es claramente libre de cuadrados sobre $\mathbb{F}_5$.

Ejemplo 4.61. Por el ejemplo 4.55, las curvas elípticas $E_7 : y^2 = x^3 + 3x$ y $E_8 : y^2 = x^3 + 4x$ son isomorfas mediante $\phi : E_7 \to E_8$, definido por $\phi(x, y) = (u^2x, u^3y)$ con $u \notin \mathbb{F}_5$, y se desprende que E_8 es un twist de E_7. Dada la curva elíptica $F : u^{-6}y^2 = x^3 + 3x$ definamos $\psi : F \to E_8$ como $\psi(x, y) = (u^2x, y)$, la cual está bien definida ya que se tiene

$$\begin{aligned} u^{-6}y^2 &= x^3 + 3x, \\ y^2 &= u^6x^3 + 3u^6x, \\ y^2 &= (u^2x)^3 + 4(u^2x). \end{aligned}$$

Sea $(x, y) \in F \cap L$, con L una recta de ecuación $y = xm+b$. Se tiene $y = u^{-2}m(u^2x)+b$ y por ello ψ respeta la operación de grupo. Además la forma homogenizada de ψ está dada por $\psi([x : y : z]) = [u^2x : y : z]$ y satisface $\psi(\mathcal{O}) = \psi([0 : 1 : 0]) = [0 : 1 : 0] = \mathcal{O}$. Por lo tanto ψ es un isomorfismo con inversa $\psi^{-1}(x, y) = (u^{-2}x, y)$, es decir E_8 es isomorfo a la curva elíptica F, donde u^{-6} es libre de cuadrados sobre $\mathbb{F}_5$.

El lema a continuación nos permite caracterizar los twist de las curvas elípticas de la forma $E : y^2 = x^3 + b_4x + b_6$. Para ello tengamos en cuenta a la familia de curvas elípticas $E_v : vy^2 = x^3 + b_4x + b_6$, con $v \in \overline{\mathbb{K}}$, que son de vital importancia pues representan todos los twist de $E : y^2 = x^3 + b_4x + b_6$.

Lema 4.62. *Las curvas elípticas* $E : w^6y^2 = x^3 + ax + b$ *y* $E' : y^2 = x^3 + \dfrac{a}{w^4}x + \dfrac{b}{w^6}$, *con* $a, b \in \mathbb{K}^*$, $w \in \overline{\mathbb{K}}$, *son isomorfas.*

Prueba. Para $(x, y) \in E$ se tiene

$$\begin{aligned} w^6 y^2 &= x^3 + ax + b, \\ y^2 &= \frac{x^3}{w^6} + \frac{a}{w^6} + \frac{b}{w^6}, \\ y^2 &= \left(\frac{x}{w^2}\right)^3 + \frac{a}{w^4}\left(\frac{x}{w^2}\right) + \frac{b}{w^6}. \end{aligned}$$

Definamos $\phi : E \to E'$ como $\phi(x, y) = \left(\frac{x}{w^2}, y\right)$, el cual claramente es una isogenía y además su inversa está definida por $\phi^{-1}(x, y) = (w^2 x, y)$, con lo cual ϕ es un isomorfismo. □

Teorema 4.63. *Sea $E : y^2 = x^3 + ax + b$ una curva elíptica, con $a, b \in \mathbb{K}^*$. Todo curva elíptica que es twist de E es isomorfa a algún E_v definido anteriormente.*

Prueba. Sea E' una curva elíptica isomorfa a E. Por los teoremas 4.56 y 4.57 se tiene que el isomorfismo $\phi : E \to E'$ está definido por $\phi(x, y) = (u^2 x, u^3 y)$ y además la curva E' es de la forma $E' : y^2 = x^3 + u^4 ax + u^6 b$, donde $u \in \overline{\mathbb{K}}^*$. Como $u^6 b, u^4 a \in \mathbb{K}$, entonces $\frac{u^6 b}{u^4 a} \in \mathbb{K}$ y con ello $u^2 \in \mathbb{K}$. Para que E' sea un twist de E debe cumplir $u \notin \mathbb{K}$. Sea $w = u$ y $v = u^{-6}$. Tenemos que v no tiene raíz cuadrada, pues en caso contrario, se tendría $u^3 \in \mathbb{K}$, y con ello $u \in \mathbb{K}$, lo cual es absurdo. Por el lema 4.62, se tiene que E_v es isomorfo a E'. Por lo tanto E_v es isomorfo a E y además v no es cuadrado perfecto. □

Observación 4.64. Sabemos que toda curva elíptica isomorfa a $E : y^2 = x^3 + b_4 x + b_6$ es de la forma $E' : y^2 = x^3 + u^{-4} b_4 x + u^{-6} b^6$. Si $b_4 = 0$, entonces E' es twist de E si u no tiene potencia sexta en $\mathbb{K}$, y para $b_6 = 0$ la curva E' será twist de E si u no tiene potencia cuarta.

Finalmente, el siguiente teorema permite determinar el orden del grupo de automorfismos para curvas elípticas de la forma $E : y^2 = x^3 + b_4 x + b_6$.

Teorema 4.65. *El grupo de automorfismos $Aut(E)$ para la curva elíptica $E : y^2 = x^3 + b_4 x + b_6$, con invariante j, tiene orden 2 si $j \neq 0, 1728$, orden 4 si $j = 1728$ y orden 6 si $j = 0$.*

Prueba. Todo automorfismo $\phi : E \to E$ está definido por $\phi(x, y) = (u^2 x, u^3 y)$ gracias a los teoremas 4.56 y 4.57.

Si $j = 0$, tenemos $b_4 = 0$. Por la proposición 4.7, con $\delta = 0$, $\nu = 0$, $\beta = 0$, se cumple

$$u^6 b_6 = b_6,$$

donde u toma seis valores distintos y por ende existen seis automorfismos.

Si $j = 1728$, se tiene $b_6 = 0$ y $b_4 \neq 0$. Por la proposición 4.7, con $\delta = 0$, $\nu = 0$, $\beta = 0$, se cumple

$$u^4 b_4 = b_4,$$

donde u toma cuatro valores y por ende quedan determinados cuatro automorfismos.

Para $j \neq 0, 1728$, se tiene $c_4 \neq 0$ y $c_6 \neq 0$ de la observación 4.51. Por otro lado, de la proposición 4.7, con $\delta = 0$, $\nu = 0$, $\beta = 0$, se satisfacen las igualdades

$$u^4 b_4 = b_4, u^6 b_6 = b_6,$$

acá u toma dos valores y aparecen dos automorfismos. □

Ejemplo 4.66. Sea la curva elíptica $E_1 : y^2 = x^3 + 1$ sobre el cuerpo $\mathbb{F}_5$, con invariante $j = 0$. Un automorfismo $\phi : E_1 \to E_1$ está definido por $\phi(x, y) = (u^2 x, u^3 y)$ y está sujeto a $1 = u^{-6}$. Tomemos α solución de $x^2 = 3$. Tenemos que las soluciones de $u^6 = 1$ son $u = 1$, $u = 4$, $u = -3 + \alpha$, $u = -3 - \alpha$, $u = -2 + \alpha$, $u = -2 - \alpha$, y en consecuencia tenemos 6 automorfismos de E_1:

$$\begin{aligned}
\phi_1(x, y) &= (x, y), \\
\phi_2(x, y) &= (x, 4y), \\
\phi_3(x, y) &= ((2 + 4\alpha)x, y), \\
\phi_4(x, y) &= ((2 + \alpha)x, y). \\
\phi_5(x, y) &= ((2 + \alpha)x, 4y), \\
\phi_6(x, y) &= ((2 + 4\alpha)x, 4y).
\end{aligned}$$

Ejemplo 4.67. Sea la curva elíptica $E_9 : y^2 = x^3 + x + 3$ sobre el cuerpo $\mathbb{F}_5$, con invariante $j = 1$. Tenemos que un automorfismo $\phi : E_9 \to E_9$ está definido por $\phi(x, y) = (u^2 x, u^3 y)$ donde debe cumplirse $1 = u^{-4}$, $1 = u^{-6}$. Lo anterior se reduce a $u^2 = 1$, cuyas soluciones son $u = 1$ y $u = 4$; por tanto los automorfismos son

$$\begin{aligned}
\phi_1(x, y) &= (x, y), \\
\phi_2(x, y) &= (x, 4y).
\end{aligned}$$

Ejemplo 4.68. Para la curva elíptica $E_5 : y^2 = x^3 + x$ sobre el cuerpo $\mathbb{F}_5$, con invariante $j = 3$, un automorfismo $\phi : E_5 \to E_5$ está definido por $\phi(x, y) = (u^2 x, u^3 y)$ donde $u^{-4} = 1$, cuyas soluciones son $u = 1$, $u = 2$, $u = 3$ y $u = 4$. Luego los automorfismos son

$$\begin{aligned}
\phi_1(x, y) &= (x, y), \\
\phi_2(x, y) &= (4x, 3y), \\
\phi_3(x, y) &= (4x, 2y), \\
\phi_4(x, y) &= (x, 4y).
\end{aligned}$$

Capítulo 5

Conclusiones

De acuerdo con el valor de la característica del cuerpo $\mathbb{K}$, deducimos que las curvas elípticas en forma de Weierstrass son singulares si y solo si su discriminante τ se anula.

Un isomorfismo $\phi : E_2 \to E_1$ entre las curvas elípticas $E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ y $E_2 : s^2 + a_1'ts + a_3's = t^3 + a_2't^2 + a_4't + a_6'$, está dado necesariamente por $\phi(t, s) = (u^2t + \delta, u^2\nu t + u^3s + \beta)$. Con ello la relación entre los coeficientes de dichas curvas satisfarán

$$\begin{aligned}
ua_1' &= a_1 + 2\nu, \\
u^2a_2' &= a_2 - \nu a_1 + 3\delta - \nu^2, \\
u^3a_3' &= a_3 + \delta a_1 + 2\beta, \\
u^4a_4' &= a_4 - \nu a_3 + 2\delta a_2 - (\beta + \delta\nu)a_1 + 3\delta^2 - 2\nu\beta, \\
u^6a_6' &= a_6 + \delta a_4 + \delta^2 a_2 + \delta^3 - \beta a_3 - \beta^2 - \delta\beta a_1, \\
u^2d_2' &= d_2 + 12\delta, \\
u^4d_4' &= d_4 + \delta d_2 + 6\delta^2, \\
u^6d_6' &= d_6 + 2\delta d_4 + \delta^2 d_2 + 4\delta^3, \\
u^8d_8' &= d_8 + 3\delta d_6 + 3\delta^2 d_2 + 3\delta^4, \\
u^4e_4' &= e_4, \\
u^6e_6' &= e_6, \\
u^{12}\tau' &= \tau.
\end{aligned}$$

Por lo tanto, como el discriminante entre dos curvas elípticas isomorfas se ve afectado por un factor no nulo u^{12}, analizar la singularidad en una curva elíptica es lo mismo que analizarla en la otra curva.

El invariante j es un factor que nos permite concluir si dos curvas elípticas son isomorfas sobre $\overline{\mathbb{K}}$. Además dicho factor define una biyección entre la clase de las curvas elípticas módulo isomorfismos y la clausura algebraica $\overline{\mathbb{K}}$

Dada una curva elíptica E y un cuerpo $\mathbb{K}$ de característica p la información se resume como sigue. Si $j \neq 0, 1728$ entonces la cantidad de automorfismos de la curva elíiptica E es 2, sin importar el valor de la característica del cuerpo $\mathbb{K}$. Si $p \neq 2, 3$, se tienen 4 automorfismos cuando $j = 1728$, y para $j = 0$ hay 6 automorfismos. Si $j = 0 = 1728$, se tienen 24 autormorfismos para $p = 2$ y 12 autormorfismos cuando

$p = 3$. Es decir, si conocemos el invariante j y la característica del cuerpo, se sabe la cantidad de automorfismos.

Para cerrar veamos un último ejemplo. Sean las curvas elípticas $E_1 : y^2 = x^3 + x + 4$ y $E_2 : 2y^2 = x^3 + 5x + 3$, sobre $\mathbb{F}_{11}$, cuyas gráficas presentamos a continuación.

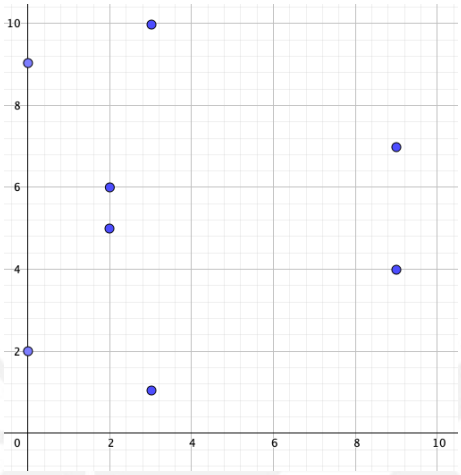

Figura 5.1: La curva E_1 en $\mathbb{F}_{11}$

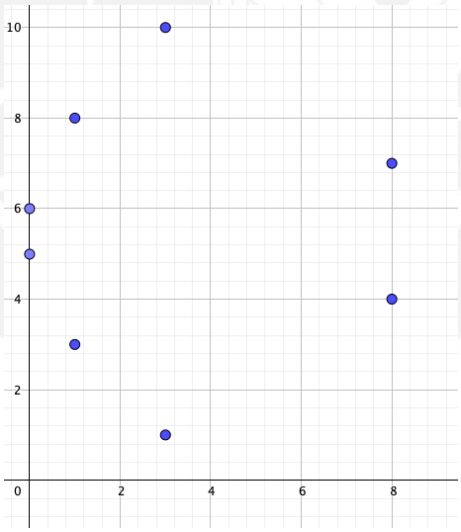

Figura 5.2: La curva E_2 en $\mathbb{F}_{11}$

En este caso $\phi : E_1 \to E_2$ definido por $\phi(x, y) = (4x, 8y)$ es un isomorfismo.

Asimismo tomemos $E_1 : y^2 = x^3 + x + 4$ y $E_3 : y^2 = x^3 + 4x + 10$, también sobre $\mathbb{F}_{11}$, La gráfica de E_3 está dada en la Figura 5.4.

Resulta que $\psi : E_1 \to E_2$, definido por $\psi(x, y) = (2x, 2uy)$ es un twist, donde $u \in \overline{\mathbb{F}}_{11}$ satisface $u^2 = 2$. Como dato anecdótico notemos que apreciamos menos puntos en la gráfica de E_1 que en la de E_3, pues u no pertenece $\mathbb{F}_{11}$.

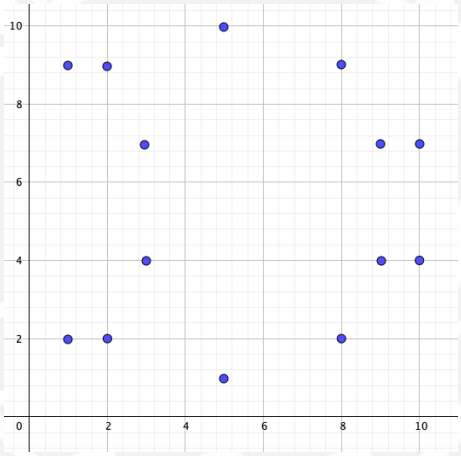

Figura 5.3: La curva E_3 en $\mathbb{F}_{11}$

Referencias

[1] Bauer, Ludwig, *Weierstrass equations*. Seminar on elliptic curves and the Weil conjectures, University of Regensburg, 2016.

[2] Cassels, J.W.S, *Lectures on elliptic curves*. London Mathematical Society Student Text 24 (1991).

[3] Connell, I, *Elliptic Curve Handbook*. McGill, 1999.

[4] Galbraith, Steven, *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012.

[5] Fulton, William, *Algebraic Curves. An Introduction to Algebraic Geometry*. Addison-Wesley, Chicago, 1969.

[6] Harris J, *Algebraic Geometry*. Springer Verlag, New York, 1992.

[7] Ivorra Castillo, Carlos, *Curvas elípticas*, <https://www.uv.es/ivorra/Libros/Elípticas.pdf>.

[8] Medina, Ruth, *Criptografía con curvas elípticas sobre cuerpos p-ádicos*. Tesis de Maestría, UNI, 2012.

[9] Navas Orozco, Jesús, *Curvas Elípticas y el Teorema de Mordell*. Memoria presentada como parte de requisitos para la obtención de Grado en Matemáticas, Universidad de Sevilla, 2019.

[10] Perez, Iván, *Associativity of the group operation on elliptic curves*. Tesis de Licenciatura, PUCP, 2017.

[11] Qureshi, Claudio, *Criptografía de curvas elípticas y logaritmo discreto*. Tesis de Maestría, Universidad de la República, 2012.

[12] Reid, Miles, *Undergraduate Algebraic Geometry*. Cambridge University Press, 1989.

[13] Santos Nunes, Hugo, *Curvas elípticas e o Teorema de Mordell-Weil*. Tesis de Maestría, Universidad Federeal de Alagoas, 2015.

[14] Shumow, Daniel, *Isogenies of Elliptic Curves: A Computational Approach*. Master of Science Thesis, Washington University, 2009.

[15] Silverman, Joseph, *The arithmetic of elliptic curves*. Springer-Verlag, New York, 2009.

[16] Sutherland, Andrew, *Isogenies*, <https://math.mit.edu/classes/18.783/2021/lectures.html>.