ISOGENIAS.

1 Notación.

Sea K un cuerpo, y $\overline{K}$ una clausura algebraica fija. ($\overline{K}$ es el cuerpo formado por todos los elementos algebraicos sobre K). Como es habitual el plano proyectivo se define como las ternas de $\overline{K}$, módulo aquellas que son proporcionales. Concretamente

$$\mathbb{P}^2 = \{[X,Y,Z] \in \overline{K}^3 - [0,0,0]\} / \sim$$

de forma que $[X,Y,Z] \sim [X_1,Y_1,Z_1]$ si existe $\lambda \in \overline{K}$ tal que $X = \lambda X_1$, $Y = \lambda Y_1$, $Z = \lambda Z_1$. Si $Z \neq 0$, entonces ambos cocientes, $\frac{X}{Z} = x$ y $\frac{Y}{Z} = y$, estan bien definidos dentro de la misma clase de equivalencia, por lo que podemos escribir $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$, donde $A^2 = \{(x,y) \in \overline{K}$ es el plano afin y $\mathbb{P}^1 = \{P \in \mathbb{P}^2 \,:\, Z = 0\}$ se conoce como recta del infinito. Cuando un conjunto esté descrito en términos de las variables X, Y, Z diremos que está en coordenadas homogeneas. Por otro lado las variables x e y serán las coordenadas afines del conjunto. En este contexto se hace la siguiente definición.

Definición 1. *Una curva elíptica es un subconjunto de $\mathbb{P}^2$ descrito como el lugar de ceros de un polinomio homogéneo cúbico no singular.*

$$E = \{P \in \mathbb{P}^2 \,:\, F(P) = 0\} \text{ donde}$$

$$F([X,Y,Z]) = ZY^2 + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \tag{1}$$

Obsérvese que, a pesar de que no está bien definido el valor de un polinomio sobre puntos de $\mathbb{P}^2$, si que tiene perfecto sentido determinar aquellos puntos que lo anulan. Ahora bien, el único punto de la recta del infinito que es solución de (1) es el punto $O = [0,1,0]$, es decir, salvo el punto O toda la curva elíptica se encuentra en la parte afin $\mathbb{A}^2$ del plano proyectivo, por lo que es suficiente describirla en coordenadas afines.

Definición 2. *Una curva elíptica E es el subconjunto de $\mathbb{A}^2$ dado por*

$$E = \{(x,y) \in \mathbb{A}^2 \,:\, f(x,y) = 0\} \cup \{O\}, \text{ donde}$$

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \tag{2}$$

aparece al deshomogeneizar el polinomio $F[X,Y,Z]$. *En este contexto, para que la curva sea no singular, se ha de tener* $(\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})_P \neq (0,0)$ *en todo punto* $P \in E$. *A las ecuaciones del estilo* (1) *o* (2) *se conocen como ecuaciones de Weierstrass de la curva* E, *y se suele utilizar la notación* $E = [a_1, a_3, a_2, a_4, a_6]$.

Definición 3. *Se dice que la curva* E *está definida sobre* L, *un cuerpo extensión de* K, *si* $a_i \in L$ *para todo* i. *En ese caso se escribe* E/L.

La ecuación de Weierstrass que define una determinada curva no es única ya que, si cambiamos x por $x+1$ en (2), nos dará otra ecuación que describe el mismo conjunto de puntos, salvo que trasladados una unidad. En este sentido es posible demostrar lo siguiente

Teorema 1. *Los únicos cambios de variable que mantienen el punto* $\{O\}$ *fijo y mandan una ecuación de Weiertrass* $E = [a_1, a_3, a_2, a_4, a_6]$ *en otra* $E' = [a_1', a_3', a_2', a_4', a_6']$ *son de la forma*

$$\begin{aligned} \psi : E &\longrightarrow E' \\ (x,y) &\to (x',y'), \end{aligned}$$

tal que

$$\begin{aligned} x &= u^2 x' + r \\ y &= u^3 y' + s u^2 x' + t, \end{aligned}$$

con $u, r, s, t \in \overline{K}$ *y* $u \neq 0$.

Demostración. [Sil, Prop. 3.1, pag. 63]

Definición 4. *Dos curvas elípticas* E, E' *son isomorfas,* $E \simeq E'$, *si existe un isomorfismo, (o cambio de variable),* $\psi(x,y)$ *como en el Teorema 1 que las relaciona. Si* $u, r, s, t \in K$ *se dice que* ψ *esta definido sobre* K, *o también que las curvas son isomorfas sobre* K.

Teniendo en cuenta que el cambio de variable viene descrito por polinomios lineales, es fácil ver el aspecto de los coeficientes de la curva E' en términos de E y las variables u, r, s, t. Concretamente,

Lema 1. *Sean*

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\ y\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= c_4^3/\Delta.
\end{aligned}$$

Entonces

$$\begin{aligned}
ua_1' &= a_1 + 2s,\\
u^2a_2' &= a_2 - sa_1 + 3r - s^2,\\
u^3a_3' &= a_3 + ra_1 + 2t,\\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,\\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,\\
u^4c_4' &= c_4,\\
u^{12}\Delta' &= \Delta\\
j' &= j.
\end{aligned}$$

Las dos cantidades definidas anteriormente, Δ y j, son de extrema importancia en la curva elíptica. Por un lado el discriminante Δ nos permite decidir si la curva es singular cuando éste es igual cero. Por otro, si dos curvas elípticas son isomorfas, entonces tienen el mismo invariante j. De hecho esta condición es suficiente.

Teorema 2. *$E \simeq E'$ si y sólo si $j = j'$.*

Demostración. [Sil, Prop. 1.4, pag. 50]

Así pues, se pueden utilizar cambios de variable para reducir al máximo las ecuaciones que definen a una curva elíptica. En concreto se puede demostrar

Lema 2. *Toda curva elíptica E/K es isomorfa a una de las que aparecen en la siguiente tabla.*

$\text{char}(K) = 2$ $\Delta = a_3^4, j = 0$	$y^2 + a_3 y = x^3 + a_4 x + a_6$
$\text{char}(K) = 2$ $\Delta = a_6, j = 1/a_6$	$y^2 + xy = x^3 + a_2 x^2 + a_6$
$\text{char}(K) = 3$ $\Delta = a_3^4 a_6, j = 0$	$y^2 = x^3 + a_4 x + a_6$
$\text{char}(K) = 3$ $\Delta = -a_2^3 a_6, j = \Delta/a_6^2$	$y^2 = x^3 + a_2 x^2 + a_6$
$\text{char}(K) \neq 2, 3$ $\Delta = -432 a_6^2, j = 0$	$y^2 = x^3 + a_6$
$\text{char}(K) \neq 2, 3$ $\Delta = -16(4a_4^3 + 27a_6^2)$ $j = -1728(4a_4)^3/\Delta$	$y^2 = x^3 + a_4 x + a_6$

Tabla 1. Modelos de Weierstrass reducidos de curvas elípticas.

Observese que en este caso el isomorfismo estará definido sobre el mismo cuerpo K, lo que permite mantener tanto la estructura geométrica de E, como el caracter algebraico de cada uno de los puntos de la curva. En este sentido es importante observar que, independientemente del cuerpo de definición, una curva elíptica es un conjunto infinito de puntos, ya que viene definida como los ceros de un polinomio en dos variables en un cuerpo algebraicamente cerrado. Lo que nos interesa es estudiar el subconjunto de puntos K-racionales

Problema. *Estudiar el número de puntos K-racionales de una curva elíptica E/K definida sobre K,*

$$E(K) = \{P \in E \,:\, (x, y) \in K^2\} \cup \{O\}.$$

Es bien sabido que, dada una curva elíptica E/K, y una extensión de K, L, entonces $E(L)$ tiene estructura de grupo conmutativo con neutro el punto O y operación dada mediante las siguientes ecuaciones polinómicas dependiendo de la característica del cuerpo.

$\mathrm{char}(K) = 2$ $j = 0, P \neq Q$	$x_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + x_1 + x_2$ $y_3 = \frac{y_1+y_2}{x_1+x_2}(x_1 + x_3) + y_1 + a_3$
$\mathrm{char}(K) = 2$ $j = 0, P = Q$	$x_3 = \frac{x_1^4+a_4^2}{a_3^2}$ $y_3 = \frac{x_1^2+a_4}{a_3}(x_1 + x_3) + y_1 + a_3$
$\mathrm{char}(K) = 2$ $j \neq 0, P \neq Q$	$x_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a_2$ $y_3 = \frac{y_1+y_2}{x_1+x_2}(x_1 + x_3) + y_1 + x_3$
$\mathrm{char}(K) = 2$ $j \neq 0, P = Q$	$x_3 = x_1^2 + \frac{a_6}{x_1^2}$ $y_3 = x_1^2 + (x_1 + \frac{y_1}{x_1})x_3 + x_3$
$\mathrm{char}(K) = 3$ $j = 0, P \neq Q$	$x_3 = \left(\frac{y_1-y_2}{x_1-x_2}\right)^2 - x_1 - x_2$ $y_3 = \frac{y_2-y_1}{x_2-x_1}(x_2 - x_3) - y_2$
$\mathrm{char}(K) = 3$ $j = 0, P = Q$	$x_3 = \left(\frac{a_4}{2y_1}\right)^2 - 2x_1$ $y_3 = \frac{a_4}{2y_1}(x_1 - x_3) - y_1$
$\mathrm{char}(K) = 3$ $j \neq 0, P \neq Q$	$x_3 = \left(\frac{y_1-y_2}{x_1-x_2}\right)^2 - a_2 - x_1 - x_2$ $y_3 = -\frac{y_2-y_1}{x_2-x_1}x_3 - \frac{y_1x_2-y_2x_1}{x_2-x_1}$
$\mathrm{char}(K) = 3$ $j \neq 0, P = Q$	$x_3 = \frac{a_2x_1}{y_1^2} - a_2 - 2x_1$ $y_3 = -x_3\frac{a_2x_1}{y_1} - \frac{x_3-a_4x_1-2a_6}{2y_1}$
$\mathrm{char}(K) \neq 2, 3$ $P \neq Q$	$x_3 = \left(\frac{y_1-y_2}{x_1-x_2}\right)^2 - x_1 - x_2$ $y_3 = \frac{y_2-y_1}{x_2-x_1}(x_2 - x_3) - y_2$
$\mathrm{char}(K) \neq 2, 3$ $P = Q$	$x_3 = \left(\frac{3x_1^2+a_4}{2y_1}\right)^2 - 2x_1$ $y_3 = \frac{3x_1^2+a_4}{2y_1}(x_1 - x_3) - y_1$

Tabla 2. Ecuaciones de la suma en una curva elíptica.

En el caso de que $K = \mathbb{F}_q$, $q = p^n$, sea un cuerpo finito, entonces $E(K)$ es un grupo finito con, como mucho, $\#\mathbb{A}^2(K) + 1 = q^2 + 1$ elementos. De hecho, es fácil obtener una cota mas aproximada al verdadero número de puntos de la curva sobre $\mathbb{F}_q$. Efectivamente, Supongamos que la curva está definida por una ecuación del estilo $y^2 = f(x)$. Entonces, dado $x \in \mathbb{F}_q$, si $f(x) \neq 0$ habrá o bien dos soluciones, o ninguna, y cada uno de los casos ocurrirá mas o menos la mitad de las veces. Por otra parte $f(x) = 0$ exactamente en tres ocasiones pues

es no singular. Añadiendo el punto del infinito tenemos

$$\#E(\mathbb{F}_q) \approx 2(\frac{q-3}{2}) + 3 + 1 = q + 1.$$

De hecho, el error cometido en esta aproximación se puede acotar gracias a la desigualdad de Hasse

Teorema 3. *(Desigualdad de Hasse) Dada $E/\mathbb{F}_q$, entonces*

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Demostración. [Sil, Teo. 1.1, pag. 131]

2 Definición y Ejemplos de isogenias.

Asi pues, el problema consiste en calcular el error exacto que se comente en la aproximación de Hasse. Ahora bien, si tenemos un conjunto finito, una forma posible de calcular su cardinal es a traves de las aplicaciones del conjunto en si mismo. De esta forma, un conjunto de cardinal 1 solamente puede tener una aplicación en si mismo. Si además el conjunto tiene cierta estructura, lo que nos interesará es entender aquellas aplicaciones que conservan la estructura. En general, las aplicaciones entre curvas elípticas que conservan la estructra se les llama isogenias, es decir, homomorfismos de grupo definidos de forma algebraica.

Definición 5. *Sean E_1/K, E_2/K curvas elípticas definidas por $F_1[X,Y,Z]$ y $F_2[X,Y,Z]$ respectivamente. Una isogenia $\varphi : E_1 \to E_2$ es una aplicación racional, es decir, $\varphi([X,Y,Z]) = [\varphi_1, \varphi_2, \varphi_3]$, tal que para $i = 1,2,3$, $\varphi_i \in \overline{K}[X,Y,Z]/F[X,Y,Z]$ son homogéneos del mismo grado con $\varphi_i \neq F_1 G$ para algún i, y para todo $G \in \overline{K}[X,Y,Z]$ homogeneo, y que cumple*

i) *Si $P \in E_1$ entonces $\varphi(P) \in E_2$,*
ii) *$\varphi(P+Q) = \varphi(P) + \varphi(Q)$*

Ejemplo 1. Sea $m \in \mathbb{Z}$. La aplicación $[m] : E \longrightarrow E$, multiplicar por m, es una isogenia. Observese que trivialmente es un homomorfismo, ya que E es un grupo conmutativo. Por otro lado, que la aplicación es racional se deduce de la Tabla 2 escribiendo m en base 2. Por último si $P \in E$ claramente $mP \in E$ por definición de grupo.

Definición 6. *Las isogenias con imagen la misma curva origen se llaman endomorfismos y se denotan por End(E).*

Es interesante observar que dos enteros $m \neq m'$ dan isogenias distintas. Con lo que, en particular, deducimos que End(E) es un conjunto infinito y que $\mathbb{Z} \subset$End(E). Para ello, restando $m - m'$, basta observar que ningun entero produce la isogenia constante.

Proposición 1. *Sea E una curva elíptica. Entonces $[m]$ es una isogenia no constante.*

Demostración. [Sil. Prop. 4.2, pag. 71]

Es un hecho básico que cualquier homomorfismo de grupos manda el neutro al neutro. Una propiedad de extrema importancia en las aplicaciones racionales entre curvas elípticas es que esta, en realidad, es una condición suficiente.

Proposicion 2. *Sea $\varphi : E_1 \to E_2$ una aplicación racional tal que $\varphi(O) = (O)$. Entonces es una isogenia.*

Para la demostración nos hará falta establecer un lema previo. Dada una una curva elíptica E consideramos el grupo $\mathrm{Pic}^0(E) = \sum n_i P_i$ con la operación natural de suma, formado por sumas finitas con $n_i \in \mathbb{Z}$, $P_i \in E$, módulo la relación de equivalencia $\sum n_i P_i = 0$ si y solo si $\sum [n_i]P_i = O$.

Lema 3. *$E \simeq Pic^0(E)$ donde el isomorfismo $\mathfrak{i}$ viene dado por $\mathfrak{i}(P) = P - O$.*

Demostración. La aplicación es inyectiva de forma trivial. Por otro lado si $\mathcal{P} = \sum n_i P_i \in \mathrm{Pic}^0(E)$, entonces, $Q = \sum [n_i]P_i \in E$ y $\mathfrak{i}(Q) = Q - O = \mathcal{P}$, por lo que la aplicación es sobreyectiva. Que efectivamente $\mathfrak{i}$ es un homomorfismo se deduce de la definición.

Demostración de la Proposición 2. Lo único que debemos demostrar es que si la aplicación manda O en O entonces es un homomorfismo. Ahora bien, toda aplicaión racional $\varphi : E_1 \to E_2$ en estas condiciones induce trivialmente un homomorfismo de grupos $\varphi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$ tal que $\varphi(\sum n_i P_i) = \sum n_i \varphi(P_i)$. De esta forma, si $\varphi(O) = O$, entonces el diagrama

$$\begin{array}{ccc} E_1 & \xrightarrow{\mathfrak{i}_1} & \mathrm{Pic}^0(E_1) \\ \varphi \downarrow & & \downarrow \varphi_* \\ E_2 & \xrightarrow{\mathfrak{i}_2} & \mathrm{Pic}^0(E_2) \end{array}$$

es conmutativo. Teniendo en cuenta que $\mathfrak{i}_1$, $\mathfrak{i}_2$, y φ_* son homomorfismos y $\mathfrak{i}_2$ es inyectivo se obtiene el resultado.

La proposición anterior nos permite, por un lado, comprobar mas fácilmente si cierta aplicación racional es una isogenia, ya que evitamos la condicion *ii*) de la definición. Por otro lado, teniendo en cuenta que el neutro es el único punto del infinito de la curva elíptica, basta describir una isogenia en la parte afin

del plano proyectivo con lo cual la isogenia queda $\Phi([X,Y,Z]) = \Phi([x,y,1]) = \varphi(x,y)$ con $\varphi(x,y) = [\varphi_1(x,y), \varphi_2(x,y), \varphi_3(x,y)]$, una 3-upla de polinomios en $K[x,y]/f(x,y)$. Si además nos restringimos al conjunto $\varphi_3(x,y) \neq 0$ entonces, dividiendo por la tercera coordenada, queda

$$\varphi(x,y) = \left[\frac{\varphi_1(x,y)}{\varphi_3(x,y)}, \frac{\varphi_2(x,y)}{\varphi_3(x,y)}, 1\right] = (\phi_1(x,y), \phi_2(x,y)).$$

De esta forma, podemos reformular nuestra definición de isogenia de la siguiente manera. Dada una curva elíptica E/K definida mediante un polinomio $f(x,y)$, llamaremos $\overline{K}(E)$ como el cuerpo de fracciones de $\overline{K}[x,y]/f(x,y)$. $K(E)$ se define análogamente como el subconjunto de fracciones de $\overline{K}(E)$ con coeficientes en el cuerpo K.

Definición 7. *Sean E_1/K, E_2/K curvas elípticas definidas mediante $f_1(x,y)$ y $f_2(x,y)$ respectivamente. Una isogenia es una pareja $\phi(x,y) = (\phi_1, \phi_2)$, con $\phi_i \in \overline{K}(E)$, $i = 1,2$, que cumple*

i) *Si $P \in E_1$ entonces $\varphi(P) \in E_2$.*

Si $\phi_i(x,y) \in K(E)$ para $i = 1,2$, entonces se dice que la isogenia está definida sobre K.

A las isogenias dadas mediante la definición anterior las llamaremos isogenias afines. Obsérvese que la aplicación no estará bien definida allí donde se anule el denominador. Ahora bien, esto ocurre exactamente en los ceros del polinomio $\varphi_3(x,y)$ en la curva E_1. Por otro lado, como por definición de isogenia se tiene que $[\varphi_1(x,y), \varphi_2(x,y), \varphi_3(x,y)]$ es un punto en E_2, $\varphi_3(x,y)$ se hará cero solamente cuando la imagen sea el punto del infinito en la curva E_2. Dicho de otra forma, los puntos no definidos mediante la Definición 6 son exactamente aquellos que van a parar al elemento neutro en E_2, es decir, el nucleo de la isogenia. Resumiendo

Observación 1. *El nucleo de la isogenia viene determinado por los ceros de un polinomio.*

Esta caracterización nos permite encontrar nuestro segundo ejemplo trivial de isogenia en los isomorfismos del Teorema 1. Teniendo en cuenta además que es una aplicación biyectiva se tiene

Proposición 3. *Sea $\psi : E_1 \to E_2$ un isomorfismo de curvas elípticas. Entonces ψ es una isogenia, que es un isomorfismo de grupos.*

Es importante observar que, en este caso, la isogenia afin viene dada por polinomios, por tanto el denominador no se anula nunca, es decir, el nucleo de la isogenia es trivial.

Si tenemos en cuenta la propia definición de nuestra curva, se pueden encontrar ejemplos mas generales de isogenias de curvas elípticas. En particular es fácil ver que las curvas $E_1 \equiv y^2 = x^3 + \beta x$ y $E_2 \equiv y^2 = x^3 - 4\beta x$ son isógenas mediante la aplicación $\phi(x,y) = (y^2/x^2, y(\beta - x^2)/x^2$, si $(x,y) \neq (0,0)$, $\phi(0,0) = O$. Efectivamente, lo único que debemos demostrar es que si $P \in E_1$, entonces $\phi(P) \in E_2$. Ahora bien, si $P = (x,y) \in E_1$, entonces trivialmente

$$(x^2 - \beta)^2 = (x^2 + \beta)^2 - 4\beta x^2 = \frac{y^4}{x^2} - 4\beta x^2.$$

Multiplicando por y^2/x^4 queda

$$\left(\frac{y(x^2-\beta)}{x^2}\right)^2 = \left(\frac{y^2}{x^2}\right)^3 - 4\beta\left(\frac{y^2}{x^2}\right),$$

con lo que $\phi(P)$ es un punto de E_2 como queríamos ver. Obsérvese que, en este caso, el denominador de la isogenia se anula cuando $x = 0$. Los únicos puntos de E_1 con primera coordenada cero son O y el $(0,0)$ que forman el nucleo de la isogenia.

En general, dada una curva de ecuación[1] $y^2 = x^3 + \alpha x^2 + \beta x$, se tiene que $y^2 - \alpha x^2 = x^3 + \beta x$, con lo que se puede utilizar el mismo truco de antes, completando cuadrados, para demostrar el siguiente resultado.

Proposicion 4. *Sea $\phi(x,y) = (y^2/x^2, y(\beta - x^2)/x^2)$ si $x \neq 0$, $\phi(0,0) = O$. Entonces ϕ es una isogenia entre las curvas elípticas $E_1 \equiv y^2 = x^3 + \alpha x^2 + \beta x$, y $E_2 \equiv y^2 = x^3 - 2\alpha x^2 + (\alpha^2 - 4\beta)x$, con nucleo $< O, (0,0) >$.*

Esta isogenia está en el centro del método AGM para contar puntos de curvas elípticas, por lo que será interesante hacer hincapie en una serie de propiedades importantes. En primer lugar obsérvese que la curva imagen E_2 es en realidad del mismo estilo que E_1. En este sentido basta componer con un isomorfismo en la curva E_2 para poner de manifiesto esta simetría en el proceso anterior. Concretamente, si escribimos el polinomio $f_1(x) = x^3 + \alpha x^2 + \beta x$ en términos de sus raíces de la forma $f(x) = x(x - a^2)(x - b^2)$, E_2 quedará definida mediante $f_2(x) = x^3 + 2(a^2 + b^2)x^2 + (a^2 - b^2)^2 x$. Es suficiente ahora "trasladar" la coordenada x para obtener la siguiente proposición. En el enunciado usaremos la misma notación introducida anteriormente. Además, dados $a, b \in K$, llamaremos $a_1 = (a+b)/2$, $b_1 = \sqrt{ab}$, a sus medias aritmética y geométrica respectivamente.

[1] Es fácil ver que cualquier curva elíptica E/K, $\mathrm{char}(K) \neq 2$, con un punto de 2-torsión definido sobre K, tiene una ecuación de este estilo.

Proposición 5. *Consideramos el cambio de variable en E_2 dado por $\psi(x,y) = (x/4 + a_1^2, -y/8)$. Entonces si $E_{a,b} \equiv y^2 = x(x-a^2)(x-b^2)$, se tiene que la aplicación $AGM = \psi \circ \phi : E_{a,b} \longrightarrow E_{a_1,b_1}$ dada por*

$$AGM(x,y) = (\frac{y^2}{4x^2} + a_1^2, -\frac{-y(a^2b^2 - x^2)}{8x^2}),$$

es una isogenia.

De hecho veremos que la isogenia AGM es la mas sencilla que existe entre dos curvas del estilo $E_{a,b}$, $E_{c,d}$, salvo en el caso de que éstas sean en realidad curvas isomorfas. No hay más que observar las ecuaciones de las curvas y de sus j invariantes respectivos para determinar en que casos se obtiene un isomorfismo.

Observación 2. *$E_{a,b} \simeq E_{c,d}$ si y sólo si el isomorfismo es del estilo $\psi(x,y) = (u^2x, u^3y)$ con $u^2 = \frac{c^2+d^2}{a^2+b^2}$ y, o bien $\left(\frac{a}{b}\right)^2 = \left(\frac{c}{d}\right)^2$, o $\left(\frac{a}{b}\right)^2 \left(\frac{d}{c}\right)^2$.*

Es conveniente resaltar que la aplicación AGM se ha definido como composición de isogenias. Es sin embargo un hecho trivial que en general la composición de isogenias define una isogenia, lo que será de extrema importancia para el desarrollo posterior de la teoría.

Lema 4. *Sean $\phi_1 : E_1 \to E_2$ y $\phi_2 : E_2 \to E_3$ isogenias de curvas elípticas. Entonces $\phi_2 \circ \phi_1 : E_1 \to E_3$ es también una isogenia.*

Demostración. Trivial

Por último si nos fijamos en las ecuaciones de AGM, vemos que, para que esté bien definida, debemos imponer que la característica del cuerpo sea distinta de 2 ya que aparece un 2 en el denominador de sus ecuaciones.

A parte del fenómeno descrito anteriormente, las isogenias que han aparecido hasta ahora estan definidas, de forma genérica, independientemente de la característica del cuerpo. Si nos restringimos a característica positiva, aparece una nueva isogenia determinante a la hora de hacer el recuento de puntos de una curva elíptica sobre cuerpos finitos. Concretamente, sea $K = \mathbb{F}_q$ el cuerpo de $q = p^n$ elementos, con p un número primo, y sea $E/\mathbb{F}_q$ una curva elíptica.

Proposición 6. *Las curvas $E = [a_1, a_3, a_2, a_4, a_6]$ y $\sigma(E) = [a_1^p, a_3^p, a_2^p, a_4^p, a_6^p]$ son isógenas mediante la aplicación*

$$\begin{aligned} F_p : E &\longrightarrow \sigma(E) \\ (x,y) &\to (x^p, y^p), \end{aligned}$$

denominada pequeño Frobenius.

Demostración. Una simple aplicación del binomio de Newton en característica p nos permite deducir

$$(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6)^p \\ = (y^p)^2 + a_1^p x^p y^p + a_3^p y^p - (x^p)^3 - a_2^p (x^p)^2 - a_4^p x^p - a_6^p,$$

por tanto, es inmediato observar que si $P \in E$, $F_p(P) \in \sigma(E)$.

Observese además que, como la aplicación se define mediante polinomios, el nucleo de la isogenia es el trivial.

Iterando el pequeño Frobenius se obtiene una cadena de curvas isogenas

$$E \to \sigma(E) \to \sigma^2(E) \cdots \sigma^r(E) \to \cdots$$

en donde $\sigma^r(E) = [a_1^{p^r}, a_3^{p^r}, a_2^{p^r}, a_4^{p^r}, a_6^{p^r}]$, con las aplicaciones $F_{p^r} : E \to \sigma^r(E)$ tal que $F_{p^r}(x, y) = (x^{p^r}, y^{p^r})$. Es fácil ver que este proceso es en realidad cíclico de longitud n, es decir,

Proposición 7. *$\sigma^n(E) = E$, y la aplicación definida de la siguiente forma*

$$F_r : E \longrightarrow \sigma^n(E) \\ (x, y) \to (x^q, y^q),$$

es un endomorfimos de curvas elípticas, llamado endomorfismo de Frobenius.

Demostración. La demostración se basa en una caracterización apropiada de los elementos en un cuerpo finito. Es bien conocido que el cuerpo finito de q elementos se puede obtener como la extensión $\mathbb{F}_p[\alpha]$ donde α es una raíz de un polinomio irreducible sobre $\mathbb{F}_p$ de grado n, o también como cuerpo de descomposición del polinomio $x^q - x$ sobre $\mathbb{F}_p$. En particular un elemento $x \in \overline{\mathbb{F}}_p$ esta en $\mathbb{F}_q$ si y sólo si cumple $x^q - x = 0$. Teniendo en cuenta la ecuación de $\sigma^n(E)$ observamos que, efectivamente, es un endomorfismo.

Esta caracterización de los elementos de $\mathbb{F}_q$ servirá de forma decisiva a la hora de hacer el recuento de puntos. Efectivamente, teniendo en cuenta las ecuaciones del endomorfismo de Frobenius, de forma inmediata obtenemos el siguiente teorema

Teorema 4. *Sea $E/\mathbb{F}_q$. Entonces $\#E(\mathbb{F}_q) = \#Ker(1 - Fr)$, donde 1 es el endomorfismo identidad.*

Demostración. Observese que dos puntos son iguales si y sólo si tienen las mismas coordenadas, por tanto $P \in Ker(1 - Fr)$ si y sólo si $x = x^q, y = y^q$, es decir, está definido sobre $\mathbb{F}_q$.

Asi pues, el recuento de puntos de curvas elípticas sobre cuerpos finitos se reduce a entender el núcleo de endomorfismos de la curva.

3 Núcleo

Definición 8. *Sea $\phi : E_1 \to E_2$ una isogenia de curvas elípticas. Entonces*

$$E_1[\phi] = Ker(\phi) = \{P \in E_1 \, : \, \phi(P) = O\},$$

es el núcleo de la isogenia.

Ejemplo 2. Ya hemos visto que, en el caso de un isomorfismo ψ, entonces $Ker(\psi) = O$, $E[AGM] =< O, (0,0) >$, y $E[F_{p^r}] =< O >$. En el caso de la multiplicación por un entero m, se puede demostrar que

Teorema 5. *Sea E una curva elíptica, l un número primo. Entonces*

1) *Si $l \neq charK$, entonces $E[l^e] \simeq \mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$ para todo $e = 1, 2, \ldots$.*
2) *Si $l = p = char(K)$ entonces,*
   - 2.1 *$E[l^e] \simeq O$, para todo $e = 1, 2, \ldots$, o*
   - 2.2 *$E[l^e] \simeq \mathbb{Z}/p^e\mathbb{Z}$ para todo $e = 1, 2, \ldots$*

Demostración. [Sil. Cor. 6.4, pag 89].

Entre las dos posibilidades en 2, la primera se da en un número finito de casos (Ver [Sil. pag 141]) que se comportan de manera singular en la teoría. Este motivo nos lleva a hacer la siguiente definición.

Definición 9. *Si $E[p^e] \simeq O$, es decir, no tiene p-torsión, entonces se dice que la curva es supersingular*

De entre las propiedades especiales de este tipo de curvas, quizá la que mas debamos destacar en este momento es que es inmediato contar el número de puntos de tales curvas sobre cuerpos finitos. Por ejemplo dada una curva supersingular $E/\mathbb{F}_p$ con $p > 3$, se tiene $\#E(\mathbb{F}_p) = p + 1$. (Ver [Sil. pag 145]).

Se puede deducir del Teorema 5 que, dado un entero m, existen m^2 puntos de m-torsión, salvo que el entero no sea primo con la característica del cuerpo de definición de la curva, en cuyo caso se reduce radicalmente el número de puntos de la torsión correspondiente. A pesar de que la demostración del teorema no es necesaria para nuestros propósitos, no es muy difícil dar una idea que nos

permita explicar este fenómeno. En la Observación 1 vimos que el núcleo de una isogenia venía determinado por los ceros del polinomio φ_3 allí definido. Supongamos por un momento que el polinomio fuese de una variable. Entonces el cardinal del núcleo sería exactamente el grado del polinomio, salvo en el caso de que éste tuviese raíces repetidas. Ahora bien, un polinomio tiene una raíz repetida cuando ésta también es raíz de su derivada. En característica positiva cualquier polinomio del estilo $f(x) = g(x^p)$ tiene todas sus raíces comunes con la derivada. En el caso de isogenias entre curvas elípticas se puede demostrar el siguiente resultado.

Proposición 8. *Sean $E_1/\mathbb{F}_q$, $E_2/\mathbb{F}_q$ curvas elípticas isógenas por $\phi : E_1 \to E_2$. Entonces existe un r maximal y una isogenia δ tal que el siguiente diagrama es conmutativo*

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ & {\scriptstyle F_{p^r}}\searrow \quad \nearrow{\scriptstyle \delta} & \\ & \sigma^r(E_1) & \end{array}$$

Se entiende que r es maximal cuando δ no se puede escribir como función de (x^p, y^p).

Demostración. [Sil. Cor. 2.12, pag. 30].

En este sentido se hace la siguiente definición.

Definición 10. *Decimos que una isogenia es separable si $r = 0$. Si $r > 0$ entonces se dice inseparable y si además δ es un isomorfismo, entonces se dice que ϕ es puramente inseparable.*

Obsérvese que, en caso de que la isogenia sea inseparable, entonces para $i = 1, 2$ se tiene $(\frac{\partial \phi_i}{\partial x}, \frac{\partial \phi_2}{\partial y}) = (0, 0)$ lo que nos da un método práctico de determinar el caracter de una isogenia concreta. Se puede demostrar lo siguiente.

Ejemplo 3. La isogenia AGM es separable y, si $E/\mathbb{F}_q$, entonces El endomorfismo $1 - Fr$ es separable. Por otro lado veremos que $[p]$ es inseparable mientras que F_r es puramente inseparable por definición. En este último caso $\delta = 1$.

En vista de lo anterior, y teniendo en cuenta que $E[F_p] = O$, en nuestro estudio del nucleo debemos distinguir la parte inseparable de la isogenia que no aportará puntos nuevos al núcleo de la isogenia composición. En este sentido la notación siguiente es de gran utilidad.

Definición 11. *En las condiciones de la Proposición 8, se define el grado de la isogenia como* $\deg(\phi) = p^r|Ker(\delta)|$.

Ejemplo 4.

$\deg(Fr) = q$ y, en general , $\deg(F_{p^r}) = p^r$.

$\deg(\psi) = 1$ para todo isomorfismo.

$\deg(AGM) = 2$ es consecuencia de que la isogenia es separable.

$\deg[m] = m^2$.

Obsérvese que del último ejemplo sólo hemos visto el caso en que $(p, m) = 1$ en el Teorema 5. El caso general lo demostraremos mas adelante en el Teorema 9.

Teniendo en cuenta que, dadas dos isogenias $\phi_1 : E_1 \to E_2$, $\phi_2 : E_2 \to E_3$ entonces $\ker(\phi_1) \subset \ker(\phi_2 \circ \phi_1)$, es fácil convencerse[2] de que el grado es en realidad una función multiplicativa respecto la composición.

Lema 5. $\deg(\phi_1 \circ \phi_2) = \deg(\phi_1)\deg(\phi_2)$

Esta sencilla observación nos permite demostrar un resultado que, sin embargo, resulta bastante espectacular.

Teorema 6. *Dos curvas elípticas* $E_1/\mathbb{F}_q$ *y* $E_2/\mathbb{F}_q$ *isógenas sobre* $\mathbb{F}_q$ *tienen el mismo número de puntos* $\mathbb{F}_q$*-definidos.*

Demostración. La misma idea que en la demostración de la Proposición 6 nos permite deducir que el siguiente diagrama es conmutativo

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ {\scriptstyle 1-Fr}\downarrow & & \downarrow{\scriptstyle 1-Fr} \\ E_1 & \xrightarrow{\phi} & E_2. \end{array}$$

El resultado es consecuencia de la multiplicatividad del grado y el Teorema 4.

Como hemos mencionado, después de la Proposición 8, el estudio del núcleo de una isogenia se reduce a su parte separable que, a su vez, está descrita como los ceros de un polinomio. Intuitivamente estos ceros se pueden escoger con completa libertad, con la única restricción de que la isogenia vaya a parar a la curva correspondiente. Esta flexibilidad nos permite demostrar un teorema de gran importancia sobre isogenias entre curvas elípticas.

[2]ver Proposición 9 mas adelante

Teorema 7. *Sea E una curva elíptica y $\Phi \leq E$ un subgrupo finito. Entonces existe una única curva elíptica E' y una isogenia separable ϕ tal que $\phi : E \to E'$ cumple*

$$Ker(\phi) = \Phi$$

Demostración. [Sil. Prop. 4.12, pag. 78].

De hecho el teorema es explícito en el sentido de que se puede proporcionar, de manera eficiente, ecuaciones tanto para la isogenia, como para la curva elíptica E'. Es conveniente resaltar que estas fórmulas, extensamente conocidas como Fórmulas de Velú, [Vel] en particular se encuentran implementadas en programas de manipulación simbolica como MAGMA.

Como corolario al teorema anterior se puede probar el siguiente resultado que nos será útil en el desarrollo posterior de la teoría.

Corolario 1. *Sea $\phi : E_1 \to E_2$ una isogenia separable y $\gamma : E_1 \to E_2$ tal que $Ker(\phi) \subset Ker(\gamma)$. Entonces existe $\lambda : E_2 \to E_3$ tal que $\gamma = \lambda \circ \phi$.*

Es decir, es posible descomponer isogenias, a traves de su núcleo.

Demostración. [Sil. Cor. 4.11, pag 76].

La isogenia λ del corolario es justamente la obtenida por las fórmulas de Velú con $Ker(\lambda) = \phi(Ker(\gamma))$. Obsérvese que si $\phi(P) = \phi(Q)$ con $Q \in Ker(\gamma)$, entonces $\phi(P - Q) = O$, con lo que $P - Q \in Ker(\phi) \subset Ker(\gamma)$.

4 La isogenia dual.

Una de las características mas importantes sobre isogenias de curvas elípticas es el hecho de que, a pesar de que del Teorema 7 se sigue que pueden tener nucleo tan grande como uno quiera, sin embargo, por ser aplicaciones suaves entre objetos compactos, se puede demostrar el siguiente resultado[3]

Proposición 9. *Toda isogenia no constante es sobreyectiva.*

Demostración. [Sil. Teo. 2.3, pag. 24].

Entre otras cosas este resultado nos permite volver hacia atras en la isogenia escogiendo alguna de las preimágenes. Es posible demostrar que, en cierta manera, existe una forma canónica de volver para atras mediante una isogenia, llamada isogenia dual.

[3]Una vez mas recuérdese que las curvas son conjuntos infinitos.

Teorema 8. *Sea $\phi : E_1 \to E_2$ una isogenia de grado m. Entonces existe una única isogenia $\hat{\phi} : E_2 \to E_1$ llamada isogenia dual tal que*

$$\hat{\phi} \circ \phi = [m].$$

Demostración. i) La isogenia es única. Supongamos $\hat{\phi}$ y $\hat{\phi}'$ dos isogenias con la misma propiedad. Entonces $(\hat{\phi} - \hat{\phi}') \circ \phi = [m] - [m] = O$, de donde se deduce el resultado ya que ϕ es sobreyectiva.

ii) Dadas dos isogenias $\phi : E_1 \to E_2$ y $\gamma : E_2 \to E_3$ de grados m y n respectivamente, supongamos que existen $\hat{\phi}$, y $\hat{\gamma}$. Entonces, teniendo en cuenta que son homomorfismos de grupos se tiene

$$(\hat{\gamma} \circ \hat{\phi}) \circ (\phi \circ \gamma) = \hat{\gamma} \circ [m] \circ \gamma = \hat{\gamma} \circ \gamma \circ [m] = [nm],$$

con lo que $(\phi \circ \gamma)\hat{} = \hat{\gamma} \circ \hat{\phi}$. Asi pues, teniendo en cuenta la Proposición 8, es suficiente demostrar el resultado para isogenias separables y para el pequeño Frobenius F_p. Ahora bien, si ϕ es separable $|Ker(\phi)| = m$, con lo cual, teniendo en cuenta que el orden de un elemento divide al orden del grupo, se tiene $Ker(\phi) \subset E[m]$. El resultado es ahora consecuencia del Corolario 1. Para la demostración del caso F_p ver [Sil. Teo. 6.1, pag. 84].

Casi de la propia definición se deducen una serie de propiedades de la isogenia dual que se recogen en el siguiente teorema.

Teorema 9. *Sea $\phi : E_1 \to E_2$ una isogenia. Entonces*

(a) *Si $m = \deg(\phi)$ entonces $\phi \circ \hat{\phi} = [m]$.*
(b) *Sea $\gamma : E_2 \to E_3$ otra isogenia. Entonces $(\phi \circ \gamma)\hat{} = \hat{\gamma} \circ \hat{\phi}$.*
(c) *Sea $\lambda : E_1 \to E_2$ otra isogenia. Entonces $(\phi + \lambda)\hat{} = \hat{\phi} + \hat{\lambda}$.*
(d) *$[m]\hat{} = [m]$ y $\deg([m]) = m^2$.*
(e) *$\deg(\hat{\phi}) = \deg(\phi)$.*
(f) *$\hat{\hat{\phi}} = \phi$.*

Demostración. Salvo (c) todas son consecuencia sencilla de la defínción. Ver [Sil. Teo. 6.2, pag. 86].

Ejemplo 5.

1)$\hat{\psi} = \psi^{-1}$ para todo isomorfismo.

2)$[m]\hat{} = [m]$.

3)Si $(AGM)\hat{} : E_{a_1,b_1} \to E_{a,b}$, entonces

$$(AGM)\hat{}(x,y) = \left(\frac{y^2}{(x-a_1^2)^2} + a_1^2, \frac{y((a^2-b^2) - 16(x-a_1^2)^2)}{8(x-a_1^2)^2} \right).$$

4)$\hat{Fr} = Ve$ (Verschiebung.)

La primera es inmediata. 2) se recoge en el Teorema 9. 3) Se puede deducir de forma sencilla mediante las fórmulas de Velú, ya que es fácil ver que $Ker(AGM)\hat{} =< O, (0,0) >$. Por último las ecuaciones concretas de la isogenia Verschiebung se pueden obtener de aquellas de $[p]$, por las definiciones del pequeño Frobenius e isogenia dual.

En este punto es importante observar que el caracter separable de una isogenia no es un invariante por dualidad. En el caso del Verschiebung se puede demostrar lo siguiente.

Lema 6. *$Ve : \sigma(E) \to E$ es separable si y sólo si E es ordinaria.*

Demostración. Por definición se tiene $V_e \circ F_p = [p]$, por tanto $Ker(Ve) \simeq \{O\} \Leftrightarrow E[p] = \{O\}$.

Esto nos permite obtener otra característica importante de las curvas supersingulares

Lema 7. *Sea $E/\mathbb{F}_q$ una curva elíptica supersingular. Entonces $j(E) \in \mathbb{F}_{p^2}$.*

Demostración. Si Ve es inseparable, por la Proposición 8 descompone a traves del Frobenius y, teniendo en cuenta el Teorema 9 (e), podemos comparar el grado de las isogenias para obtener un diagrama como el siguiente

$$\begin{array}{ccc} \sigma(E) & \xrightarrow{Ve} & E \\ & {\scriptstyle F_p}\searrow \quad \nearrow{\scriptstyle \psi} & \\ & \sigma^2(E) & \end{array}$$

con ψ un isomorfismo. Por tanto, por el Teorema 2, $j(E) = j(\sigma^2(E)) = j(E)^2$, en donde hemos utilizado la fórmula explicita del invariante j en términos de los coeficientes de la curva, (Lema 1), y las ecuaciones del Frobenius para la última igualdad. El resultado se sigue de la caracterización de $\mathbb{F}_{p^2}$ hecha después de la Proposición 7.

De entre las distintas aplicaciones que aparecen de la existencia de isogenia dual, quiza una de las mas llamativas esta en las consecuencias que produce en la estructura del conjunto de endomorfismos de una curva elíptica. Sea $E/\mathbb{F}_q$ una curva elíptica, y $\mathrm{End}(E)$ el conjunto de endomorfismos de la curva. La primera observación importante es que, en este caso, las isogenias se pueden sumar de forma natural de forma que, si $\phi_1, \phi_2 \in \mathrm{End}(E)$, entonces $\phi_1 + \phi_2(P) = \phi_1(P) + \phi_2(P)$. Es fácil ver que la suma, junto con la composición de isogenias,

dotan al conjunto End(E) de estructura de anillo. La isogenia dual será una herramienta decisiva para determinar la estructura concreta de este anillo.

Ya hemos visto después de la Proposicin 1 que End(E) tiene estructura de $\mathbb{Z}$ módulo. De hecho se puede ver que además es libre, íntegro y de característica 0. (Para la demostración ver [Sil. Prop. 4.2, pag 71]). Ahora bien, del Teorema 9 se deduce que $\hat{}$:End(E) $\rightarrow$End(E) es una antiinvolución, lo cual restringe a tres las posibles estructuras que puede adquirir End(E). Concretamente, (Ver [Sil. Teo. 9.3, pag. 100]), o bien es $\mathbb{Z}$, o un orden en un cuerpo cuadrático imaginario, o un orden en un álgebra de cuaterniones sobre $\mathbb{Q}$. En este sentido es fácil demostrar el siguiente resultado.

Lema 8. *Sea $E/\mathbb{F}_q$ una curva elíptica y End(E) su anillo de endomorfismos. Entonces para toda $\phi \in$End(E) existen $tr(\phi), m(\phi) \in \mathbb{Z}$ tal que ϕ es raíz del polinomio de segundo grado $P[x] \in \mathbb{Z}[x]$, $P(x) = x^2 - tr(\phi)x + m(\phi)$.*

Demostración. Sea $d = \deg(1+\phi)$, $m(\phi) = m = \deg(\phi)$ y $\mathrm{tr}(\phi) = \phi + \hat{\phi}$. Entonces, por definición de isogenia dual se tiene

$$[d] = (1+\phi) \circ (1+\phi)\hat{} = 1 + \mathrm{tr}(\phi) + [m], \tag{3}$$

con lo cual $tr(\phi) \in \mathbb{Z}$. El resultado se concluye observando que $\phi^2 - (\phi + \hat{\phi})\phi + \hat{\phi}\phi = 0$ trivialmente.

Definición 12. *A la isogenia $\phi + \hat{\phi} = tr(\phi)$ se le llama traza de ϕ.*

El siguiente ejemplo es decisivo en el recuento de puntos de curvas elíptica sobre cuerpos finitos.

Ejemplo 6. 1) Sustituyendo $\phi = -Fr$ en la identidad anterior (3), se obtiene $[\mathrm{tr}\ (Fr)] = [\deg(1 - Fr) - q - 1]$.

2) $tr(\phi) = tr(\hat{\phi})$.

Los anteriores resultados permiten determinar completamente la estructura del anillo de endomorfismos de una curva elíptica. En el siguiente teorema destacamos el caso en el que la curva esté definida sobre cuerpos de característica positiva.

Teorema 10. *Sea $E/\mathbb{F}_q$. Entonces la inclusión End(E) es estricta, y E es ordinaria si y sólo si End(E) es un orden, $\mathbb{Z}[\tau]$, en un cuerpo cuadrático imaginario.*

Demostración. [Sil. Teo. 3.1, pag. 137].

Observación 3. *En las condiciones del teorema, si E es ordinaria, el operador $\hat{}: End(E) \to End(E)$ corresponde a conjugación en el orden correspondiente.*

5 Leading coefficient

En este sección vamos a utilizar el Ejemplo 6 para dar una fórmula cerrada del número de puntos de una curva elíptica en términos de la traza. La ventaja es que ésta aparece de forma explícita en las ecuaciones de la isogenia, en lo que se denomina el leading coefficient.

Dada una curva elíptica, el cuerpo $\overline{K}(E)$ introducido en la Definición 7 se denomina cuerpo de funciones de la curva elíptica. Se puede demostrar que el anillo $\overline{K}(E)_P = \{\frac{f}{g} : f, g \in \overline{K}(E), g(P) \neq 0\}$ es un anillo de valoración discreta. (Ver [Sil. Prop. 1.1, pag. 21]). Si $P = O$ entonces el parámetro local se puede tomar como la función $f = x/y$, por lo que toda función en $\overline{K}(E)_O$ se puede desarrollar en serie de Taylor en potencias de f. Esto nos permite demostrar la siguiente proposición.

Proposición 10. *Sea E_1/K, E_2/K curvas elípticas y $\phi = (\phi_1, \phi_2) : E_1 \to E_2$, definida sobre K. Entonces existe $\lambda \in K$ tal que*

$$\frac{\phi_1}{\phi_2} = \lambda \frac{x}{y} + O\left(\frac{x}{y}\right)^2,$$

como serie de potencias en $\frac{x}{y}$.

Demostración. Para una demostración completa ver [Sil. Cap. 4, sec. 1]. Una idea de porque no tiene término constante puede verse de la siguiente forma. En coordenadas proyectivas la isogenia tiene la forma $\varphi = [\varphi_1, \varphi_2, \varphi_3]$, de forma que teniendo en cuenta $\varphi(O) = O$, se tiene que $\varphi_1(O) = 0$, $\varphi_2(O) = 1$, $\varphi_3(O) = 0$, con lo que $1/\varphi_2$ es analítica alrededor de O, y φ_1 tiene coeficiente constante 0. El resultado se seguiría de que $\frac{\varphi_1}{\varphi_2} = \frac{\phi_1}{\phi_2}$.

Definición 13. *Al coeficiente λ de la Proposición 10 se le conoce como leading coefficient de la isogenia ϕ, y se denota $lc(\phi)$.*

Ejemplo 7.

$lc(\psi) = u$, para todo isomorfismo ψ como en el Teorema 1.
$lc(AGM) = 2; \quad lc(AGM)\hat{} = 1.$
$lc(Fr) = 0.$

El segundo ejemplo se obtiene sin más que desarrollar por Taylor las ecuaciones explícitas dadas en la Proposición 5 y el Ejemplo 5 respectivamente. Obsérvese que, en este caso, se cumple $lc(AGM)lc(AGM)\hat{} = 2$, que coincide con el grado de la isogenia. Este de hecho no es un caso aislado y, en general, se puede demostrar lo siguiente.

Proposición 11.

$$lc(\phi \circ \hat{\phi}) = lc(\phi)lc(\hat{\phi}),$$
$$lc(\phi_1 + \phi_2) = lc(\phi_1) + lc(\phi_2)$$

Demostración. Las dos se pueden demostrar simplemente desarrollando por Taylor las expresiones correspondientes. Sin embargo hay que notar que, en la segunda, intervendrán en el desarrollo las fórmulas explícitas para la operación suma en curvas elípticas.

Corolario 2.
a) lc[m]=m
b) Si ϕ es separable de grado d, entonces $lc(\hat{\phi}) = \frac{d}{lc(\phi)}$.

Demostración. La primera parte se demuestra fácilmente por inducción ya que $lc(1) = 1$ de forma trivial. Para la segunda aplicar la proposición.

Corolario 3. *Sea ϕ una isogenia separable. Entonces $tr(\phi) = lc(\phi) + \frac{d}{lc(\phi)}$.*

El anterior resultado nos permite reducir el cálculo de puntos de una curva elíptica al del leading coefficient de la isogenia Ve.

Teorema 11. *Sea $E/\mathbb{F}_q$ entonces $\#E(\mathbb{F}_q) = lc(Ve) + \frac{q}{lc(Ve)} + q + 1$.*

Demostración. El resultado es consecuencia del Teorema 4, Ejemplo 3, Ejemplo 6, Teorema 9 (e), y Corolario 3.