

ÍNDICE GENERAL

1	DESAROLLO MATEMÁTICO	1
1.1	Teoría básica de curvas elípticas	1
1.1.1	Definición de curva elíptica	1
1.1.2	Ecuaciones de Weierstrass simplificadas	3
1.1.3	Ley de grupo	5
1.1.4	Multiplicación escalar	8
1.1.5	Puntos proyectivos	9
1.1.6	Endomorfismos	10
1.1.7	Puntos de torsión	13
I	APÉNDICE	17
	BIBLIOGRAFÍA	19

ÍNDICE DE FIGURAS

Figura 1	Curvas elípticas sobre \mathbb{R}	2
Figura 2	Método de la cuerda y la tangente	5

ÍNDICE DE TABLAS

ACRÓNIMOS

DESAROLLO MATEMÁTICO

En este capítulo haremos el estudio matemático de la teoría de curvas elípticas. En el apartado 1.1 se desarrolla la teoría básica, mientras que en el apartado ?? se particulariza a curvas elípticas sobre cuerpos finitos y por último en el apartado ?? se ve...

Las referencias utilizadas para el desarrollo matemático han sido [4], [1] y [3].

1.1 TEORÍA BÁSICA DE CURVAS ELÍPTICAS

En este apartado se tratarán las ecuaciones de Weierstrass, las operaciones de adición y duplicación, los puntos proyectivos, los endomorfismos de curvas elípticas y la estructura de los puntos de torsión.

Las principales referencias utilizadas en este capítulo han sido [4, cap. 2] y [1, cap. 3].

1.1.1 Definición de curva elíptica

En esta apartado veremos la definición general de curva elíptica aunque posteriormente simplificaremos la ecuación que la define.

Definición 1.1. Una *curva elíptica* E se define por una ecuación de la forma

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

donde $a_1, a_2, a_3, a_4, a_6 \in K$ y $\Delta \neq 0$, siendo Δ el *discriminante* de E y definiéndose como:

$$\left. \begin{aligned} \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\ d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + 4a_2 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned} \right\} \quad (2)$$

Si L es una extensión del cuerpo K , entonces el conjunto de puntos L -*racionales* de E es:

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\}$$

Nota 1.2 (comentarios de la definición 1.1).

- La ecuación (1) se conoce como la *ecuación de Weierstrass*.
- Diremos que E *está definida sobre* K y lo notaremos E/K . A K lo llamaremos *cuerpo base*.
- La condición $\Delta \neq 0$ asegura que la curva elíptica no tenga puntos *singulares*, esto es, puntos que anulen las derivadas parciales de la función polínómica

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

asociada a la curva elíptica. Esto asegura que no haya puntos en los que la curva tenga dos o más rectas tangentes.

- El punto ∞ lo llamaremos *punto del infinito*. Es el único punto en la recta del infinito que satisface la forma proyectiva de la ecuación de Weierstrass (véase apartado 1.1.5).

Ejemplo 1.3 (curvas elípticas sobre \mathbb{R}). Consideramos las curvas elípticas:

$$E_1 : y^2 = x^3 - x$$

$$E_2 : y^2 = x^3 + x$$

definidas sobre el cuerpo \mathbb{R} de los números reales. Los puntos $E_1(\mathbb{R})$ y $E_2(\mathbb{R})$ se han representado en la Figura 1.

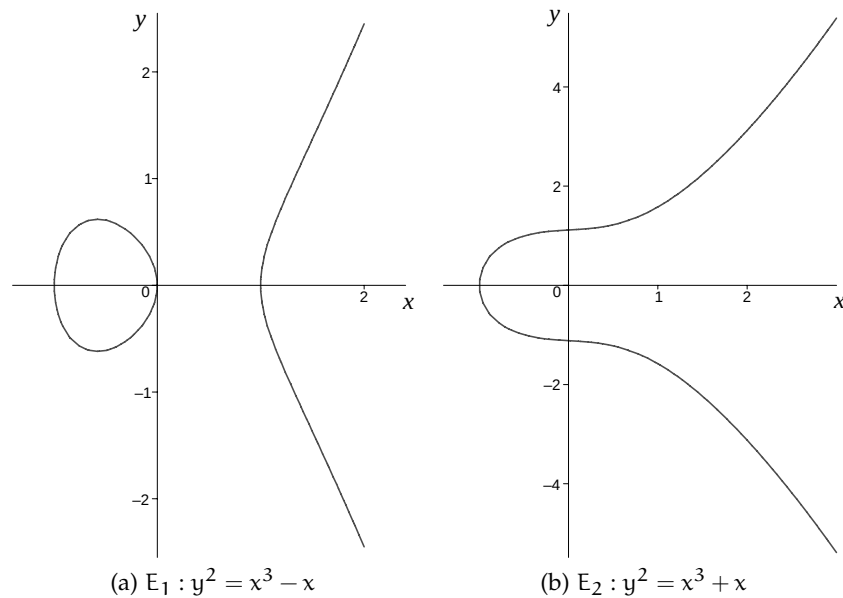


Figura 1: Curvas elípticas sobre \mathbb{R}

1.1.2 Ecuaciones de Weierstrass simplificadas

Nuestro objetivo es transformar la ecuación (1) por una ecuación más sencilla. En este apartado veremos varias transformaciones según la característica del cuerpo base.

Definición 1.4. Dos curvas elípticas E_1 y E_2 definidas sobre K y dadas por las ecuaciones de Weierstrass:

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$E_2 : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6$$

se dicen que son *isomorfas sobre K* si existen $u, r, s, t \in K$, $u \neq 0$, tal que el cambio de variables lineal

$$(x, y) \mapsto (u^2x + r, u^3y + u^2sx + t) \quad (3)$$

transforma la ecuación E_1 en la ecuación E_2 . La transformación (3) se llama un cambio de variables admisible.

El cambio de variables (3) es el único que deja «fijo» el punto del infinito y preserva la forma de la ecuación de Weierstrass. No vamos a entrar en más detalle, pero puede consultar [3, prop. III.3.1b] para más información.

Una ecuación de Weierstrass

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

puede simplificarse considerablemente aplicando cambios de variables admisibles. Veamos el caso en el que la característica del cuerpo base no es ni 2 ni 3.

Lema 1.5. Si $\text{char}(K) \neq 2, 3$, entonces el cambio de variables admisible

$$(x, y) \mapsto \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{240} \right)$$

transforma E en la curva

$$y^2 = x^3 + ax + b \quad (4)$$

donde $a, b \in K$. El discriminante de esta curva es $\Delta = -16(4a^3 + 27b^2)$.

Demostración. Basta aplicar el cambio de variables y ver que efectivamente se obtiene la expresión (4). En su lugar, veamos el proceso por el cual se obtuvo dicha simplificación.

Dada la ecuación de Weierstrass (1), sumamos en ambos lados por $(a_1a_3x)/2 + a_3^2/4 + (a_1^2x^2)/4$ (podemos dividir por 2 ya que $\text{char}(K) \neq 2$) para completar el cuadrado:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2} \right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4} \right) x^2 + \left(a_4 + \frac{a_1a_3}{2} \right) x + \left(a_6 + \frac{a_3^2}{4} \right)$$

Haciendo $y_1 = y + (a_1x)/2 + a_3/2$, obtenemos

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

para algunas constantes $a_2', a_4', a_6' \in K$. Finalmente, sustituyendo $x_1 = x + a_2'/3$ (podemos dividir por 3 ya que $\text{char}(K) \neq 3$) resulta

$$y_1^2 = x_1^3 + ax_1 + b$$

para algunas constante $a, b \in K$. Para obtener el discriminante Δ basta sustituir el valor de las constantes $a_4 = a$, $a_6 = b$ y $a_1 = a_3 = a_2 = 0$ en (2). \square

Nota 1.6 (comentarios del lema 1.5).

- Si el cuerpo base tiene característica 2, la ecuación anterior (4) no es válida ya que tiene puntos singulares.
- Para cuerpos base con característica 3, la ecuación anterior (4) si es válida, pero existan curvas que no tienen esta forma.

En la mayor parte del trabajo, desarrollaremos la teoría de curvas elípticas utilizando la ecuación de Weierstrass simplificada (4). Sin embargo, como los cuerpos finitos de característica dos son de especial interés en computación, ocasionalmente señalaremos que modificaciones son necesarias para los cuerpos base de característica dos. Veamos la primera modificación.

Lema 1.7. Si la característica de K es 2, hay dos casos que considerar. Si $a_1 \neq 0$, entonces el cambio de variables admisible

$$(x, y) \mapsto \left(a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3} \right)$$

transforma E en la curva

$$y^2 + xy = x^3 + ax^2 + b$$

donde $a, b \in K$. Tales curvas se llaman *no supersingulares* (véase ??) y tienen discriminante $\Delta = b$. Si $a_1 = 0$, entonces el cambio de variables admisible

$$(x, y) \mapsto (x + a_2, y)$$

transforma E en la curva

$$y^2 + cy = x^3 + ax + b$$

donde $a, b, c \in K$. Tales curvas se llaman *supersingulares* (véase ??) y tienen discriminante $\Delta = c^4$.

Demostración. Basta sustituir el cambio de variables en la ecuación general de Weierstrass y operar. \square

1.1.3 Ley de grupo

En este apartado veremos como dotar de estructura de grupo al conjunto de puntos una curva elíptica. Para ello definiremos una ley de composición o ley de grupo y le daremos sentido a la «suma» de puntos.

Sea E una curva elíptica definida sobre un cuerpo K . El siguiente método geométrico permite dados dos puntos en $E(K)$ producir un tercero en $E(K)$. Este método será la base para definir la ley de grupo.

Algoritmo 1.8 (Método de la cuerda y la tangente). Dados dos puntos P y Q , veamos como producir un tercer punto R . En primer lugar si P y Q son distintos, los pasos son:

1. Se dibuja una recta L de P a Q .
2. Esta recta intersecta la curva elíptica en un tercer punto.
3. Tomamos R como la reflexión de este punto sobre el eje- x .

Si los puntos P y Q son iguales, los pasos son:

1. Se dibuja la línea tangente L a la curva elíptica en P .
2. Esta línea intersecta la curva elíptica en un segundo punto.
3. Tomamos R como la reflexión de este punto sobre el eje- x .

Esto método se puede apreciar en la figura 2.

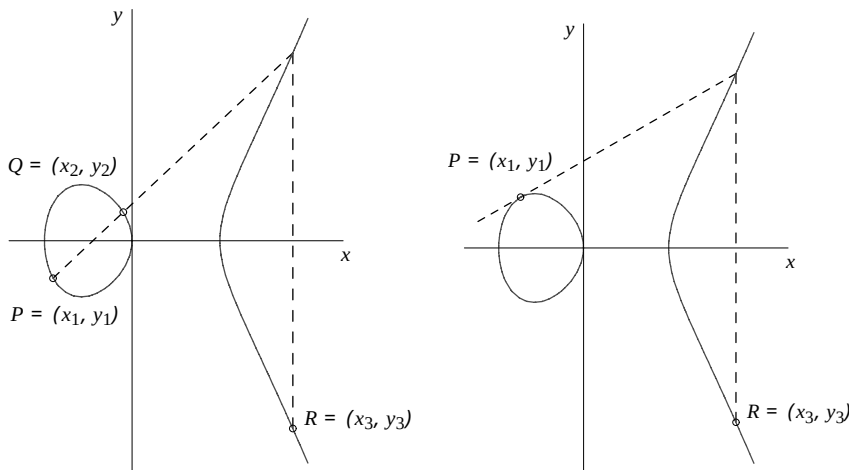


Figura 2: Método de la cuerda y la tangente

Nota 1.9 (comentarios del algoritmo 1.14). El hecho de que $L \cap E$, contando multiplicidades, consiste en exactamente tres puntos (no necesariamente distintos) es un caso especial del teorema de Bézout [2, sec. I.7.8]. Sin embargo, como a continuación vamos a dar fórmulas explícitas, haremos la demostración utilizando dichas fórmulas y no será necesario utilizar un teorema tan general.

Inspirándonos en el método de la cuerda y la tangente, definimos la siguiente ley de composición para el grupo de puntos de una curva elíptica.

Definición 1.10 (ley de grupo). Sea E una curva elíptica definida por la ecuación $y^2 = x^3 + ax + b$ sobre un cuerpo K de característica distinta de 2 y 3. Definimos la operación binaria $+$: $E(K) \times E(K) \rightarrow E(K)$ como sigue:

- a) $P + \infty = \infty + P = P$, para todo $P \in E(K)$
- b) Si $P = (x, y) \in E(K)$, entonces $(x, y) + (x, -y) = \infty$. El punto $(x, -y)$ se denotará por $-P$ y se llamará el *opuesto* de P . Además, $-\infty = \infty$.
- c) Sea $P = (x_1, y_1) \in E(K)$ y $Q = (x_2, y_2) \in E(K)$, donde $P \neq \pm Q$. Entonces $P + Q = (x_3, y_3)$, donde

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2, \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) - y_1$$

- d) Sea $P = (x_1, y_1) \in E(K)$, donde $P \neq -P$. Entonces $2P = (x_3, y_3)$ donde:

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1, \quad y_3 = \left(\frac{3x_1^2 + a}{2y_1} \right) (x_1 - x_3) - y_1$$

Demostración. Tenemos que comprobar que $+$ es una operación binaria válida, esto es, que a cada par de elementos de $E(K) \times E(K)$ le corresponde un único elemento de $E(K)$. Como la casuística anterior es total y exclusiva, basta ver que $+$ es una operación cerrada. Los casos a) y b) son triviales. Veamos los otros dos casos con detalle.

CASO c) Supongamos $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P, Q \in E(K)$ con $P \neq \pm Q$. Consideramos la recta que los contiene:

$$L : y = m(x - x_1) + y_1, \text{ donde } m = \frac{y_2 - y_1}{x_2 - x_1}$$

Nótese que $x_2 \neq x_1$ ya que $P \neq \pm Q$. Para hallar la intersección de L con E sustituimos y :

$$(m(x - x_1) + y_1)^2 = x^3 + ax + b$$

Podemos reescribir esto de la forma

$$0 = x^3 - m^2x^2 + b'x + c' \quad (5)$$

para algunas constantes $b', c' \in K$. Así, las raíces de esta cúbica es justamente $L \cup E$.

Sabemos que las raíces de un polinomio están relacionadas con sus coeficientes. De hecho, para un polinomio cúbico mónico $x^3 + c_2x^2 + c_1x + c_0$ con raíces r, s, t se tiene:

$$\begin{aligned} x^3 + c_2x^2 + c_1x + c_0 &= (x - r)(x - s)(x - t) \\ &= x^3 - (r + s + t)x^2 + (rs + rt + st)x - rst \end{aligned}$$

En particular, $r + s + t = -c_2$. Como P y Q están en la intersección, x_1 y x_2 son dos raíces de (5), luego la tercera raíz α es $m^2 - x_1 - x_2$. Sustituyendo α en L resulta $\beta = m(x_3 - x_1) + y_1$, luego $(\alpha, \beta) \in E(K)$. Entonces $(\alpha, -\beta) = (x_3, y_3) \in E(K)$.

CASO d) Sea $P = (x_1, y_1)$, donde $P \neq -P$. Consideramos la recta tangente a E en P

$$L : y = m(x - x_1) + y_1, \text{ donde } m = \frac{3x_1^2 + a}{2y_1}$$

Nótese que $y_1 \neq 0$ ya que si no estaríamos en el caso b). Hallamos la intersección con E de forma análoga al caso c) y obtenemos la cúbica:

$$0 = x^3 - m^2x^2 + b'x + c'$$

para algunas constantes $b', c' \in K$. Análogamente al caso c), como x_1 es una raíz doble de la cúbica (derívese y evalúe en x_1) tenemos que la tercera raíz α es $m^2 - 2x_1$. Sustituyendo α en L resulta $\beta = m(x_3 - x_1) + y_1$, luego $(\alpha, \beta) \in E(K)$. Entonces $(\alpha, -\beta) = (x_3, y_3) \in E(K)$. \square

Nota 1.11 (comentarios de la definición 1.10). Para cuerpos base con característica 2 o 3, las fórmulas cambian. Por ejemplo, si E es una curva elíptica definida sobre un cuerpo K por la ecuación general de Weierstrass (1), el opuesto de un punto $P = (x, y) \in E(K)$ viene dado por

$$-P = (x, -a_1x - a_3 - y)$$

En el apartado ?? veremos la ley de composición para una curva elíptica sobre un cuerpo finito de característica 2.

Con la operación binaria 1.10, el conjunto de puntos de una curva elíptica es un grupo abeliano.

Teorema 1.12. La suma 1.10 de puntos en una curva elíptica E sobre un cuerpo K de característica distinta de 2 y 3 satisface la siguientes propiedades:

- *Conmutatividad.* $P_1 + P_2 = P_2 + P_1, \forall P_1, P_2 \in E(K)$.
- *Existencia de elemento neutro.* $P + \infty = P, \forall P \in E(K)$.
- *Existencia de elemento opuesto.* $P + (-P) = \infty, \forall P \in E(K)$.

- *Asociatividad.* $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3), \forall P_1, P_2, P_3 \in E(K).$

En otras palabras, $(E(K), +, \infty)$ es un grupo abeliano.

Demostración. La conmutatividad es trivial en los casos a), b) y d). Para el caso c) también es fácil ya que la recta que une P_1 y P_2 es la misma que la recta que une P_2 y P_1 . La existencia de elemento neutro e inverso también es directo de la definición 1.10.

La asociatividad puede probarse utilizando las fórmulas caso por caso, pero supone un esfuerzo demasiado laborioso. En su lugar, puede abordarse de forma más sofisticada bien estudiando las líneas y sus intersecciones con la curva elíptica en el plano proyectivo [4, sec. 2.4] o bien usando teoremas más generales como el de Riemann-Roch [3, teo. III.3.4.e]. \square

Nota 1.13 (comentarios del teorema 1.12). Puede encontrar una versión más general del teorema anterior para cuerpos bases de cualquiera característica en [3].

1.1.4 Multiplicación escalar

En este apartado veremos un método eficiente para calcular la duplicación reiterada de un punto.

Sea P es un punto de una curva elíptica y k un entero positivo. Denotaremos kP a la suma $P + \dots + P$ de k -sumandos. El siguiente algoritmo calcula kP más rápido que el método directo (sumar P consigo mismo repetidamente).

Algoritmo 1.14 (multiplicación por duplicación). Sea k un entero positivo y sea P un punto de una curva elíptica. El siguiente algoritmo calcula kP .

1. Se empieza con $a = k$, $B = \infty$ y $C = P$.
2. Si a es par, se toma $a = a/2$, $B = B$ y $C = 2C$.
3. Si a es impar, se toma $a = a - 1$, $B = B + C$ y $C = C$.
4. Si $a \neq 0$, se va al paso 2.
5. Se devuelve B .

La salida B es kP .

Nota 1.15 (comentarios del algoritmo 1.14).

- El único problema de este método es que el tamaño de las coordenadas incrementa muy rápidamente.
- Si trabajamos sobre un cuerpo finito, podemos evitar este inconveniente reduciendo módulo p en cada operación.

1.1.5 Puntos proyectivos

En este apartado introduciremos los puntos proyectivos y veremos de donde procede el punto del infinito de una curva elíptica. Como en la mayor parte del trabajo no vamos a trabajar con puntos proyectivos, veremos este apartado de manera más informal.

Sea K un cuerpo. El *espacio proyectivo* dos dimensional sobre K , $\mathbb{P}^2(K)$, está dado por clases de equivalencia de ternas (x, y, z) con $x, y, z \in K$ y al menos algún x, y, z no nulo. Dos ternas (x_1, y_1, z_1) y (x_2, y_2, z_2) se dicen que son *equivalentes* si existe un elemento no nulo $\lambda \in K$ tal que

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$$

y en tal caso escribiremos $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. La clase de equivalencia de una terna solo depende de los ratios entre x, y, z . Por ello, la clase de equivalencia de (x, y, z) la denotaremos por $(x : y : z)$ y diremos que es un *punto proyectivo*.

Si $(x : y : z)$ es un punto proyectivo con $z \neq 0$, entonces $(x : y : z) = (x/z : y/z : 1)$ y de hecho $(x/z, y/z, 1)$ es el único representante de esta clase de equivalencia con $z = 1$. Tenemos así una correspondencia 1 – 1 entre el conjunto de puntos proyectivos

$$\mathbb{P}^2(K)^* = \{(x : y : z) : x, y, z \in K, z \neq 0\}$$

y el *plano afín*

$$\mathbb{A}(K) = \{(x, y) : x, y \in K\}.$$

Si $z = 0$, el conjunto de puntos proyectivos de la forma $(x : y : 0)$ se llaman *recta del infinito* ya que sus puntos no se corresponden con ninguno del plano afín.

La *forma proyectiva* de una ecuación de Weierstrass de una curva elíptica E definida sobre K se obtiene remplazando x por x/z , y por y/z y quitando denominadores. Si alguna terna (x, y, z) no nula satisface la ecuación proyectiva entonces también las satisfacen las ternas $(x', y', z') \in (x : y : z)$. Podemos decir entonces que un punto proyectivo $(x : y : z)$ está en E . Tenemos así una correspondencia 1-1 entre los puntos del plano afín que están en E y los puntos proyectivos de $\mathbb{P}^2(K)^*$ que están en E .

Si hacemos $z = 0$ en la forma proyectiva de la ecuación, obtenemos $0 = x^3$ y como alguna componente tiene que ser no nula, tenemos $y \neq 0$. Así, el único punto de la recta del infinito que está en E es el punto $(0 : y : 0) = (0 : 1 : 0)$. Este punto se corresponde con el punto ∞ de la definición 1.1.

Hay situaciones en la que usar coordenadas proyectivas puede ser ventajoso (véase [4, sec 2.6]). Sin embargo, nosotros utilizaremos las coordenadas del plano afín y trataremos el punto del infinito como caso especial cuando sea necesario.

1.1.6 Endomorfismos

El principal objetivo de este apartado es probar la proposición 1.20 que será utilizada en la demostración del teorema de Hasse ???. Para ello, es necesario utilizar algunos resultados técnicos, los cuales solo los enunciaremos (puede encontrar su demostración en [4, sec. 2.9]).

Definición 1.16. Sea E una curva elíptica definida sobre un cuerpo K y sea \bar{K} su clausura algebraica. Un *endomorfismo* de E es un homomorfismo $\alpha : E(\bar{K}) \rightarrow E(\bar{K})$ dado por funciones racionales (cocientes de polinomios). Dicho de otro modo, α preserva la suma y el elemento neutro de $E(\bar{K})$.

El endomorfismo trivial que lleva cada punto a ∞ lo denotaremos por 0 .

Supondremos que α es no trivial a partir de ahora. El siguiente resultado técnico nos facilitará el manejo de endomorfismos de una curva elíptica.

Lema 1.17. Si α es un endomorfismo de una curva elíptica definida por la ecuación de Weierstrass simplificada (4), entonces α se puede escribir como

$$\alpha(x, y) = (r_1(x), r_2(x)y)$$

donde

- $r_1(x) = p(x)/q(x)$, con $p(x), q(x)$ polinomios sin factores comunes.
- Si $q(x) = 0$ para algún punto (x, y) , entonces definimos $\alpha(x, y) = \infty$.
- Si $q(x) \neq 0$, entonces $r_2(x)$ está definida.

Definición 1.18. El *grado* de un endomorfismo α es

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\}$$

si α es no trivial. Si $\alpha = 0$, definimos $\deg(0) = 0$.

Definición 1.19. Un endomorfismo α no trivial es *separable* si la derivada $r_1(x)'$ no es idénticamente cero.

El siguiente resultado será crucial en la demostración del teorema de Hasse ??

Proposición 1.20. Sea $\alpha \neq 0$ un endomorfismo separable de una curva elíptica E . Entonces

$$\deg(\alpha) = |\ker(\alpha)|$$

donde $\ker(\alpha)$ es el núcleo del homomorfismo $\alpha : E(\bar{K}) \rightarrow E(\bar{K})$. Si $\alpha \neq 0$ no es separable, entonces

$$\deg(\alpha) > |\ker(\alpha)|$$

Demostración. Por el lema 1.17, $\alpha(x, y) = (r_1(x), r_2(x)y)$ con $r_1(x) = p(x)/q(x)$. Supongamos que α es separable. Entonces $r_1' \neq 0$, por lo que $p'q - pq'$ no es el polinomio cero.

Sea S el conjunto de $x \in \bar{K}$ tal que $(pq' - p'q)(x)q(x) = 0$. Sea $(u, v) \in E(\bar{K})$ tal que

1. $u \neq 0, v \neq 0, (u, v) \neq \infty$,
2. $\deg(p(x) - uq(x)) = \max\{\deg(p), \deg(q)\} = \deg(\alpha)$,
3. $u \notin r_1(S)$ y
4. $(u, v) \in \alpha(E(\bar{K}))$.

Como $p'q - pq'$ no es el polinomio nulo, S es un conjunto finito, por lo que su imagen bajo α es finita. Por otro lado $\alpha(E(\bar{K}))$ es un conjunto infinito. Así, tal (u, v) existe.

Veamos que existen exactamente $\deg(\alpha)$ puntos $(x_1, y_1) \in E(\bar{K})$ tal que $\alpha(x_1, y_1) = (u, v)$. Para tales puntos, se tiene

$$\frac{p(x_1)}{q(x_1)} = u, \quad y_1 r_2(x_1) = v$$

Como $(u, v) \neq \infty$, $q(x_1) \neq 0$ luego $r_2(x_1)$ está definido. Como $v \neq 0$ y $y_1 r_2(x_1) = v$, se tendrá $y_1 = v/r_2(x_1)$, esto es, x_1 determina y_1 , por lo que solo tenemos que contar valores de x_1 .

Por la propiedad (2), $p(x) - uq(x)$ tiene $\deg(\alpha)$ raíces, contando multiplicidades. Tenemos que ver que $p - uq$ no tiene raíces múltiples. Supongamos que x_0 es una raíz múltiple. Entonces

$$p(x_0) - uq(x_0) = 0, \quad p'(x_0) - uq'(x_0) = 0$$

Multiplicando las ecuaciones $p = uq$ y $uq' = p'$ resulta

$$up(x_0)q'(x_0) = up'(x_0)q(x_0)$$

Como $u \neq 0$, esto implica que x_0 es una raíz de $p'q - p'q$, por lo que $x_0 \in S$. Así $u = r_1(x_0) \in r_1(S)$, contrario a la propiedad (3). Concluimos que $p - uq$ no tiene raíces múltiples y por ello tiene $\deg(\alpha)$ raíces distintas.

Como hay exactamente $\deg(\alpha)$ puntos (x_1, y_1) con $\alpha(x_1, y_1) = (u, v)$, el núcleo de α tiene $\deg(\alpha)$ elementos.

Nótese que como α es un homomorfismo, para cada $(u, v) \in \alpha(E(\bar{K}))$ hay exactamente $\deg(\alpha)$ puntos (x_1, y_1) con $\alpha(x_1, y_1) = (u, v)$. Las hipótesis sobre (u, v) se hicieron para obtener el resultado para al menos un punto, lo cual es suficiente.

Si α no es separable, entonces los pasos de la demostración siguen siendo válidos, excepto que $p' - uq'$ es siempre el polinomio cero en este caso, por lo que $p(x) - uq(x) = 0$ tiene siempre raíces múltiples y por ello tiene menos de $\deg(\alpha)$ soluciones. \square

Veamos un par de resultados que serán útiles para describir la estructura de los puntos de torsión del apartado ??.

Proposición 1.21. Sea E una curva elíptica definida sobre el cuerpo K . Sea $\alpha \neq 0$ un endomorfismo de E . Entonces α es sobreyectiva.

Demostración. Sea $(u, v) \in E(\bar{K})$. Como $\alpha(\infty) = \infty$, supongamos que $(u, v) \neq \infty$. Por el lema 1.17, α será de la forma $\alpha(x, y) = (r_1(x), r_2(x)y)$ con $r_1(x) = p(x)/q(x)$. Consideramos el polinomio $p(x) - uq(x)$. Distinguimos dos casos.

Supongamos que $p(x) - uq(x)$ no es un polinomio constante. Entonces tendrá una raíz x_0 . Como p y q no tiene raíces en común, $q(x_0) \neq 0$. Sea $y_0 \in \bar{K}$ una raíz cuadrada de $x_0^3 + ux_0 + v$. Como $q(x_0) \neq 0$, $r_2(x)$ está definido y por lo tanto $\alpha(x_0, y_0)$ también y valdrá (u, v') para algún v' . Como $v'^2 = u^3 + au + b = v^2$, tenemos $v' = \pm v$. Si $v' = v$, hemos terminado. Si $v' = -v$, entonces $\alpha(x_0, -y_0) = (u, -v') = (u, v)$.

Supongamos que $p - uq$ es un polinomio constante. Como $E(\bar{K})$ no es finito y el núcleo de α sí es finito, solo un número finito de puntos de $E(\bar{K})$ puede tener como imagen un punto con una componente x dada. Así, bien $p(x)$ o $q(x)$ no es constante. Si p y q son dos polinomios no constantes, entonces hay como mucho una constante u tal que $p - uq$ es constante (si u' fuera otra constante que lo verificara, se tendría $(u' - u)q = (p - uq) - (p - u'q)$ es constante y $(u - u')p = u'(p - uq) - u(p - u'q)$ es constante, lo que implicaría que p y q son constantes). Así, hay al menos dos puntos, (u, v) y $(u, -v)$ para algún v , que no están en la imagen de α . Sea (u_1, v_1) otro punto. Entonces $\alpha(P_1) = (u_1, v_1)$ para algún P_1 . Podemos elegir (u_1, v_1) tal que $(u_1, v_1) + (u, v) \neq (u, \pm v)$, por lo que existe P_2 con $\alpha(P_2) = (u_1, v_1) + (u, v)$. Entonces $\alpha(P_2 - P_1) = (u, v)$ y $\alpha(P_1 - P_2) = (u, -v)$. □

Proposición 1.22. Sea E una curva elíptica definida sobre un cuerpo K y sea n un entero no cero. Consideramos el endomorfismo *multiplicación por n* dado por

$$n(P) = nP, \forall P \in E(\bar{K})$$

Supongamos que está dado por funciones racionales R_n y S_n , esto es,

$$n(x, y) = (R_n(x), yS_n(x))$$

para todo $(x, y) \in E(\bar{K})$. Entonces

$$\frac{R'_n(x)}{S_n(x)} = n.$$

Por tanto, la multiplicación por n es separable si y sólo si n no es un múltiplo de la característica del cuerpo base.

Para demostrar esta proposición, necesitamos un resultado técnico. La demostración de este lema se puede encontrar en [4, sec 2.9].

Lema 1.23. Sean $\alpha_1, \alpha_2, \alpha_3$ endomorfismos no triviales de una curva elíptica E con $\alpha_1 + \alpha_2 = \alpha_3$. Supongamos que cada endomorfismo está dado de la siguiente forma

$$\alpha_j(x, y) = (R_{\alpha_j}(x), yS_{\alpha_j}(x))$$

y que existen constantes $c_{\alpha_1}, c_{\alpha_2}$ tal que

$$\frac{R'_{\alpha_1}(x)}{S_{\alpha_1}(x)} = c_{\alpha_1}, \quad \frac{R'_{\alpha_2}(x)}{S_{\alpha_2}(x)} = c_{\alpha_2}.$$

Entonces

$$\frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = c_{\alpha_1} + c_{\alpha_2}$$

Demostración de la proposición 1.22. Dado un endomorfismo cualquiera α , se tiene

$$\alpha(x, -y) = \alpha(-(x, y)) = -\alpha(x, y).$$

En particular, $R_{-\alpha} = R_{\alpha}$ y $S_{-\alpha} = -S_{\alpha}$. Luego $R'_{\alpha}/S_{\alpha} = -R'_{-\alpha}/S_{-\alpha}$ y basta probar el resultado para n positivos.

Para $n = 1$, la primera parte de la proposición es cierta. Aplicando el lema anterior, si es cierta para n , también es cierta para $n + 1$ (la suma de n y 1). Así,

$$\frac{R'_n(x)}{S_n(x)} = n.$$

Por otro lado, $R'_n(x) \neq 0$ si y solo si $R'_n(x)/S_n(x) \neq 0$, que es equivalente a que la característica de K no divida a n . Por la definición de separabilidad, esto prueba la segunda parte. \square

1.1.7 Puntos de torsión

En este apartado introduciremos los puntos de torsión y su estructura que jugarán un papel importante en las curvas elípticas sobre cuerpos finitos. También veremos el emparejamiento Weil el cual utilizaremos en la demostración del teorema de Hasse ??.

Definición 1.24. Un elemento de una curva elíptica E cuyo orden es finito se llamará *punto de torsión*.

Definición 1.25. Llamaremos *subgrupo de n -torsión* al subgrupo

$$E[n] = \{P \in E(\bar{K}) \mid nP = \infty\}.$$

Estos conjuntos son subgrupos ya que son los núcleos del endomorfismo multiplicación por n (definido en el apartado 1.1.6).

Teorema 1.26. Sea E una curva elíptica sobre un cuerpo K y sea n un entero positivo. Si la característica de K no divide a n , o es cero, entonces

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Si la característica de K es $p > 0$ y $p|n$, entonces

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \text{ o } \simeq \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$$

donde $n = p^r n'$ con $p \nmid n'$.

Para demostrar este teorema vamos a usar un resultado cuya demostración técnica, extensa y laboriosa omitiremos. Puede consultar su demostración en [4, sec. 3.2].

Proposición 1.27. Sea E una curva elíptica. El endomorfismo multiplicación por n de E tiene grado n^2 .

Demostración del teorema 1.26. Supongamos primero que n no es múltiplo de la característica p del cuerpo. Por la proposición 1.22, como n no es múltiplo de la característica p , el endomorfismo multiplicación por n es separable. Por la proposición 1.20 y 1.27, el núcleo de este endomorfismo, $E[n]$, tiene orden n^2 .

Por el teorema de estructura para grupos abelianos finitos, $E[n]$ es isomorfo a

$$\mathbb{Z}_{n_1} \simeq \mathbb{Z}_{n_2} \simeq \dots \simeq \mathbb{Z}_{n_k}$$

para algunos enteros n_1, n_2, \dots, n_k con $n_i | n_{i+1} \forall i$ y donde \mathbb{Z}_{n_i} denota el grupo de enteros módulo n_i .

Sea l un primo que divide a n_1 . Entonces $l | n_i \forall i$. Esto implica que $E[l] \subset E[n]$ tiene orden l^k . Como acabamos de probar que $E[l]$ tiene orden l^2 , k debe ser 2. Multiplicar por n anula $E[n] \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, por lo que $n_2 | n$. Como $n^2 = |E[n]| = n_1 n_2$, se tiene $n_1 = n_2 = n$. Así,

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$$

Supongamos ahora que la característica p divide a n . Primero veamos la estructura de los subgrupos de torsión para una potencia de p .

Por la proposición 1.22, el endomorfismo multiplicación por p no es separable. Por tanto, por la proposición 1.20, el núcleo $E[p]$ del endomorfismo multiplicación por p tiene orden estrictamente menor que el grado de este endomorfismo, que es p^2 por la proposición 1.27. Como todo elemento de $E[p]$ tiene orden 1 o p , el orden de $E[p]$ es una potencia de p , por lo que debe ser 1 o p . Si $E[p] = \infty$, entonces $E[p^k]$ debe ser trivial $\forall k$. Ahora supongamos que $E[p]$ tiene orden p . Veamos $E[p^k] \simeq \mathbb{Z}_{p^k} \forall k$.

Supongamos existe un elemento P de orden p^j . Por la proposición 1.21, el endomorfismo multiplicación por p es sobreyectivo, así que existirá un punto Q tal que $pQ = P$. Como

$$p^j Q = p^{j-1} P \neq \infty \quad \text{pero} \quad p^{j+1} Q = p^j P = \infty$$

Q tiene orden p^{j+1} . Por inducción, hay puntos de orden $p^k \forall k$. Por tanto, $E[p^k]$ es cíclico de orden p^k .

Escribiendo $n = p^r n'$ con $r \geq 0$ y $p \nmid n'$, resulta

$$E[n] \simeq E[n'] \oplus E[p^r].$$

donde $E[n'] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$, ya que $p \nmid n'$. Acabamos de ver que $E[p^r] \simeq 0$ o \mathbb{Z}_{p^r} . El teorema chino del resto nos dice que

$$\mathbb{Z}_{n'} \oplus \mathbb{Z}_{p^r} \simeq \mathbb{Z}_{n'p^r} \simeq \mathbb{Z}_n$$

por lo que concluimos con

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \text{o} \quad \mathbb{Z}_{n'} \oplus \mathbb{Z}_n.$$

□

Parte I

APÉNDICE

BIBLIOGRAFÍA

- [1] Darrel Hankerson, Alfred J. Menezes y Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003. ISBN: 038795273X.
- [2] R. Hartshorne. *Algebraic Geometry*. Encyclopaedia of mathematical sciences. Springer, 1977. ISBN: 9780387902449.
- [3] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009. ISBN: 9780387094946.
- [4] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. 2.^a ed. Chapman & Hall/CRC, 2008. ISBN: 9781420071467.