El Módulo de Tate y representaciones de Galois

Alberto Angurel Andrés

7 de diciembre de 2021

Resumen:

El objetivo de este trabajo es realizar una exposición del concepto de módulo de Tate de una curva elíptica y de las representaciones del grupo de Galois $\mathcal{G}(\overline{K}|K)$. Esta discusión estará basada en [1]. Para ello, hemos empezado definiendo el automorfismo de Fröbenius, importante para computar los grupos de torsión de la curva. Posteriormente, se ha introducido el concepto de módulo de Tate, que se ha utilizado para deducir propiedades del anillo de endomorfismos de una curva elíptica, y se han expuesto las representaciones del grupo de Galois sobre dicho módulo. Por último, se ha demostrado el teorema de Hasse que estima el número de puntos racionales sobre una curva elíptica definida sobre un cuerpo finito, para lo cual ha sido necesario introducir el concepto de diferencial invariante de una curva elíptica. Por último, se ha utilizado el módulo de Tate para ver cómo calcular el número de puntos en $\mathbb{F}_{q^n}$ de una curva elíptica a partir del número de puntos de esta sobre $\mathbb{F}_q$.

1. Morfismo de Fröbenius

Sea C una curva definida sobre un cuerpo perfecto K. Supongamos que $\text{char}(K) = p > 0$ y sea $q = p^r$ para algún $r \in \mathbb{N}$. Dado un polinomio $f \in K[X]$, definimos el polinomio $f^{(q)} \in K[X]$ como el polinomio que se obtiene al elevar todos los coeficientes de f a la q-ésima potencia. También definimos la curva $C^{(q)}$ como aquella dada por el ideal $I(C^{(q)})$ generado por $\{f^{(q)} : f \in I(C)\}$. Así, tenemos un morfismo natural, denotado por *morfismo de Fröbenius asociado a la potencia* q y que se define como:

$$\phi : C \to C^{(q)} : \ [x_0 : \cdots : x_n] \mapsto [x_0^q : \cdots : x_n^q]$$

Proposición **1.1.** Sea C una curva definida sobre K y sea ϕ el morfismo de Fröbenius asociado a la q-ésima potencia. Entonces:

$$\phi^*(K(C^{(q)}) = K(C)^q$$

Demostración. Se sigue de que, como K es perfecto, dado $f, g \in K[X_0, \ldots, X_n]$, podemos escribir

$$\phi^* \left(\frac{f}{g} \right) = \frac{f \circ \phi}{g \circ \phi} = \frac{f(X_0^q, \ldots, X_n^q)}{g(X_0^q, \ldots, X_n^q)} = \left(\frac{\tilde{f}(X_0, \ldots, X_n)}{\tilde{g}(X_0, \ldots, X_n)} \right)^q$$

donde $\tilde{f}$ y $\tilde{g}$ son los polinomios que se obtienen sustituyendo los coeficientes α de f y g por el elemento $\beta \in K$ tal que $\alpha = \beta^q$. □

Corolario **1.1.** ϕ es puramente inseparable.

Lema **1.1.** Sea C una curva no singular y sea $t \in K(C)$ tal que $\text{ord}_P(t) = 1$ para algún punto $P \in C$. Entonces $K(C)|K(t)$ es una extensión finita y separable.

Demostración. La finitud es clara por igualdad en grados de trascendencia. Sea $x \in K(C)$. Veamos que x es separable sobre $K(t)$. En cualquier caso, x es algebraico sobre $K(t)$, luego satisface una relación polinomial $\phi(t, j) = \sum_{i,j} a_{ij} t^i x^j = 0$, donde ϕ se escoge para que tenga grado mínimo en x. Siendo $p = \text{char}(K)$, si x no fuese separable, entonces $j \equiv 0 \ (\text{mód } p)$ para todo término no nulo. Entonces, como estamos suponiendo que K es perfecto, podemos escribir

$$\phi(T, X) = \psi(T, X^p) = \sum_{k=0}^{p-1} \left(\sum_{i,j} b_{ijk} T^i X^j \right)^p T^k = \sum_{k=0}^{p-1} \phi_k(T, X)^p T^k$$

Como $\mathrm{ord}_P(t) = 1$, tenemos que si $\phi_k(t,x) \neq 0$, entonces

$$\mathrm{ord}_P(\phi_k(t,x)^p t^k) = p \cdot \mathrm{ord}_P(\phi_k(t,x)) + k\mathrm{ord}_P(t) \equiv k \ (\mathrm{mód} p)$$

Como $\phi(t,x) = 0$ y, dado que si los sumandos fuesen no nulos tendrían distinto orden en p, la única posibilidad es que $\phi_i(t,x) = 0 \ \forall i = 1, \ldots, p-1$. Pero algún $\phi_k(x,t)$ debe incluir a x, lo que contradice la elección de grado mínimo de x. Esta contradicción prueba que x es separable. □

Proposición **1.2.** El grado del automorfismo de Fröbenius asociado a la potencia q-ésima es q.

Demostración. Sea $t \in K(C)$ tal que $\mathrm{ord}_P(t) = 1$. Como $K(C)|K(t)$ es separable por el lema 1.1 y $K(C)|K(C)^{(q)}$ es puramente inseparable por el corolario 1.1, mirando grados de transcendencia separable e inseparables se ve que $K(C) = K(C)^{(q)}(t)$. Por tanto,

$$\deg(\phi) = [K(C)^q(t) : K(C)^q] = q$$

Y esto se ve porque $t^q \in K(C)^q$ y, además, $t^{q/p} \notin K(C)^q$ ya que en tal caso, existiría $f \in K(C)$ tal que $t^{q/p} = f^q$, de modo que se tendría que $\mathrm{ord}_P(f) = \frac{1}{p}$, lo cual no es posible porque ha de ser un entero. □

2. Módulo de Tate

Definición **2.1.** Dada una curva elíptica E, sus m-puntos de torsión son aquellos cuyo orden divide a m (con la operación de grupo asociada a la curva). Es decir, son aquellos puntos tales que

$$[m]P = O$$

Claramente, estos puntos forman un subgrupo que se denota por $E[m]$.

Proposición **2.1.** Sea E una curva elíptica y $m \in \mathbb{Z} \setminus \{0\}$.

1. Si $m \neq 0$ en K, es decir, si $\mathrm{char}(K) = 0$ o si $p = \mathrm{char}(K) \not| m$, entonces

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

2. Si $p = \mathrm{char}(K) > 0$, entonces se cumple una de las siguientes afirmaciones:
   - $E[p^e] = \{0\} \ \forall e \in \mathbb{N} \cup \{0\}$
   - $E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}} \ \forall e \in \mathbb{N} \cup \{0\}$

Demostración. Como el grado de $[m]$ es m^2, entonces si $p \not| m^2$, $[m]$ tiene que ser separable, de modo que

$$\#E[m] = \#\ker[m] = m^2$$

Como esto vale también para todo $d|m$, hay exáctamente d^2 elementos de $E[m]$, cuyo orden divide a d. Por el teorema de clasificación de grupos abelianos finitos, la única posibilidad es que

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

Para la segunda parte, sea ϕ el automorfismo de Fröbenius asociado a la p-ésima potencia. Entonces, como $\deg \phi = 1$

$$\#E[p^e] = \deg_s[p^e] = \left(\deg_s(\widehat{\phi} \circ \phi)\right)^e = (\deg_s \widehat{\phi})^e$$

Como $\deg \widehat{\phi} = \deg \phi = p$, su grado de separabilidad puede ser 1 ó p. En el primer caso:

$$\#E[p^e] = 1 \ \forall e \in \mathbb{N} \cup \{0\} \Rightarrow \#E[p^e] = \{O\} \ \forall e \in \mathbb{N} \cup \{0\}$$

En cambio, en el segundo caso:

$$\#E[p^e] = p^e \ \forall e \in \mathbb{N} \cup \{0\} \Rightarrow \#E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}} \ \forall e \in \mathbb{N} \cup \{0\}$$

□

Definición **2.2.** Dada una curva elíptica E y un número primo $l \in \mathbb{Z}$, se define el *l-ádico módulo de Tate* de E como el grupo

$$T_l(E) = \varprojlim_n E[l^n]$$

donde el límite inverso se toma utilizando las aplicaciones naturales de multiplicar por l:

$$[l] : \ E[l^{n+1}] \to E[l^n] : \ P \mapsto [l]P$$

La importancia del módulo de Tate reside en el hecho de que toda isogenia entre dos curvas elípticas puede expresarse como un homomorfismo entre sus módulos de Tate, siendo esta relación funtorial. Para ver esto, necesitamos considerar primero unos lemas.

Lema **2.1.** Un subgrupo aditivo $\Gamma \subset \mathbb{R}^n$ discreto es finitamente generado.

Demostración. Sea V el subespacio vectorial de $\mathbb{R}^n$ generado por los elementos de Γ y tomamos una base $u_1, \dots, u_m$ de V contenida en Γ. Entonces, tenemos

$$\Gamma_0 := \mathbb{Z}u_1 + \cdots + \mathbb{Z}u_m \subset \Gamma$$

Afirmamos que el índice $(\Gamma : \Gamma_0)$ es finito. En efecto, de cada elemento del cociente, podemos tomar un representante dentro de la celda fundamental

$$\Phi_0 = \{x_1u_1 + \cdots + x_mu_m : x_i \in [0,1) \ \forall i = 1, \dots, m\}$$

Estos representantes constituyen un conjunto discreto contenido en un conjunto precompacto, por lo que tienen que ser un conjunto finito.

Si denotamos $q := (\Gamma : \Gamma_0)$, entonces $q\Gamma \subset \Gamma_0$, es decir,

$$\Gamma \subset \frac{1}{q}\Gamma_0 = \mathbb{Z}\left(\frac{1}{q}u_1\right) + \cdots + \mathbb{Z}\left(\frac{1}{q}u_m\right)$$

Por tanto, Γ es un subgrupo de un grupo abeliano libre finitamente generado. Como $\mathbb{Z}$ es dominio de ideales principales, Γ admite una base como $\mathbb{Z}$-módulo formada por m o menos elementos. □

Lema **2.2.** Sea $M \subset \mathrm{Hom}(E_1, E_2)$ un subgrupo finitamente generado. Definimos

$$M^{div} = \{\phi \in \mathrm{Hom}(E_1, E_2) : [m] \circ \phi \in M \text{ para algún } m \in \mathbb{N}\}$$

Entonces, M^{div} es finitamente generado.

Demostración. En $\mathrm{Hom}(E_1, E_2)$ tenemos definida una forma cuadrática

$$\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z} : \ \phi \mapsto \deg(\phi)$$

Si $M \subset \mathrm{Hom}(E_1, E_2)$ es un subgrupo finitamente generado, la restricción del grado a M da una nueva forma cuadrática en M. Como M es finitamente generado y no tiene elementos de torsión, el teorema de estructura de $\mathbb{Z}$ módulos finitamente generados dice que M es un $\mathbb{Z}$-módulo libre. De esta forma, los elementos de una base de M forman una base de $M \otimes \mathbb{R}$ como $\mathbb{R}$-espacio vectorial y podemos extender la forma cuadrática al producto tensorial.

Como $\mathrm{Hom}(E_1, E_2)$ es un $\mathbb{Z}$-módulo libre de torsión, tenemos una inclusión natural

$$M^{div} \subset M \otimes \mathbb{R} : \ \psi \mapsto ([m] \circ \psi) \otimes \frac{1}{m}$$

donde m es el mínimo entero tal que $[m] \circ \psi \in M$, es decir, el orden de ψ en el cociente M^{div}/M. Además, dada $\phi \in M^{div}$ y sea $m \in \mathbb{N}$ tal que $[m] \circ \phi \in M$, entonces

$$\deg \phi = \frac{1}{m^2} \deg([m] \circ \phi) \in \mathbb{Z}$$

El grado es una forma bilineal en $M \otimes \mathbb{R}$, luego es continua, por lo que el conjunto

$$U = \{\phi \in M \otimes \mathbb{R} : \deg \phi < 1\}$$

es un entorno abierto del 0 tal que $M^{div} \cap U = \{0\}$. De este modo, M^{div} es un subgrupo discreto de $\mathbb{R}^n$, luego es finitamente generado por el lema 2.1

□

Teorema **2.1.** Sean E_1 y E_2 curvas elípticas y sea $l \neq \text{char}(K)$ un número primo. Entonces existe una aplicación natural inyectiva

$$\text{Hom}(E_1, E_2) \otimes \mathbb{Z}_l \to \text{Hom}\left(T_l(E_1), T_l(E_2)\right)$$

Demostración. Si tenemos una isogenia $\phi : E_1 \to E_2$, la podemos considerar como un homomorfismo de grupos, de manera que podemos restringirla a los puntos de torsión

$$\phi : \ E_1[l^n] \to E_2[l^n]$$

Además, precisamente por ser homomorfismos de grupos, conmutan bien con las aplicaciones que definen el límite inverso, luego podemos considerar sus aplicaciones asociadas

$$\phi_l : \ T_l(E_1) \to T_l(E_2)$$

Además, hemos dicho que $T_l(E_2)$ es un $\mathbb{Z}_l$-módulo, de modo que podemos definir la aplicación bilineal

$$\text{Hom}(E_1, E_2) \times \mathbb{Z}_l \to \text{Hom}\left(T_l(E_1), T_l(E_2)\right) : \ (\phi, a) \mapsto a \cdot \phi_l$$

Por la propiedad universal del producto tensorial, tenemos el homomorfismo

$$\Psi : \text{Hom}(E_1, E_2) \otimes \mathbb{Z}_l \to \text{Hom}\left(T_l(E_1), T_l(E_2)\right) : \ \phi \otimes a \mapsto a \cdot \phi_l$$

Veamos que Ψ es inyectiva. Sea entonces $\phi \in \ker \Psi \subset \text{Hom}(E_1, E_2) \otimes \mathbb{Z}_l$. Entonces, por las propiedades del producto tensorial, existe un submódulo finitamente generado $M \subset \text{Hom}(E_1, E_2)$ tal que $\phi \in M \otimes \mathbb{Z}_l$. Según el lema anterior M^{div} es finitamente generado y no tiene elementos de torsión, luego por el teorema de estructura de grupos abelianos finitamente generados, M^{div} es un grupo abeliano libre. Sea entonces

$$\{\psi_1, \ldots, \psi_t\} \subset \text{Hom}(E_1, E_2)$$

una base de M^{div}, por lo que existen ciertos (y únicos) $\alpha_1, \ldots, \alpha_t \in \mathbb{Z}_l$ tales que

$$\phi = \alpha_1\psi_1 + \cdots + \alpha_t\psi_t$$

Fijemos ahora un $n \in \mathbb{N}$ y elijamos $a_1, \ldots, a_t \in \mathbb{Z}$ tales que

$$a_i \equiv \alpha_i \ (\text{mód } l^n)$$

Si $\Psi(\phi) = 0$, tenemos que la isogenia

$$\psi = [a_1] \circ \psi_1 + \cdots + [a_t] \circ \psi_t \in \text{Hom}(E_1, E_2)$$

se anula en $E_1[l^n]$. Así, $\ker[l^n] \subset \ker[\psi]$, luego existe un a isogenia $\lambda : E_1 \to E_2$ que verifica que

$$\psi = \lambda \circ [l^n] = [l^n] \circ \lambda$$

donde hemos usado que λ también es homomorfismo de grupos por ser una isogenia. Entonces $\lambda \in M^{div}$, luego puede escribirse como

$$\lambda = [b_1] \circ \psi_1 + \cdots + [b_t] \circ \psi_t$$

Como $\{\psi_1, \ldots, \psi_t\}$ es una base de M^{div} como $\mathbb{Z}$-módulo, estas expresiones son únicas, luego $a_i = l^n b_i \ \forall i = 1, \ldots, t$. Entonces, $\alpha_i \equiv 0 \ (\text{mod } l^n)$. Como esto vale para todo $n \in \mathbb{N}$, se tiene que $\alpha_i = 0 \ \forall i = 1, \ldots, t$ y, por tanto, $\phi = 0$. Entonces, Ψ es inyectiva. □

Corolario **2.1.** Sean E_1 y E_2 curvas elípticas. Entonces $\text{Hom}(E_1, E_2)$ es un $\mathbb{Z}$-módulo libre de rango menor o igual que 4.

Demostración. Como $\text{Hom}(E_1, E_2)$ es un módulo sin elementos de torsión, y finitamente generado porque Ψ es inyectiva, el teorema de estructura de módulos finitamente generados sobre dominios de ideales principales afirma que es un grupo libre. Por tanto, el producto tensorial con $\mathbb{Z}_l$ también es libre como $\mathbb{Z}_l$-módulo y se verifica que:

$$\text{rank}_{\mathbb{Z}}\text{Hom}(E_1, E_2) = \text{rank}_{\mathbb{Z}_l} \ \text{Hom}(E_1, E_2) \otimes \mathbb{Z}_l$$

Por el teorema 2.1, tenemos que $\text{Hom}(E_1, E_2) \otimes \mathbb{Z}_l$ es isomorfo a un submódulo de $\text{Hom}\left(T_l(E_1), T_l(E_2)\right) \cong \mathcal{M}_2\left(\mathbb{Z}_l\right)$. Por tanto,

$$\text{rank}_{\mathbb{Z}_l} \ \text{Hom}(E_1, E_2) \otimes \mathbb{Z}_l \leq \text{rank}_{\mathbb{Z}_l} \ \text{Hom}\left(T_l(E_1), T_l(E_2)\right) = \text{rank}_{\mathbb{Z}_l}\mathcal{M}_2\left(\mathbb{Z}_l\right) = 4$$

□

3. Grupo de endomorfismos de una curva elíptica

Los resultados obtenidos a partir del módulo de Tate, nos permiten caracterizar el grupo de endomorfismos de una curva elíptica $End(E)$. Hasta ahora, conocemos una serie de características de este que nos van a permitir caracterizarlo:

- $End(E)$ es un anillo de característica cero, sin divisores de cero y con rango menor o igual que 4 como $\mathbb{Z}$-módulo.
- $End(E)$ tiene una antiinvolución $\phi \mapsto \hat{\phi}$ que verifica las siguientes propiedades:

$$\widehat{\psi \circ \phi} = \widehat{\phi} \circ \widehat{\psi}, \quad \widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}, \quad \hat{\hat{\phi}} = \phi$$

- Para todo $\phi \in End(E)$, $\phi\widehat{\phi} = \deg \phi \geq 0$ y $\phi\widehat{\phi} = 0 \Leftrightarrow \phi = 0$.

Veremos que estas propiedades permiten caracterizar el anillo de endomorfismos $End(E)$.

Definición **3.1.** Sea $\mathcal{K}$ una $\mathbb{Q}$-álgebra (no necesariamente conmutativa) finitamente generada. Un *orden* $\mathcal{R}$ de $\mathcal{K}$ es un subanillo finitamente generado como $\mathbb{Z}$-módulo que verifica que $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

Definición **3.2.** Un *álgebra de cuaterniones* es un álgebra de la forma

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

donde la operación multiplicativa verifica que

$$\alpha^2, \beta^2 \in \mathbb{Q}, \quad \alpha^2 < 0, \ \beta^2 < 0, \ \beta\alpha = -\alpha\beta$$

Teorema **3.1.** Sea $\mathcal{R}$ un anillo de característica 0 sin divisores de cero que verifica las siguientes propiedades:

1. $\mathcal{R}$ tiene rango menor o igual que 4 como $\mathbb{Z}$-módulo.
2. $\mathcal{R}$ tiene una anti-involución $\alpha \mapsto \hat{\alpha}$ tal que

$$\widehat{\alpha + \beta} = \widehat{\alpha} + \widehat{\beta}, \quad \widehat{\alpha\beta} = \widehat{\beta}\widehat{\alpha}, \quad \hat{\hat{\alpha}} = \alpha, \ \widehat{n} = n \ \forall n \in \mathbb{Z} \subset \mathcal{R}$$

3. Para todo $\alpha \in \mathcal{R}$, el producto $\alpha\hat{\alpha}$ es un entero no negativo y $\alpha\hat{\alpha} = 0$ si y sólo si $\alpha = 0$.

Entonces $\mathcal{R}$ verifica una de las siguientes afirmaciones:

- $\mathcal{R} \cong \mathbb{Z}$.
- $\mathcal{R}$ es un orden de una extensión cuadrática imaginaria de $\mathbb{Q}$.
- $\mathcal{R}$ es un orden de un álgebra de cuaterniones sobre $\mathbb{Q}$.

Demostración. Sea $\mathcal{K} = \mathcal{R} \otimes \mathbb{Q}$. Como $\mathcal{R}$ es finitamente generado como $\mathbb{Z}$-módulo, basta ver que $\mathcal{K}$ es bien $\mathbb{Q}$, bien un cuerpo cuadrático imaginario o bien un álgebra de cuaterniones. Extendemos la involución a $\mathcal{K}$ de la forma natural:

$$\mathcal{R} \otimes \mathbb{Q} \to \mathcal{R} \otimes \mathbb{Q} : \ \phi \otimes q \mapsto \widehat{\phi} \otimes q$$

Ahora, definimos la norma y la traza en $\mathcal{K}$:

$$N : \mathcal{K} \to \mathbb{Q} : \ \alpha \mapsto \alpha\hat{\alpha}, \quad T : \mathcal{K} \to \mathbb{Q} : \alpha \mapsto \alpha + \widehat{\alpha}$$

Estas aplicaciones verifican las siguientes propiedades

- $T\alpha = 1 + N\alpha - N(\alpha - 1) \ \forall \alpha \in \mathcal{K}$.
- T es $\mathbb{Q}$-lineal.
- $\alpha \in \mathbb{Q} \Rightarrow T\alpha = 2\alpha$
- $T\alpha = 0 \Rightarrow 0 = (\alpha - \alpha)(\alpha - \widehat{\alpha}) = \alpha^2 - (T\alpha)\alpha + N\alpha = \alpha^2 + N\alpha \Rightarrow \alpha^2 = -N\alpha$ Por tanto, $\alpha \neq 0 \wedge T\alpha = 0 \Rightarrow \alpha^2 \in \mathbb{Q}, \wedge \alpha^2 < 0$.

Si $\mathcal{K} = \mathbb{Q}$, no hay nada que probar. En caso contrario, $\exists \alpha \in \mathcal{K} \setminus \mathbb{Q}$. Reepmplazando α por $\alpha - \frac{1}{2}T\alpha$, podemos suponer que $T\alpha = 0$. De este modo, $\alpha^2 \in \mathbb{Q}$ y $\alpha^2 < 0$, luego $\mathbb{Q}(\alpha)$ es una extensión cuadrática imaginaria de $\mathbb{Q}$. Nuevamente, si $\mathcal{K} = \mathbb{Q}(\alpha)$, ya hemos acabado.

En caso contrario, $\exists \beta \in \mathcal{K} \setminus \mathbb{Q}(\alpha)$. Reemplazamos β por

$$\beta - \frac{1}{2}T\beta - \frac{T(\alpha\beta)}{2\alpha^2}\alpha = 0$$

Fácilmente se ve que

$$T\beta = T(\alpha\beta) = 0$$

En particular, $\beta^2 \in \mathbb{Q}$ y $\beta^2 < 0$. Además, como las trazas son nulas, $\alpha = -\widehat{\alpha}$, $\beta = -\widehat{\beta}$ y $\alpha\beta = -\widehat{\alpha\beta}$. Entonces,

$$\alpha\beta = -\widehat{\alpha\beta} = -\widehat{\beta}\widehat{\alpha} = -\beta\alpha$$

Por tanto, se tiene que

$$\mathbb{Q}[\alpha, \beta] = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

Falta únicamente ver que $\mathbb{Q}[a, b] = \mathcal{K}$. Para ver esto, como $\dim_{\mathbb{Q}} \mathcal{K} = 4$, únicamente hace falta ver que 1 ,α, β y $\alpha\beta$ son linealmente independientes sobre $\mathbb{Q}$. Sea una combinación lineal

$$w + x\alpha + y\beta + z\alpha\beta = 0, \quad w, x, y, z \in \mathbb{Q}$$

Tomando trazas, llegamos a que $w = 0$. Multiplicando por α por la izquierda y por β por la derecha, llegamos a

$$(x\alpha^2)\beta + (y\beta^2)\alpha + z\alpha^2\beta^2 = 0$$

Como 1, α y β son linealmente independientes porque $\alpha \notin \mathbb{Q}$ y $\beta \notin \mathbb{Q}(\alpha)$, entonces

$$x\alpha^2 = y\beta^2 = z\alpha^2\beta^2 = 0$$

y como $\alpha^2, \beta^2 \in \mathbb{Q}^*$, entonces $x = y = z = 0$.

□

4. Representaciones de Galois

Si E es una curva elíptica definida sobre K, la ley de grupo viene dada por funciones racionales definidas sobre K, de modo que conmuta con los automorfismos del grupo de Galois $\mathcal{G}(\overline{K}|K)$, en el sentido de que

$$(P_1 + P_2)^\sigma = P_1^\sigma + P_2^\sigma \ \forall P_1, P_2 \in E, \ \forall \sigma \in \mathcal{G}(\overline{K}|K) \tag{1}$$

En particular,

$$[m]\,(P^\sigma) = ([m]P)^\sigma = O^\sigma = O \ \forall \sigma \in \mathcal{G}(\overline{K}|K)$$

Entonces, obtenemos una representación del grupo de Galois

$$\mathcal{G}(\overline{K}|K) \to \mathrm{Aut}\,([E[m])$$

Además, según la ecuación 4, la acción de Galois conmuta con los homomorfismos del límite directo que define el módulo de Tate, por lo que tenemos otra representación

$$\rho_l : \mathcal{G}(\overline{K}|K) \to \mathrm{Aut}\,(T_l(E))$$

que se denomina *l-ádica representación de* $\mathcal{G}(\overline{K}|K)$ *asociada a* E.

5. La diferencial invariante

Definición **5.1.** Dada una curva elíptica E definida sobre K por la ecuación de Weierstrass

$$E : F(x, y) = y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = 0$$

se define su deferencial invariante como

$$\omega := \frac{dx}{2y + a_1x + a_3} \in \Omega_E$$

Lema **5.1.** Sea E una curva elíptica. Su diferencial invariante ω no tiene ceros ni polos.

Demostración. Sea $P = (x_0, y_0) \in E \setminus \{0\}$ y supongamos que E se describe por la ecuación de Weierstrass

$$E : F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

de modo que la diferencial invariante se escribe

$$\omega = \frac{d(x - x_0)}{F_y(x, y)} = -\frac{d(y - y_0)}{F_x(x, y)}$$

F no puede tener un polo, puesto que, en tal caso, $F_x(P) = F_y(P) = 0$ y E sería singular en P.

Como $[K(E) : K(x)] = 2$, entonces $\mathrm{ord}_P(x-x_0) \leq 2$ dándose la igualdad si y sólo si el polinomio cuadrático $F(x_0, y)$ tiene una raíz doble. En resumen, bien $\mathrm{ord}_P(x - x_0) = 1$ o bien $\mathrm{ord}_P(x - x_0) = 2$ y $F_y(x_0, y_0) = 0$. En ambos casos,

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P(x - x_0) - \mathrm{ord}_P(F_y) - 1 = 0^1$$

En cuanto al punto O, sea t un uniformizador en O. Entonces, $x = t^-2f$ e $y = t^{-3}g$, para ciertas funciones $f, g \in K(E)$ tales que $\mathrm{ord}_P(f) = \mathrm{ord}_P(g) = 0$. Entonces

$$\omega = \frac{dx}{F_y(x, y)} = \frac{-2f + tf'}{2g + a_1tf + a_3t^3}dt$$

Si $\mathrm{char}(K) \neq 2$, entonces se ve que $\mathrm{ord}_P(\omega) = 0$, mientras que si $\mathrm{char}(K) = 2$, entonces este hecho se vería a partir de que

$$\omega = -\frac{dy}{F_x(x, y)} = \frac{-3g + tg'}{3f^2 + 2aft^2 + a_4 - a_1tg}$$

□

Proposición **5.1.** Sea E una curva elíptica definida sobre K y ω su diferencial invariante. Sea $Q \in E$ y $\tau_Q : E \to E : \ P \mapsto P + Q$. Entonces,

$$\tau_Q^*\omega = \omega$$

Demostración. Como Ω_E es un $\overline{K}(E)$-espacio vectorial de dimensión 1, existe $a_Q \in \overline{K}(E)$ tal que $\tau_Q^*\omega = a_Q\omega$. Entonces,

$$\mathrm{div}(a_Q) = \mathrm{div}(\tau_Q^*\omega) - \mathrm{div}(\omega) = \tau_Q^*\mathrm{div}(\omega) - \mathrm{div}(\omega) = 0$$

Por tanto, $a_Q \in \overline{K}$ por no tener ceros ni polos. Si consideramos la aplicación

$$f : E \to \mathbb{P}^1 : \ Q \mapsto [a_Q, 1]$$

Esta función es racional porque a_Q puede expresarse como una función racional de $x(Q)$ e $y(Q)$, ya que se escribe como

$$\frac{dx(P + Q)}{2y(P + Q) + a_1x(P + Q) + a_3} = a_Q\frac{dx(P)}{2y(P) + a_1x(P) + a_3}$$

luego f es una función racional. Como $[1 : 0] \notin \mathrm{Im}(f)$, se tiene que f es constante. Por tanto,

$$a_Q = a_O = 1 \ \forall Q \in E \Rightarrow \tau_Q^*\omega = \omega \ \forall Q \in E$$

□

Teorema **5.1.** Sean E y E' dos curvas elípticas, sea ω la diferencial invariante de E y sea $\phi, \psi : E' \to E$ isogenias. Entonces,

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$$

Demostración. Si $\phi = [0]$ o $\psi = [0]$, la igualdad es clara. Si $\phi + \psi = [0]$. entonces

$$\psi^* = (-\phi)^* = \phi^* \circ [-1]^*$$

[1] El caso $\mathrm{char}(K) = 2$ merece un comentario especial. En ese caso, F_{yy} sería idénticamente cero, por lo que $F(x_0, y)$ tendría orden infinito, de modo que ω no sería regular en P, lo que ya se ha dicho que no es posible.

de modo que únicamente hace falta comprobar que $[-1]^*\omega = -\omega$. Esto es evidente a partir de la fórmula de negación

$$[-1](x,y) = (x, -y - a_1x - a_3) \Rightarrow$$
$$[-1]^*\omega = [-1]^*\left(\frac{dx}{2y + a_1x + a_3}\right) = \frac{dx}{2(-y - a_1x - a_3) + a_1x + a_3} = -\frac{dx}{2y + a_1x + a_3} = -\omega$$

En adelante, supongamos que ni ϕ, ni ψ ni $\phi + \psi$ son nulas. Dadas las coordenadas de Weierstrass (x_1, y_1) y (x_2, y_2), la suma

$$(x_3, y_3) := (x_1, y_1) + (x_2, y_2)$$

viene dada por la ley de grupo. Como los pares (x_1, y_1) y (x_2, y_2) satisfacen la ecuación de Weierstrass de E, se tiene que

$$(2y_i + a_1x_i + a_3)dy_i = (3x_i^2 + 2a_2x_i + a_4 - a_1y_i)dx_i \ \forall i = 1, 2$$

de modo que, por las reglas de diferenciacion $\omega(x_3, y_3)$ se escribe como

$$\omega(x_3, y_3) = f(x_1, y_1, x_2, y_2)\omega(x_1, y_1) + g(x_1, y_1, x_2, y_2)\omega(x_2, y_2)$$

Queremos ver que tanto f como g son idénticamente 1. Para ello, fijamos los valores de $x_2 = x(Q)$ y $y_2 = y(Q)$. Entonces $dx_2 = dx(Q) = 0$, luego $\omega(x_2, y_2) = 0$. Por la proposición 5.1,

$$\omega(x_3, y_3) = \tau_Q^*\omega(x_1, y_1) = \omega(x_1, y_1)$$

Así, $f(x_1, y_1, x(Q), y(Q)) = 1$, para todo $x_1, y_1 \in \overline{K}$. Como esto vale para todo $x(Q)$ e $y(Q)$, tenemos que $f \equiv 1$. Análogamente, $g \equiv 1$. Recapitulando, si $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ (con la operación de grupo de la curva), entonces tenemos (sumando como diferenciales)

$$\omega(x_3, y_3) = \omega(x_1, y_1) + \omega(x_2, y_2)$$

Entonces, tenemos que

$$(\omega \circ (\phi + \psi))(x, y) = (\omega \circ \phi)(x, y) + (\omega \circ \psi)(x, y)$$

Como esto vale para todos los valores de x e y, escribimos

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$$

□

Corolario **5.1.** Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$ de característica p y sea ϕ su automorfismo de Frobenius. Entonces $1 - \phi$ es separable.

Demostración. Tenemos que

$$(1 - \phi)^*\omega = \omega - \phi^*\omega = \omega$$

de modo que $(1 - \phi)^*$ no es nula y, por tanto, $1 - \phi$ es separable. □

6. Teorema de Hasse

Lema **6.1.** Sea A un grupo abeliano y sea $d : A \to \mathbb{Z}$ una forma cuadrática definida positiva. Entonces,

$$|d(\psi - \phi) - d(\phi) - d(\psi)| \leq 2\sqrt{d(\phi)d(\psi)}$$

Demostración. Sea

$$L(\psi, \phi) = d(\psi - \phi) - d(\psi) - d(\phi)$$

la forma bilineal asociada. Como d es definida positiva, se tiene que

$$d(m\psi + n\phi) = m^2d(\psi) + mnL(\psi, \phi) + n^2d\phi \geq 0 \ \forall m, n \in \mathbb{Z}$$

Tomando

$$m = -L(\psi, \phi), \quad n = 2d(\psi)$$

tenemos que

$$d(\psi)\left(4d(\phi)d(\psi) - L(\psi, \phi)^2\right) \geq 0$$

Entonces, como d es definida positiva, si $\psi \neq 0$, entonces $d(\psi) \neq 0$ y ha de cumplirse la desigualdad buscada. El caso en el que $\psi = 0$ es trivial. □

Teorema **6.1.** (Hasse) Sea E una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$. Entonces,

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

Demostración. Consideramos una ecuación de Weierstrass para E con coeficientes en $\mathbb{F}_q$ y sea

$$\phi : E \to E,\ (x, y) \mapsto (x^q, y^q)$$

el morfismo de Fröbenius asociado a la potencia q. Entonces, dado $P \in E(\overline{\mathbb{F}_q})$, se tiene que

$$P \in E(\mathbb{F}_q) \Leftrightarrow \phi(P) = P$$

Esto equivale a decir que

$$E(\mathbb{F}_q) = \ker(1 - \phi)$$

Como, por el corolario 5.1, $(1 - \phi)$ es separable:

$$\#E(\mathbb{F}_q) = \#\ker(1 - \phi) = \deg(1 - \phi)$$

Y como el grado es una forma cuadrática, la desigualdad se sigue del lema 6.1 teniendo en cuenta que $\deg \phi = q$. □

El módulo de Tate nos proporciona un método para computar $\#E(\mathbb{F}_{q^n})$ a partir de $\#E(\mathbb{F}_q)$. Esto puede verse a partir de la igualdad $\deg \phi = \det(\phi_l)$ (ver apéndice). A partir de esta igualdad, un cálculo directo da la igualdad

$$\mathrm{tr}(\phi) = 1 + \deg(\phi) - \deg(1 - \phi)$$

En particular, para el homomorfismo de Fröbenius, tenemos que su traza es

$$a = 1 + q - \#E(\mathbb{F}_q)$$

Entonces, su imagen $\phi_l \in End(T_l(E))$ es raíz de su polinomio característico:

$$\phi_l^2 - a\phi_l + q = (\phi_l - \alpha)(\phi_l - \beta) = 0$$

donde α y β son las raíces de este polinomio en $\overline{\mathbb{Q}_l}$. Además como la inclusión $\Psi : End(E) \otimes \mathbb{Z}_l \hookrightarrow End(T_l(E))$, el morfismo de Fröbenius ϕ también verifica esta ecuación.

De manera análoga a como lo hemos visto con $1 - \phi$, podemos demostrar que $1 - \phi^n$ es separable. Entonces, si expresamos ϕ_l en su forma de Jordan (en el cuerpo $\overline{\mathbb{Q}_p}$), tenemos que

$$\#E(\mathbb{F}_{q^n}) = \#\ker(1 - \phi^n) = \deg(1 - \phi^n) = \det(1 - \phi_l^n) = \begin{vmatrix} 1 - \alpha^n & x \\ 0 & 1 - \beta^2 \end{vmatrix} = 1 - \alpha^n - \beta^n + q^n$$

Esta operación se basa en la aritmética del cuerpo de descomposición del polinomio $T^2 - aT + q$ sobre $\mathbb{Q}$. Como este cuerpo de descomposición es único salvo isomofía, puede suponerse contenido en $\mathbb{C}$ a efectos de calcular el determinante.

7. Apéndice: El emparejamiento de Weil

El objetivo de este apéndice es probar que, dada una isogenia $\phi \in End(E)$, entonces $\deg \phi = \det \phi_l$. Para ello, necesitamos una forma bilineal que cumpla ciertas propiedades. Su construcción se conoce como *emparejamiento de Weil*.

Definición **7.1.** Dado un punto $T \in E[m]$ como la ley de grupo de la curva coincide con la de $Pic^0(E)$, entonces, existe $f \in \overline{K}(E)$ tal que

$$\mathrm{div}(f) = m(T) - m(O)$$

Análogamente, tomando un $T' \in E$ tal que $[m]T' = T$, existe $g \in \overline{K}(E)$ tal que

$$\mathrm{div}(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (T' + R) - (R)$$

Entonces, salvo multiplicación más constantes, tenemos que

$$m\,\mathrm{div}(g) = [m]^*\mathrm{div}(f) = \mathrm{div}([m]^* f) = \mathrm{div}(f \circ [m]) \Rightarrow g^m = f \circ [m]$$

Sea entonces otro $S \in E[m]$, entonces para todo $X \in E$, se tiene que

$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m$$

Entonces, el morfismo

$$E \to \mathbb{P}^1 : \ X \mapsto \frac{g(X+S)}{g(X)}$$

no es suprayectivo porque toma únicamente valores en las raices m-ésimas de la unidad. Por tanto, es constante. Así, definimos el *emparejamiento de Weil* como

$$e_m : E[m] \times E[m] \mapsto \mu_m : \ (S,T) \mapsto e_m(S,T) = \frac{g(X+S)}{g(X)}$$

Proposición **7.1.** El emparejamiento de Weil es bilinear.

$$e_m(S_1+S_2,T) = e_m(S_1,T)E_m(S_2,T)$$
$$e_m(S,T_1+T_2) = e_m(S,T_1)e_m(S,T_2)$$

Demostración. La linealidad en la primera variable viene de

$$e_m(S_1+S_2,T) = \frac{g(X+S_1+S_2)}{g(X)} = \frac{g(X+S_1+S_2)}{g(X+S_1)}\frac{g(X+S_1)}{g(X)} = e_m(S_2,T)e_m(S_1,T)$$

Para ver la linealidad de la segunda. variable, sean $f_1, f_2, f_3, g_1, g_2, g_3$ las funciones racionales asociadas a T_1, T_2 y $T_3 = T_1 + T_2$. Además, $\exists h \in \overline{K}(E)$ tal que

$$\mathrm{div}(h) = (T_1+T_2) - (T_1) - (T_2) - (O)$$

Entonces,

$$\mathrm{div}\left(\frac{f_3}{f_1 f_2}\right) = m\mathrm{div}(h) \Rightarrow \exists c \in \overline{K}^* : f_3 = c f_1 f_2 h^m \Rightarrow \exists c' \in \overline{K}^* : g_3 = c' g_1 g_2 (h \circ [m])$$

Por tanto,

$$e_m(S,T_1+T_2) = \frac{g_3(X+S)}{g_3(X)} = \frac{g_1(X+S)g_2(X+S)h([m]X+[m]S)}{g_1(X)g_2(X)h([m]X)} = e_m(S,T_1)e_m(S,T_2)$$

□

Proposición **7.2.** El emparejamiento de Weil es alternado, es decir, $e_m(S,T) = e_m(T,S)^{-1}$.

Demostración. Por la bilinealidad, se tiene que

$$e_m(S+T,S+T) = e_m(S,S)e_m(S,T)e_m(T,S)e_m(T,T) \ \forall S,T \in E[m]$$

Entonces, basta ver que $e_m(T,T) = 1 \ \forall T \in E[m]$. Para ello, consideramos

$$\mathrm{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}\right) = m\sum_{i=0}^{m-1}[([1-i]T) - ([-i]T)] = 0 \Rightarrow \prod_{i=0}^{m-1} f \circ \tau_{[i]T} \in \overline{K}^* \Rightarrow \prod_{i=0}^{m-1} g \circ \tau_{[i]T'} \in \overline{K}^*$$

donde $T' \in E$ es tal que $[m]T' = T$ y donde la última implicación se debe a que su m-ésima potencia es la constante anterior. Por tanto, como el último producto toma el mismo valor en X y en $X+T'$, entonces

$$g(X) = g(X+[m]T') = g(X+T) \Rightarrow e_m(T,T) = \frac{g(X+T)}{g(X)} = 1$$

□

Proposición **7.3.** El emparejamiento de Weil es no degenerado:

$$e_m(S,T) = 1 \ \forall S \in E[m] \Rightarrow T = O$$

Demostración. Si $e_m(S,T) = 1 \ \forall S \in E[m]$, entonces $g(X+S) = g(X) \ \forall S \in E[M]$. Entonces, existe $h \in \overline{K}(E)$ tal que $g = h \circ [m]$. Así,

$(h\circ[m])^m = g^m = f\circ[m] \Rightarrow f = [h]^m \Rightarrow m\,\mathrm{div}(h) = \mathrm{div}(f) = m(T) - m(O) \Rightarrow \mathrm{div}(h) = (T) - (O) \Rightarrow (T) = (O)$

□

Proposición **7.4.** El emparejamiento de Weil verifica que

$$e_{mm'}(S,T) = e_m([m']S,T)\ \forall S \in E[mm'],\ \forall T \in E[m]$$

Demostración. Tomando f y g como en la definición de emparejamiento de Weil, tenemos que

$$\mathrm{div}(f^{m'}) = mm'(T) - mm'(O), \quad (g \circ [m'])^{mm'} = (f \circ [mm'])^{m'}$$

Entonces, directamente de la definición

$$e_{mm'}(S,T) = \frac{g \circ [m'](X+S)}{g \circ [m'](X)} = \frac{g([m']X + [m']S)}{g([m']X)} = e_m([m']S,T)$$

□

Proposición **7.5.** Si $\phi : E_1 \to E_2$ es una isogenia para todo $S \in E_1[m]$ y $T \in E_2[m]$, entonces

$$e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T)$$

Demostración. Por propiedades de las isogenias duales, existe $h \in \overline{K}(E)$ tal que

$$\phi^*((T)) - \phi^*((O)) = (\hat{\phi}T) - (O) + \mathrm{div}(h)$$

Entonces, se tiene que

$$\mathrm{div}\left(\frac{f \circ \phi}{h^m}\right) = \phi^* \mathrm{div}(f) - m\,\mathrm{div}(h) = m(\hat{\phi}T) - m(O)$$
$$\left(\frac{g \circ \phi}{h \circ [m]}\right)^m = \frac{f \circ [m] \circ \phi}{(h \circ [m])^m} = \left(\frac{f \circ \phi}{h^m}\right) \circ [m]$$

Entonces, de la definición se llega a

$$e_m(S, \hat{\phi}T) = \frac{(g \circ \phi)/(h \circ [m])(X+S)}{(g \circ \phi)/(h \circ [m])(X)} = \frac{g(\phi X + \phi S)}{g(\phi X)} \frac{h([m]X)}{h([m]X + [m]S)} = e_m(\phi S, T)$$

□

Definición **7.2.** El emparejamiento de Weil $e : T_l(E) \times T_l(E) \to T_l(\mu)$ se define como el límite inverso de los emparejamientos e_{l^n}. Esto puede definirse puesto que, de la proposición 7.4 se deduce que

$$e_{l^{n+1}}(S,T)^l = e_{l^n}([l]S, [l]T)$$

Corolario **7.1.** Existe una forma bilineal, alternada y no degenerada

$$e : T_l(E) \times T_l(E) \to T_l(\mu)$$

Además, si $\phi : E_1 \to E_2$ es una isogenia, entonces $e(\phi S, T) = e(S, \hat{\phi}T)$

Proposición **7.6.** Sea $\phi \in End(E)$ y sea $\phi_l : T_l(E) \to T_l(E)$ su homomorfismo inducido en el módulo de Tate. Entonces,

$$\det(\phi_l) = \deg(\phi)$$

Demostración. Sea $\{v_1, v_2\}$ una base de $T_l(E)$ como $\mathbb{Z}_l$ módulo. Escribimos $\phi_l(v_1) = av_1 + cv_2$ y $\phi_l(v_2) = bv_1 + dv_2$. Entonces, a partir de las propiedades del emparejamiento de Weil:

$$e(v_1,v_2)^{\deg\phi} = e([\deg\phi]v_1, v_2) = e(\hat{\phi}_l\phi_l v_1, v_2) = t(\phi_l v_1, \phi_l v_2) = e(v_1,v_2)^{\det\phi_l}$$

□

Como e es no degenerada, entonces $\deg\phi = \det\phi_l$.

Referencias

[1] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 2009

[2] Henning Stichtenoch. *Algebraic Function Fields and Codes.* Springer-Verlag, 2009.