UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN CIENCIAS MATEMÁTICAS

FACULTAD DE CIENCIAS

UNA DESCRIPCIÓN DE LAS EXTENSIONES DE UN CAMPO CUADRÁTICO IMAGINARIO.

QUE PARA OBTENER EL GRADO ACADÉMICO DE

MAESTRO EN CIENCIAS

P R E S E N T A

ADRIÁN ZENTENO GUTIÉRREZ

DIRECTOR DE LA TESINA:
TIMOTHY MOONEY GENDRON THORNTON

MÉXICO, D.F. ABRIL, 2011

UNA DESCRIPCIÓN DE LAS EXTENSIONES ABELIANAS DE UN CAMPO CUADRÁTICO IMAGINARIO

ADRIÁN ZENTENO GUTIÉRREZ

RESUMEN. Esta trabajo tiene como objetivo describir de manera detallada la teoría de multiplicación compleja para curvas elípticas así como brindar un panorama global de las distintas generalizaciones de ésta teoría. Dicha teoría nos proporciona una descripción completa de las extensiones abelianas de los campos cuadráticos imaginarios de la misma manera que las extensiones ciclotómicas describen las extensiones abelianas de $\mathbb{Q}$.

INDICE

1. INTRODUCCIÓN

El teorema de Kronecker-Weber, anunciado por Leopold Kronecker (1853) y demostrado por Heinrich Martin Weber (1886), describe las extensiones abelianas de $\mathbb{Q}$. De manera más precisa, dice que toda extensión abeliana de $\mathbb{Q}$ está contenida en una extensión generada por raíces de la unidad (extensiones ciclotómicas). Desde el punto de vista del análisis complejo, podemos construir las raíces de la unidad como valores especiales de la función exponencial.

El "Jugendtraum" de Kronecker ("sueño de juventud" de Kronecker), conocido también como el problema doce de Hilbert, sugiere que las extensiones abelianas de un campo numérico arbitrario deben estar contenidas en ciertas extensiones generadas por valores especiales de funciones analíticas.

Date: 25 de Abril de 2011.

El primer caso después de $\mathbb{Q}$, es respondido por la teoría de multiplicación compleja la cual proporciona una descripción completa de las extensiones abelianas de un campo cuadrático imaginario.

Estudiando funciones elípticas, Abel noto, que ciertas integrales elípticas tenían propiedades algebraicas inusuales. Estas integrales se convertían en múltiplos complejos de ellas mismas bajo ciertos cambios de variable. Este fenómeno fue conocido como "multiplicación compleja". Kronecker observo que los valores de estas integrales generaban extensiones abelianas de campos cuadráticos imaginarios. Motivado por el caso de extensiones ciclotómicas para $\mathbb{Q}$, conjeturo que todas las extensiones de un campo cuadrático imaginario podían ser obtenidas de este modo. Así fue como dio inicio la teoría de multiplicación compleja.

Kronecker y Weber demostraron sus resultados estudiando la expansión de Fourier de ciertas funciones modulares. Siguiendo esta linea, Hasse logra dar demostraciones completas de los principales resultados de la teoría de multiplicación compleja. Para un estudio detallado de la teoría de multiplicación compleja desde el punto de vista de funciones modulares véase [3] y [18].

Tiempo después la teoría de multiplicación compleja llego a ser vista desde una nueva perspectiva motivada por la geometría algebraica. La teoría de superficies de Riemann desarrollada en el siglo XIX, proporciona una correspondencia natural entre latices del plano complejo y curvas algebraicas de genero 1, conocidas como curvas elípticas. Luego, es posible investigar la teoría de multiplicación compleja estudiando las propiedades de las curvas elípticas en lugar de estudiar latices. Uno de los beneficios de este punto de vista es que las curvas elípticas pueden ser definidas sobre cualquier campo.

Deuring fue quien inicio esta nueva linea de investigación. Usando el proceso de reducción reconstruyo y extendió los resultados de Kronecker, Weber y Hasse y presento pruebas más simples y elegantes. Tomando ventaja de la elegancia y simplicidad de la formulación algebraica presentaremos una demostración completa de los resultados principales de multiplicación compleja siguiendo la linea de [16] y [22].

Agradecimientos: Agradezco al profesor Timothy Gendron por todas sus observaciones, consejos y paciencia en la dirección de este trabajo. Así mismo, agradezco a la Facultad de ciencias de la UNAM por la licencia con goce de sueldo durante el periodo 2011-2.

2. TEORÍA DE CAMPOS DE CLASE

En esta sección daremos un breve resumen de los conceptos de teoría de campos de clase que serán utilizados en el resto de este trabajo. Un estudio detallado sobre ésta teoría puede encontrarse en [5], [13] y [27].

Sea L/K una extensión finita y separable de campos numéricos y O_L, O_K sus anillos de enteros. Dado un ideal primo $\mathfrak{p} \neq 0$ de O_K, este se descompone en O_L de manera única como

$$\mathfrak{p} = \mathfrak{p}O_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \tag{1}$$

con e_i enteros positivos los cuales son llamados *indices de ramificación*. Diremos que los ideales $\mathfrak{P}_i$ *dividen a* $\mathfrak{p}$ y lo denotaremos como $\mathfrak{P}_i|\mathfrak{p}$.

Un ideal primo $\mathfrak{P}_i$ en la descomposición 1 es *no ramificado* si $e_i = 1$ y $k(\mathfrak{P}_i)/k(\mathfrak{p})$ [1] es separable, en otro caso se dice que $\mathfrak{P}_i$ *se ramifica*. Luego, se dice que $\mathfrak{p}$ es *no ramificado* si $\mathfrak{P}_i$ es no ramificado para toda $\mathfrak{P}_i$ que divide a $\mathfrak{p}$. Si L/K es separable se puede demostrar que sólo hay un número finito de ideales primos en O_K que se ramifican en O_L ([13] p. 49).

Por otro lado, al grado de la extensión de campos $f_i = [k(\mathfrak{P}_i) : k(\mathfrak{p})]$ lo llamaremos *grado de inercia* de $\mathfrak{P}_i$ sobre $\mathfrak{p}$. Si $[L : K] = n$ se tiene la siguiente identidad fundamental

$$\sum_{i=1}^{r} e_i f_i = n. \tag{2}$$

Se dice que un ideal primo $\mathfrak{p} \in O_K$ *no se escinde* sobre L si $r = 1$ en la descomposición 1 de lo contrario diremos que $\mathfrak{p} \in O_K$ *se escinde* en L. En particular, si $r = n$ diremos que $\mathfrak{p}$ se *escinde completamente* en L.

Sea L/K una extensión de Galois de un campo numérico y $\mathrm{Gal}(L/K)$ su grupo de Galois. Si $\mathfrak{P}|\mathfrak{p}$ entonces $\sigma\mathfrak{P}|\mathfrak{p}$ para todo $\sigma \in \mathrm{Gal}(L/K)$. A los ideales $\sigma\mathfrak{P}$ los llamaremos ideales primos *conjugados* a $\mathfrak{P}$. Es posible demostrar que $\mathrm{Gal}(L/K)$ actúa transitivamente en el conjunto de ideales primos de O_L que dividen a $\mathfrak{p}$ ([13] p. 54).

Si $\mathfrak{P}$ es un ideal primo de O_L el subgrupo

$$G_{\mathfrak{P}} = \left\{\sigma \in \mathrm{Gal}(L/K) : \sigma\mathfrak{P} = \mathfrak{P}\right\},$$

es llamado el *subgrupo de descomposición* de $\mathfrak{P}$ sobre K. En el caso Galois los indices de ramificación $e_1, \cdots, e_r$ en la descomposición 1 son independientes de i. Es decir, $e_1 = \ldots = e_r = e$. Luego, la identidad 2 se convierte en $n = efr$.

El núcleo $I_{\mathfrak{P}} \subset G_{\mathfrak{P}}$ del homomorfismo

$$G_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})),$$

es llamado el *grupo de inercia* de $\mathfrak{P}$ sobre K. Al campo fijo $T_{\mathfrak{P}}$ de $I_{\mathfrak{P}}$ lo llamaremos el *campo de descomposición* de $\mathfrak{P}$ sobre K. Luego, tenemos la siguiente sucesión exacta

$$1 \to I_{\mathfrak{P}} \to G_{\mathfrak{P}} \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \to 1,$$

de donde se sigue que $\left|I_{\mathfrak{P}}\right| = \left[L : T_{\mathfrak{P}}\right] = e$, pues $\left|G_{\mathfrak{p}}\right| = ef$ ([13] p. 57).

Supongamos que $\mathfrak{p}$ es no ramificado, entonces $I_{\mathfrak{P}} = \{1\}$ y $G_{\mathfrak{P}} \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$. Además, existe uno y sólo un automorfismo $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$ tal que

$$\sigma_{\mathfrak{P}} x \equiv x^q \bmod \mathfrak{P},$$

para toda $x \in O_L$, donde $q = N_{\mathbb{Q}}^K(\mathfrak{p}) = [k(\mathfrak{P}) : k(\mathfrak{p})]$. Este es llamado el *automorfismo de Frobenius* y se tiene que $G_{\mathfrak{P}}$ es un grupo cíclico generado por $\sigma_{\mathfrak{P}}$.

Si $\mathfrak{P}_1$ y $\mathfrak{P}_2$ son dos primos que dividen a $\mathfrak{p}$, $\sigma_{\mathfrak{P}_1}$ y $\sigma_{\mathfrak{P}_2}$ son conjugados. Luego, si L/K es una extensión abeliana podemos definir $\sigma_{\mathfrak{P}_1} = \sigma_{\mathfrak{P}_2} = \sigma_{\mathfrak{p}}$ como

$$\sigma_{\mathfrak{p}} x \equiv x^q \bmod \mathfrak{P},$$

para todo $\mathfrak{P}$ que divide a $\mathfrak{p}$.

Sea $\mathfrak{c}$ un ideal de O_K divisible por todos los ideales primos que se ramifican en L y sea $I(\mathfrak{c})$ el grupo de ideales fraccionarios de K primos relativos con $\mathfrak{c}$. Definimos el *mapeo de Artin*

$$(\cdot, L/K) : I(\mathfrak{c}) \to G(L/K),$$

como el homomorfismo de grupos definido localmente en los ideales primos por $(\mathfrak{p}, L/K) = \sigma_{\mathfrak{p}}$. Luego tenemos una versión débil de la ley de reciprocidad de Artin.

[1] $k(\mathfrak{P}_i) = O_L/\mathfrak{P}_i$ y $k(\mathfrak{p}) = O_K/\mathfrak{p}$

Teorema 1 (Ley de reciprocidad de Artin)**.** *([5] Cap. X) Sea L/K una extensión abeliana finita de campos numéricos. Entonces existe un ideal $\mathfrak{c} \subset O_K$, divisible precisamente por los ideales primos de K que se ramifican en L, tal que*

$$(\mathfrak{a}, L/K) = 1$$

para todo

$$\mathfrak{a} \in P(\mathfrak{c}) = \left\{(\alpha) : \alpha \in K^* \text{ y } \alpha \equiv 1 (\bmod \mathfrak{c})\right\}.$$

Si la ley de reciprocidad de Artin se cumple para $\mathfrak{c}_1$ y $\mathfrak{c}_2$ se cumple para $\mathfrak{c}_1 + \mathfrak{c}_2$. En consecuencia existe un ideal maximal $\mathfrak{c}_{L/K}$ para el cual se cumple ésta ley. A $\mathfrak{c}_{L/K}$ lo llamaremos el *conductor* de L/K.

Definición 1. Sea $\mathfrak{c}$ un ideal de O_K. El *campo de clase de rayos* de K (módulo $\mathfrak{c}$) es una extensión abeliana finita $K_\mathfrak{c}/K$ con la propiedad de que para toda extensión abeliana finita L/K, $\mathfrak{c}_{L/K}|\mathfrak{c}$ implica que $L \subset K_\mathfrak{c}$. Además, definimos el *grupo de clase de rayos* $Cl(\mathfrak{c})$ como el cociente

$$Cl(\mathfrak{c}) = I(\mathfrak{c})/P(\mathfrak{c}).$$

Intuitivamente podemos pensar al campo de clase de rayos como el campo "más grande" para un conductor dado.

Teorema 2 (Teoría de Campos de Clase)**.** *([13] Cap. VI, § 7) Sea L/K una extensión abeliana finita de un campo numérico y sea $\mathfrak{c}$ un ideal entero de K.*

i) *El mapeo de Artin*

$$(\cdot, L/K) : I(\mathfrak{c}_{L/K}) \longrightarrow \mathrm{Gal}(L/K),$$

es un homomorfismo suprayectivo.

ii) *El núcleo del mapeo de Artin es $(N_K^L I_L)P(\mathfrak{c}_{L/K})$ donde I_L es el grupo de ideales fraccionarios de L distintos de cero.*

iii) *Existe un único campo de clase de rayos $K_\mathfrak{c}$ de K (módulo $\mathfrak{c}$) y el conductor de $K_\mathfrak{c}/K$ divide a $\mathfrak{c}$.*

iv) *El campo de clase de rayos es caracterizado por la propiedad de ser una extensión abeliana de K donde los ideales primos de K que se escinden completamente en $K_\mathfrak{c}$ son exactamente los ideales primos de $P(\mathfrak{c})$.*

Definición 2. Definimos el *campo de clase de Hilbert* H de K, como el campo de clase de rayos de K módulo $\mathfrak{c} = (1)$.

El campo de clase de Hilbert de K es la extensión abeliana maximal en la cual todos los ideales primos de O_K son no ramificados.

Notemos que $I((1))$ coincide con el conjunto de todos los ideales fraccionarios no cero de K y $P((1))$ coincide con el conjunto de ideales principales de K. Luego, el mapeo de Artin induce el siguiente isomorfismo

$$(\cdot, H/K) : \mathscr{CL}(O_K) \xrightarrow{\cong} \mathrm{Gal}(H/K).$$

Donde $\mathscr{CL}(O_K) = Cl(O_K)$ es el campo de clase de ideales de O_K. Finalmente necesitaremos el siguiente teorema, el cual es una versión generalizada del teorema de Dirichlet para primos en progresiones aritméticas el cual afirma que dados $a, b \in \mathbb{Z}$ tales que $(a, b) = 1$ existe una infinidad de primos congruentes con a módulo b.

Teorema 3 (Dirichlet)**.** *([12] p. 345) Sea K un campo numérico y $\mathfrak{c}$ un ideal entero de K. Entonces cada clase de ideales en $I(\mathfrak{c})/P(\mathfrak{c})$ contiene un número infinito de primos con grado de inercia igual a 1.*

3. CURVAS ELÍPTICAS

En esta sección haremos un repaso breve y sin demostraciones de la teoría básica de curvas elípticas sobre un campo K. Para un estudio más detallado sobre curvas elípticas véase [2], [3], [14] y [21].

Definición 3. Una *curva elíptica* es una pareja (E,O), donde E es una curva proyectiva de genero 1 y O es un punto de E.[2] Diremos que la curva E es definida sobre K, y escribiremos E/K, si E es definida sobre K como curva y el punto $O \in E(K)$.

Usando el teorema de Riemann-Roch se puede demostrar que toda curva elíptica E/K, es isomorfa a una curva dada por *la ecuación de Weierstrass* (en su forma afín)

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

donde $a_i \in K$. Recíprocamente, toda curva suave dada por una ecuación de Weierstrass es una curva elíptica con $O = [0,1,0]$. Si la característica de K es distinta de 2 y 3 la ecuación de Weierstrass puede ser simplificada a la forma

$$E : y^2 = x^3 + Ax + B.$$

Bajo el supuesto de suavidad de E tenemos que el *discriminante*

$$\Delta = -16(4A^3 + 27B^2) \neq 0.$$

Luego, podemos definir el j-invariante asociado a E como

$$j(E) = -1728\frac{64A^3}{\Delta} = 1728\frac{64A^3}{4A^3 + 27B^2}.$$

Teorema 4. *(*[21] p. 50*) Sea E y E' curvas elípticas definidas sobre un campo algebraicamente cerrado $\bar{K}$. Entonces E es $\bar{K}$-isomorfa a E' si y sólo si $j(E) = j(E')$. Además, dado $j_0 \in \bar{K}$, existe una curva elíptica definida sobre $K(j_0)$ con j-invariante igual a j_0.*

Una de las propiedades más importantes de una curva elíptica es su estructura de grupo abeliano con O como elemento identidad. Esta estructura puede ser inducida de dos maneras. Una es dando una biyección entre E y la parte del grupo de divisores de grado cero de E ($\mathrm{Pic}^0(E)$). La otra es geometricamente utilizando su ecuación de Weierstrass y la ley de cuerda tangente.

Si el discriminate de E es cero la curva elíptica tiene exactamente un punto singular. Para este tipo de curvas tenemos dos posibilidades. Si el punto singular tiene dos distintas direcciones tangentes diremos que E tiene un $nodo$ y si sólo tiene una dirección tangente diremos que E tiene una *cúspide*. El conjunto E_{ns} de puntos no singulares de E, tiene estructura de grupo y es isomorfo a $\bar{K}^*$ si E tiene un nodo y a $\bar{K}^+$ si tiene una cúspide.

Un morfismo no constante $\phi : E_1 \to E_2$ entre curvas elípticas que satisface que $\phi(O) = O$ es llamado $isogenea$. Se puede probar que las isogeneas son los únicos morfismos entre curvas elípticas que preservan la estructura de grupo.

El conjunto de isogeneas de E_1 en E_2 forman un grupo bajo la adición el cual denotaremos por $\mathrm{Hom}(E_1,E_2)$. Más aun el conjunto $\mathrm{End}(E) = \mathrm{Hom}(E,E)$ tiene estructura de anillo donde el producto es inducido por la composición de isogeneas.

Para cada curva elíptica E y $m \in \mathbb{Z}$ tenemos la isogenea multiplicación por m

$$[m] : E \to E,$$

[2] A partir de ahora escribiremos E en lugar de (E,O).

definida como $P \mapsto P + \ldots + P$ (m-veces). Luego, estas isogeneas inducen una inyección

$$[\cdot] : \mathbb{Z} \to \mathrm{End}(E).$$

Cuando este mapeo no es un isomorfismo diremos que E tiene *multiplicación compleja por* $\mathrm{End}(E)$. De manera más precisa tenemos el siguiente teorema.

Teorema 5. *Dada E/K una curva elíptica se tiene que* $\mathrm{End}(E)$ *es isomorfo a*

i) $\mathbb{Z}$,
ii) *un orden en un campo cuadrático imaginario o*
iii) *un orden maximal en un álgebra cuaterniónica.*

De hecho, ésta ultima sólo ocurre si $\mathrm{char}(K) > 0$.

El núcleo de $[m]$ consiste de los puntos cuyo orden divide a m. Este subgrupo lo denotaremos por

$$E[m] = \ker[m] = \{P \in E : [m]P = O\}.$$

El *subgrupo de torsión* de E es el conjunto

$$E_{tors} = \left\{P \in E : [m]P = O \text{ para algún } m \geq 1\right\} = \bigcup_{m \geq 1} E[m].$$

De manera más general, si E es una curva elíptica con multiplicación compleja por $\mathrm{End}(E) \cong O_K$ (K un campo cuadrático imaginario), podemos definir el endomorfimo $[\alpha] : E \to E$, $\alpha \in O_K$, donde $[\alpha]$ es el endomorfismo asociado a $\alpha \in O_K$ vía el isomorfismo del teorema 5. Luego, para todo ideal entero $\mathfrak{a}$ de O_K definimos el *grupo de puntos de* $\mathfrak{a}$*-torsión* de E como el conjunto

$$E[\mathfrak{a}] = \left\{P \in E : [\alpha]P = 0 \text{ para todo } \alpha \in \mathfrak{a}\right\}.$$

Notemos que si $\mathfrak{a} = (m)$, $m \in \mathbb{Z}$, es un ideal principal se tiene que $E[\mathfrak{a}] = E[m]$. En particular, cuando E tiene multiplicación compleja se puede probar que $E[\mathfrak{a}]$ es un $O_K/\mathfrak{a}$-módulo libre de rango 1 ([22] p. 102).

Consideremos el caso particular de las curvas elípticas E definidas sobre un campo local K_v. Con ecuación de Weierstrass como en (3). Remplazando (x, y) por $(u^{-2}x, u^{-3}y)$, $u \in K_v$ podemos encontrar una ecuación de Weierstrass con todos sus coeficientes en O_v. Entonces, el discriminante Δ satisface $v(\Delta) \geq 0$ para v la valuación discreta de K_v, luego podemos elegir una ecuación de Weierstrass tal que el valor de $v(\Delta)$ sea mínimo. A dicha ecuación la llamaremos *ecuación mínima de Weierstrass* de E.

Consideremos el mapeo natural de $O_v \to k_v$ dado por $t \mapsto \tilde{t}$, donde $k_v = O_v/\pi O_v$ es el campo de residuos. Aplicando este mapeo a una curva elíptica E definida en K_v con ecuación minimal de Weierstrass obtenemos una curva $\tilde{E}/k_v$, posiblemente singular, llamada *la reducción de E módulo π*.

Sea E/K_v una curva elíptica y m un entero positivo primo relativo con $\mathrm{char}(k_v)$. Definimos *el mapeo de reducción*

$$E(K_v)[m] \to \tilde{E}(k_v), \tag{4}$$

donde $E(K_v)[m]$ es el conjunto de puntos de orden m en $E(K_v)$.

Teorema 6. *Sea E/K_v una curva elíptica. Si la curva reducida $\tilde{E}/k_v$ es no singular, el mapeo de reducción* (4) *es inyectivo.*

Si $K = \mathbb{C}$, existe una relación entre el conjunto de curvas elípticas $E/\mathbb{C}$ y el conjunto de latices $\Lambda \subset \mathbb{C}$.

Teorema 7 (Uniformización)**.** *(*[21] pp. 161-162*)*

i) *Sea $E/\mathbb{C}$ una curva elíptica. Entonces existe una latiz $\Lambda \subset \mathbb{C}$, única salvo homotecias, y un isomorfismo analítico*

$$\varphi : \mathbb{C}/\Lambda \to E(\mathbb{C}),$$

de grupos de Lie complejos dado por $z \mapsto \left[\mathscr{P}(z,\Lambda), \mathscr{P}'(z,\Lambda), 1\right]$, donde

$$\mathscr{P}(z,\Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

es la función $\mathscr{P}$ de Weierstrass y $\mathscr{P}'$ es su derivada.

ii) *Sea Λ una latiz de $\mathbb{C}$. Entonces el mapeo*

$$\phi : E(\mathbb{C}) \to \mathbb{C}/\Lambda,$$

es un isomorfismo de grupos de Lie complejos dado por $P \to \int_O^P dy/x \pmod{\Lambda}$.

Luego, dada una latiz $\Lambda \subset \mathbb{C}$ podemos definir la curva elíptica $E_\Lambda = \mathbb{C}/\Lambda$.

Lema 1. *Sean E_Λ una curva elíptica con multiplicación compleja por $End(E_\Lambda) = O_K$ (K un campo cuadrático imaginario) y (ω_1, ω_2) generadores de Λ. Entonces existe una latiz Λ' homotetica a Λ tal que $\Lambda' \subset K$.*

Demostración. Definimos $\Lambda' = \mathbb{Z} \oplus \tau\mathbb{Z}$, $\tau = \omega_1/\omega_2$, la cual es homotetica a Λ. Sea

$$R = \left\{ \alpha \in \mathbb{C} : \alpha\Lambda' \subset \Lambda \right\} \cong \mathrm{End}(E_\Lambda).$$

Para toda $\alpha \in R$ existe $a, b, c, d \in \mathbb{Z}$, tales que $\alpha = a + \tau b$ y $\tau\alpha = c + \tau d$. Eligiendo $\alpha \in R - \mathbb{Z}$ tenemos que $b \neq 0$ y τ satisface la siguiente ecuación cuadrática

$$b\tau^2 + (a-d)\tau - c = 0,$$

de donde se sigue que τ es algebraico. Luego $\Lambda' \subset K$. □

4. Clases de isomorfismos de curvas elípticas

Sea K un campo cuadrático imaginario y sea $\mathfrak{a}$ un ideal fraccionario. Fijando un encaje $\tau : K \hookrightarrow \mathbb{C}$ tenemos que la imagen de $\mathfrak{a}$ es una latiz en $\mathbb{C}$ pues $\mathfrak{a}$ es un $\mathbb{Z}$-módulo de rango 2 que no está contenido en $\mathbb{R}$. Entonces podemos definir la curva elíptica $E_\mathfrak{a}$ cuyo anillo de endomorfismos es

$$\mathrm{End}(E_\mathfrak{a}) \cong \{\alpha \in \mathbb{C} : \alpha\mathfrak{a} \subset \mathfrak{a}\} = \{\alpha \in K : \alpha\mathfrak{a} \subset \mathfrak{a}\} = O_K.$$

Luego, cada ideal fraccionario de K, distinto de cero, induce una curva elíptica con multiplicación compleja sobre O_K. Por otro lado, sea

$$\mathscr{ELL}(R) = \frac{\left\{ \text{curvas elípticas } E/\mathbb{C} \text{ con } \mathrm{End}(E) \cong R \right\}}{\text{isomorfismos sobre } \mathbb{C}}$$
$$= \frac{\{\text{latices } \Lambda \text{ con } \mathrm{End}(E_\Lambda) \cong R\}}{\text{homotecias}}.$$

Notemos que latices homoteticas inducen curvas elípticas isomorfas. Por ejemplo, $\mathfrak{a}$ y $c\mathfrak{a}$, $c \in \mathbb{C}$, son la misma curva elíptica en $\mathscr{ELL}(R)$. En particular, el mapeo

$$\mathscr{CL}(O_K) \longrightarrow \mathscr{ELL}(O_K)$$
$$\tilde{\mathfrak{a}} \longmapsto E_{\tilde{\mathfrak{a}}},$$

está bien definido. En general, si Λ es cualquier latiz con $E_\Lambda \in \mathscr{ELL}(O_K)$ y $\mathfrak{a}$ es cualquier ideal fraccionario de K podemos definir

$$\mathfrak{a}\Lambda = \{\alpha_1\lambda_1 + \ldots + \alpha_r\lambda_r : \alpha_i \in \mathfrak{a},\ \lambda_i \in \Lambda\}.$$

Teorema 8. *Sea Λ una latiz con $E_\Lambda \in \mathscr{ELL}(O_K)$ y sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales fraccionarios, distintos de cero, de K.*

i) *$\mathfrak{a}\Lambda$ es una latiz en $\mathbb{C}$.*
ii) *$\mathrm{End}(E_{\mathfrak{a}\Lambda}) \cong O_K$.*
iii) *$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ si y sólo si $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$ en $\mathscr{CL}(O_K)$.*
iv) *La acción*

$$\bar{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda},$$

de $\mathscr{CL}(O_K)$ en $\mathscr{ELL}(O_K)$ es simplemente transitiva. En particular

$$|\mathscr{CL}(O_K)| = |\mathscr{ELL}(O_K)|.$$

Demostración. (i)Como $\mathrm{End}(E_\Lambda) = O_K$ se tiene que $O_K\Lambda = \Lambda$. Por teoría de números elemental podemos elegir $d \in \mathbb{Z}$ tal que $d\mathfrak{a} \subset O_K$ ([13] p. 21). Entonces $\mathfrak{a}\Lambda \subset \frac{1}{d}\Lambda$ lo que implica que $\mathfrak{a}\Lambda$ es un subgrupo discreto de $\mathbb{C}$. Similarmente, escogiendo un entero $d \neq 0$ tal que $dO_K \subset \mathfrak{a}$ ([13] p. 12) tenemos que $d\Lambda \subset \mathfrak{a}\Lambda$ lo que implica que $\mathfrak{a}\Lambda$ tiene rango ≥ 2 en $\mathbb{C}$. Por lo que $\mathfrak{a}\Lambda$ es una latiz.

(ii) Para todo $\alpha \in \mathbb{C}$ y todo ideal fraccionario $\mathfrak{a} \neq 0$ tenemos que $\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda$ si y sólo si $\mathfrak{a}^{-1}\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}^{-1}\mathfrak{a}\Lambda$ si y sólo si $\alpha\Lambda \subset \Lambda$. Luego,

$$\mathrm{End}(E_{\mathfrak{a}\Lambda}) = \{\alpha \in \mathbb{C} : \alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda\} = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\} = \mathrm{End}(E_\Lambda) = O_K.$$

(iii) Notemos que $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ si y sólo si existe $c \in \mathbb{C}$ tal que $\mathfrak{a}\Lambda = c\mathfrak{b}\Lambda$ si y sólo si

$$\Lambda = c\mathfrak{a}^{-1}\mathfrak{b}\Lambda.$$

De manera similar $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$ si y sólo si

$$\Lambda = c^{-1}\mathfrak{a}\mathfrak{b}^{-1}\Lambda.$$

Por lo tanto, si $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{b}\Lambda}$, $c\mathfrak{a}^{-1}\mathfrak{b}$ y $c^{-1}\mathfrak{a}\mathfrak{b}^{-1}$ envían a Λ en si misma, lo que implica que ambos están contenidos en O_K luego son iguales a O_K pues $O_K = (c\mathfrak{a}^{-1}\mathfrak{b})(c^{-1}\mathfrak{a}\mathfrak{b}^{-1}) \subset (c\mathfrak{a}^{-1}\mathfrak{b}) \cap (c^{-1}\mathfrak{a}\mathfrak{b}^{-1})$. Entonces $\mathfrak{a} = c\mathfrak{b}$. Luego, $c \in K$ y $\bar{\mathfrak{a}} = \bar{\mathfrak{b}}$.

(iv) Observemos que

$$\bar{\mathfrak{a}} * (\bar{\mathfrak{b}} * E_\Lambda) = \bar{\mathfrak{a}} * E_{\mathfrak{b}^{-1}\Lambda} = E_{\mathfrak{a}^{-1}(\mathfrak{b}^{-1}\Lambda)} = E_{(\mathfrak{a}\mathfrak{b})^{-1}\Lambda} = (\bar{\mathfrak{a}}\bar{\mathfrak{b}}) * E_\Lambda,$$

está bien definido por (iii). Lo cual muestra que $\bar{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$ efectivamente define una acción del grupo de clase de ideales de O_K en $\mathscr{ELL}(O_K)$.

Sean $E_{\Lambda_1}, E_{\Lambda_2} \in \mathscr{ELL}(O_K)$. Para mostrar la transitividad tenemos que encontrar un ideal fraccionario $\mathfrak{a}$ tal que $\bar{\mathfrak{a}} * E_{\Lambda_1} = E_{\Lambda_2}$. Escojamos λ_1 uno de los generadores de Λ_1 y consideremos la latiz $\mathfrak{a}_1 = \frac{1}{\lambda_1}\Lambda_1$ la cual está en K por el lema 1 y es finitamente generada como O_K-módulo. Por lo tanto, $\mathfrak{a}_1$ es un ideal fraccionario de K. Análogamente, eligiendo un generador λ_2 de Λ_2, obtenemos el ideal fraccionario $\mathfrak{a}_2 = \frac{1}{\lambda_2}\Lambda_2 \subset K$. Luego

$$\frac{\lambda_2}{\lambda_1}\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_1 = \lambda_2\mathfrak{a}_2 = \Lambda_2.$$

Si consideramos el ideal fraccionario $\mathfrak{a} = \mathfrak{a}_2^{-1}\mathfrak{a}_1$, tenemos que

$$\bar{\mathfrak{a}} * E_{\Lambda_1} = E_{\mathfrak{a}^{-1}\Lambda_1} = E_{\frac{\lambda_1}{\lambda_2}\Lambda_2} \cong E_{\Lambda_2}.$$

Por ultimo la acción es simplemente transitiva por (ii).

□

Corolario 1. *Sea K un campo cuadrático imaginario*

i) *Existe sólo un número finito de clases de isomorfismo de curvas elípticas $E/\mathbb{C}$ con multiplicación compleja por O_K.*

ii) *Sea $E/\mathbb{C}$ una curva elíptica con multiplicación compleja por O_K. Entonces $j(E) \in \bar{\mathbb{Q}}$.*

iii)
$$\mathscr{E}\mathscr{L}\mathscr{L}(O_K) = \frac{\{\textit{curvas elípticas } E/\bar{\mathbb{Q}} \textit{ con End}(E) \cong O_K\}}{\textit{isomorfismos sobre } \bar{\mathbb{Q}}}.$$

Demostración. La parte (i) se sigue directamente de la finitud del grupo de clase de ideales $\mathscr{C}\mathscr{L}(O_K)$ ([13] p. 36).

(ii) Sean $E/\mathbb{C}$ una curva elíptica, $\sigma \in \mathrm{Aut}(\mathbb{C})$, E^σ la curva elíptica obtenida al hacer actuar σ en los coeficientes de la ecuación de Weierstrass de E y $j(E)$ una combinación racional de esos coeficientes. Luego, es claro que $j(E^\sigma) = j(E)^\sigma$.

Por la misma razón dado un endomorfismo $\phi : E \to E$ este induce un endomorfismo $\phi^\sigma : E^\sigma \to E^\sigma$ donde ϕ^σ significa aplicar σ a todos los coeficiente de las funciones racionales que determinan a ϕ. Luego se sigue que el siguiente diagrama

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E \\ \downarrow & & \downarrow \\ E^\sigma & \xrightarrow{\phi^\sigma} & E^\sigma \end{array}$$

conmuta y por lo tanto $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$.

Como $\mathrm{End}(E^\sigma) \cong O_K$ el teorema 8 implica que E^σ es una de sólo un número finito de clases de curvas elípticas $\mathbb{C}$-isomorfas. Como las clases de curvas elípticas son determinadas por sus j-invariantes, se sigue que $j(E)^\sigma$ sólo toma un número finito de valores al hacer correr σ sobre todos los automorfismos de $\mathbb{C}$ luego se tiene que $\left[\mathbb{Q}(j(E)) : \mathbb{Q}\right]$ es finita por teoría de campos ([29] p. 486) y por lo tanto $j(E)$ es un número algebraico.

(iii) Para todo subcampo F de $\mathbb{C}$ denotemos por $\mathscr{E}\mathscr{L}\mathscr{L}_F(O_K)$ al conjunto

$$\frac{\{\text{ curvas elípticas } E/F \text{ con } \mathrm{End}(E) \cong R\}}{\text{isomorfismos sobre } F}.$$

Si fijamos un encaje $\bar{\mathbb{Q}} \subset \mathbb{C}$, este induce un mapeo natural

$$\epsilon : \mathscr{E}\mathscr{L}\mathscr{L}_{\bar{\mathbb{Q}}}(O_K) \longrightarrow \mathscr{E}\mathscr{L}\mathscr{L}_{\mathbb{C}}(O_K).$$

Sea $E/\mathbb{C}$ el representante de un elemento en $\mathscr{E}\mathscr{L}\mathscr{L}_{\mathbb{C}}(O_K)$. Por (ii), $j(E) \in \bar{\mathbb{Q}}$ luego, por el teorema 4 existe una curva elíptica $E'/\mathbb{Q}(j(E))$ con $j(E') = j(E)$ lo cual implica que E es isomorfa a E' sobre $\mathbb{C}$. Entonces $\epsilon(E') = E$ por lo que ϵ es suprayectiva.

Sea $E_1/\bar{\mathbb{Q}}$ y $E_2/\bar{\mathbb{Q}}$ representantes de dos elementos en $\mathscr{E}\mathscr{L}\mathscr{L}_{\bar{\mathbb{Q}}}(O_K)$ y supongamos que $\epsilon(E_1) = \epsilon(E_2)$. Por el teorema 4 $j(E_1) = j(E_2)$ luego, E_1 y E_2 son isomorfas sobre $\bar{\mathbb{Q}}$. Luego, E_1 y E_2 representan el mismo elemento de $\mathscr{E}\mathscr{L}\mathscr{L}_{\bar{\mathbb{Q}}}(O_K)$ lo cual muestra que ϵ es inyectiva y por lo tanto biyectiva.

□

Nota 1. De hecho se puede demostrar que $j(E)$ es entero algebraico véase [17] y [22].

De ahora en adelante denotaremos por $\mathscr{E}\mathscr{L}\mathscr{L}(O_K)$ al conjunto de clases de curvas elípticas $\bar{\mathbb{Q}}$-isomorfas. Notemos que existe una acción natural de $\mathrm{Gal}(\bar{K}/K)$ en $\mathscr{E}\mathscr{L}\mathscr{L}(O_K)$ definida por la propiedad de que $\sigma \in \mathrm{Gal}(\bar{K}/K)$ envía la clase de E en la clase E^σ. Por otro lado el teorema 8 dice que la acción del grupo de clase $\mathscr{C}\mathscr{L}(O_K)$ en $\mathscr{E}\mathscr{L}\mathscr{L}(O_K)$ es simplemente transitiva. Luego existe un único $\mathfrak{a} \in \mathscr{C}\mathscr{L}(O_K)$, que depende de σ, tal que $\mathfrak{a} * E = E^\sigma$. En otras palabras existe un mapeo bien definido

$$F : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathscr{C}\mathscr{L}(O_K) \tag{5}$$

caracterizado por la propiedad de que

$$E^{\sigma} = F(\sigma) * E$$

para todo $\sigma \in \mathrm{Gal}(\bar{K}/K)$. De hecho, se puede demostrar que F es un homomorfismo de grupos y además es independiente de la elección de $E \in \mathscr{E}\mathscr{L}\mathscr{L}(O_K)$([22] p. 112).

Nota 2. Observemos que la definición de F es esencialmente analítica, pues $F(\sigma)$ depende de como cambia la latiz de una curva elíptica cuando la latiz es multiplicada por un ideal. Luego si denotamos por $j(\Lambda)$ al j-invariante de la curva elíptica E_Λ sabemos que $j(\Lambda)$ es una función analítica de Λ. Entonces, el mapeo F es caracterizado por la fórmula

$$j(\Lambda)^{\sigma} = j(F(\sigma)^{-1}\Lambda).$$

Luego, F convierte la acción algebraica de σ en la acción analítica de multiplicar por $F(\sigma)^{-1}$.

5. Campo de Clase de Hilbert

El objetivo de esta sección es mostrar que el campo de clase de Hilbert de un campo cuadrático imaginario K es generado por el j-invariante de la curva elíptica E tal que $\mathrm{End}(E) \cong O_K$. Para ésto necesitaremos el siguiente lema técnico, cuya demostración puede ser consultada en [22].

Lema 2. *Existe un conjunto finito de primos $S \in \mathbb{Z}$ tal que si $p \notin S$ es un primo que se escinde en K, digamos como $pO_K = \mathfrak{p}\mathfrak{p}'$, entonces*

$$F(\sigma_{\mathfrak{p}}) = \bar{\mathfrak{p}} \in \mathscr{C}\mathscr{L}(O_K).$$

Teorema 9 (Weber-Fueter)**.** *Sea E un representante de una clase en $\mathscr{E}\mathscr{L}\mathscr{L}(O_K)$*

i) *$K(j(E))$ es el campo de clase de Hilbert H de K.*
ii) *$\big[\mathbb{Q}(j(E)) : \mathbb{Q}\big] = \big[K(j(E)) : K\big] = h_K$, donde h_K es el número de clase de K.*
iii) *Sea $E_1, \cdots, E_h$ un conjunto completo de representantes de $\mathscr{E}\mathscr{L}\mathscr{L}(O_K)$. Entonces $j(E_1), \cdots, j(E_h)$ es un conjunto completo de $\mathrm{Gal}(\bar{K}/K)$-conjugados de $j(E)$.*
iv) *Para todo ideal primo $\mathfrak{p}$ de K*

$$j(E)^{\sigma_{\mathfrak{p}}} = j(\bar{\mathfrak{p}} * E).$$

De manera más general, para cada ideal fraccionario $\mathfrak{a}$, distinto de cero, de K

$$j(E)^{(\mathfrak{a}, H/K)} = j(\bar{\mathfrak{a}} * E).$$

Demostración. (i) Sea L/K la extensión finita correspondiente al homomorfismo (5), donde L es el campo fijado por el núcleo de F. Entonces

$$\begin{aligned}
\mathrm{Gal}(\bar{K}/L) &= \ker F \\
&= \big\{\sigma \in \mathrm{Gal}(\bar{K}/K) : F(\sigma) = 1\big\} \\
&= \big\{\sigma \in \mathrm{Gal}(\bar{K}/K) : F(\sigma) * E = E\big\} \\
&= \big\{\sigma \in \mathrm{Gal}(\bar{K}/K) : E^{\sigma} = E\big\} \\
&= \big\{\sigma \in \mathrm{Gal}(\bar{K}/K) : j(E^{\sigma}) = j(E)\big\} \\
&= \mathrm{Gal}(\bar{K}/K(j(E))).
\end{aligned}$$

Por lo tanto $L = K(j(E))$([6] p. 262). Además, de teoría básica de Galois F induce un isomorfismo $\tilde{F} : (L/K) \to \mathscr{C}\mathscr{L}(O_K)$, por lo tanto L/K es una extensión abeliana.

Ahora, demostraremos que $L = H$. Sea $\mathfrak{c}_{L/K}$ el conductor de L/K, y consideremos la composición del mapeo de Artin con $\tilde{F}$,

$$I(\mathfrak{c}_{L/K}) \overset{(\cdot, L/K)}{\to} \mathrm{Gal}(L/K) \overset{\tilde{F}}{\to} \mathscr{C}\mathscr{L}(O_K).$$

Veamos que esta composición es justo la proyección natural de $I(\mathfrak{c}_{L/K})$ en $\mathscr{CL}(O_K)$. En otras palabras queremos ver que

$$\tilde{F}((\mathfrak{a}, L/K)) = \bar{\mathfrak{a}}, \tag{6}$$

para toda $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$. Sea $\mathfrak{a} \in I(\mathfrak{c}_{L/K})$ y sea S un conjunto finito de primos como los descritos en el lema 2. Del teorema de Dirichlet (teorema 3) existe un primo con grado de inercia igual a 1, $\mathfrak{p} \in I(\mathfrak{c}_{L/K})$, en la misma $P(\mathfrak{c}_{L/K})$-clase de ideales que $\mathfrak{a}$ y no divide a ningún primo de S. Ya que $\bar{\mathfrak{a}} = \bar{\mathfrak{p}}$ existe un $\alpha \in K^*$ que satisface

$$\alpha \equiv 1 (\text{mod } \mathfrak{c}_{L/K}) \quad \text{y} \quad \mathfrak{a} = (\alpha)\mathfrak{p},$$

de donde se sigue que

$$\tilde{F}((\mathfrak{a}, L/K)) = \tilde{F}(((\alpha)\mathfrak{p}, L/K)) = \tilde{F}((\mathfrak{p}, L/K)).$$

Dado que $N_{\mathbb{Q}}^{K}\mathfrak{p} \notin S$ del lema 2 tenemos que

$$\tilde{F}((\mathfrak{p}, L/K)) = \bar{\mathfrak{p}} = \bar{\mathfrak{a}}.$$

Notemos que de (6) se tiene que $\tilde{F}(((\alpha), L/K)) = 1$ para todo ideal principal $(\alpha) \in I(\mathfrak{c}_{L/K})$, y no sólo para los que son congruentes con 1 módulo $\mathfrak{c}_{L/K}$. Por otro lado sabemos que el mapeo $\tilde{F}$:Gal$(L/K) \to \mathscr{CL}(O_K)$ es un isomorfismo, lo cual implica que $((\alpha), L/K) = 1$ para toda $(\alpha) \in I(\mathfrak{c}_{L/K})$. Pero el conductor $\mathfrak{c}$ de L/K es el ideal entero más grande con la propiedad de que $\alpha \equiv 1 (\text{mod } \mathfrak{c})$ entonces $((\alpha), L/K) = 1$. Luego, se sigue que $\mathfrak{c}_{L/K} = (1)$.

Finalmente, del teorema 1 sabemos que todos los primos ramificados dividen al conductor, luego L/K es no ramificada. Por lo tanto L está contenido en el campo de clase de Hilbert H de K.

Por otro lado, como $\tilde{F}$:Gal$(L/K) \to \mathscr{CL}(O_K)$ es isomorfismo

$$[L : K] = |\text{Gal}(L/K)| = |\mathscr{CL}(O_K)| = |\text{Gal}(H/K)| = [H : K]. \tag{7}$$

Esto combinado con la inclusión $L \subset H$ muestra que $K(j(E)) = L = H$.

(ii) La segunda igualdad se sigue de (7). Por otro lado, de la prueba del corolario $1(ii)$ y del teorema $8(iv)$ tenemos que si End$(E) \cong O_K$,

$$\left[\mathbb{Q}(j(E)) : \mathbb{Q}\right] \leq h_K.$$

Usando que $\left[K(j(E)) : K\right] = h_K$ y que $[K : \mathbb{Q}] = 2$ tenemos que $\left[\mathbb{Q}(j(E)) : \mathbb{Q}\right] = h_K$.

(iii) Del teorema 8 sabemos que $\mathscr{CL}(O_K)$ actúa transitivamente en el conjunto de j-invariantes

$$\mathscr{J} = \left\{j(E_1), \cdots, j(E_h)\right\},$$

pues el conjunto $\mathscr{ECL}(O_K)$ puede ser identificado con los j-invariantes de sus elementos. El mapeo F : Gal$(\bar{K}/K) \to \mathscr{CL}(O_K)$ es definido por identificar la acción de Gal$(\bar{K}/K)$ en $\mathscr{J}$ con la acción de $\mathscr{CL}(O_K)$ en $\mathscr{J}$. Luego, Gal$(\bar{K}/K)$ también actúa transitivamente en $\mathscr{J}$. Por lo tanto $\mathscr{J}$ es un conjunto completo de Gal$(\bar{K}/K)$-conjugados de $j(E)$.

Por ultimo observemos que (iv) se sigue de (6) para todo ideal en $I(\mathfrak{c}_{L/K})$, pues como $\mathfrak{c}_{L/K} = (1)$ entonces, $I(\mathfrak{c}_{L/K})$ es el conjunto de todos los ideales fraccionarios de K distintos de 0. □

6. Extensiones abelianas de $\mathbb{Q}$

Antes de continuar con la descripción de las extensiones abelianas de un campo cuadrático imaginario K recordemos de manera breve e intuitiva el caso análogo de extensiones ciclotómicas para $\mathbb{Q}$ [5], [13]. En este caso remplazamos la curva elíptica $E(\mathbb{C})$ por el grupo multiplicativo $\mathbb{G}_m(\mathbb{C}) = \mathbb{C}^*$. Sea

$$\varphi_N : \mathbb{G}_m(\mathbb{C}^*) \to \mathbb{G}_m(\mathbb{C}^*),$$

dada por $z \mapsto z^N$. Definimos $\mu_N = \ker\varphi_N$, el grupo de N-puntos de torsión de $\mathbb{G}_m$, que corresponde al grupo de N-raíces de la unidad. Como es bien sabido la extensión $\mathbb{Q}(\mu_N)/\mathbb{Q}$ es una extensión abeliana que sólo se ramifica en los primos que dividen a N. Sean p un primo que no divide a N, ζ un generador de μ_N, $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ el elemento de Frobenius asociado a p y $\mathfrak{P}$ un primo en $\mathbb{Q}(\zeta)$ tal que $\mathfrak{P}|p$. Por la definición de $\sigma_{\mathfrak{p}}$ tenemos que

$$\zeta^{\sigma_p} \equiv \zeta^p \pmod{\mathfrak{P}}.$$

Pero $1, \zeta, \zeta^2, \cdots, \zeta^{N-1}$ son distintos módulo $\mathfrak{P}$ pues por hipótesis $\mathfrak{P}$ no divide a N lo cual implica que $X^{N-1} - 1$ es separable en característica p. Usando ésto se puede probar que la congruencia es una igualdad

$$\zeta^{\sigma_p} = \zeta^p,$$

y luego concluir que $\sigma_p = 1$ si y sólo si $p \equiv 1 \pmod{N}$. Por lo tanto $\mathbb{Q}(\zeta) = \mathbb{Q}(\mu_N)$ es el campo de clase de rayos de $\mathbb{Q}$ de conductor N.

Sea $L/\mathbb{Q}$ una extensión abeliana y N el conductor de L. Por la definición del campo de clase de rayos y la teoría de campos de clase (teorema $2(iii)$), L está contenido en el campo de clase de rayos de conductor N. Luego, tenemos el siguiente teorema.

Teorema 10 (Kronecker-Weber)**.** *Toda extensión abeliana de $\mathbb{Q}$ está contenida en una extensión ciclotómica. i.e. dada una extensión abeliana finita $L/\mathbb{Q}$, existe una raíz de la unidad ζ tal que $L \subset \mathbb{Q}(\zeta)$.*

Nota 3. Notemos que el campo de clase de rayos de $\mathbb{Q}$ de conductor N *es generado por los valores de la función analítica*

$$e^{2\pi i z} = \sum_{n \geq 0} \frac{(2\pi i z)^n}{n!},$$

evaluada en los puntos de orden N del grupo circular $\mathbb{R}/\mathbb{Z}$. *i.e.* el campo de clase de rayos de $\mathbb{Q}$ es generado por elementos de la forma $e^{2\pi i a/N}$ con $a, N \in \mathbb{Z}$. Además, la acción del elemento de Frobenius σ_p en los valores $e^{2\pi i a/N}$ es dada explícitamente por la fórmula

$$(e^{2\pi i a/N})^{\sigma_p} = e^{2\pi i a p/N},$$

para todo p que no divide a N. Luego, la acción de Galois de σ_p es trasformada en la acción de multiplicar en el grupo circular.

7. Extensiones abelianas de K

El objetivo principal de esta sección es demostrar que los puntos de torsión de una curva elíptica con multiplicación compleja por O_K pueden ser usados para generar las extensiones abelianas de K, como los puntos de orden finito del grupo circular nos sirvieron para generar las extensiones abelianas de $\mathbb{Q}$.

Definición 4. Sea E/H una curva elíptica donde H es el campo de clase de Hilbert de K. Definimos la *función de Weber* para E/H como el mapeo

$$h : E \to E/\mathrm{Aut}(E),$$

Si consideramos la ecuación de Weierstrass de E, $y^2 = x^3 + Ax + B$, con $A, B \in H$ se tiene que la función de Weber para E/H está dada por el mapeo

$$h(P) = h(x,y) = \begin{cases} x & \text{si } AB \neq 0, \\ x^2 & \text{si } B = 0, \\ x^3 & \text{si } A = 0. \end{cases}$$

En esencia, salvo para los caso excepcionales en que $j = 0$ o $j = 1728$ la función de Weber es justo la coordenada x de la curva. Ahora usaremos los valores de la función de Weber en los puntos de torsión para generar las extensiones abelianas de K. Antes de proceder a demostrar este hecho enunciaremos un lema técnico cuya demostración puede ser consultada en ([22] p. 133).

Lema 3. *Sean K un campo cuadrático imaginario, H el campo de clase de Hilbert de K y E/H una curva elíptica con multiplicación compleja por O_K. Para todos salvo un número finito de primos $\mathfrak{p}$ de K con grado de inercia igual a 1 que satisfacen*

$$(\mathfrak{p}, H/K) = 1,$$

existe un único $\pi = \pi_{\mathfrak{p}} \in O_K$ tal que $\mathfrak{p} = \pi O_K$ y el siguiente diagrama

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\phi} & \tilde{E} \end{array}$$

conmuta, donde ϕ es la p-ésima potencia de Frobenius y $\tilde{E}$ es la reducción de E módulo $\mathfrak{p}$. Luego, la condición $(\mathfrak{p}, H/K) = 1$, es equivalente a que $\mathfrak{p}$ sea principal.

Teorema 11. *Sean K un campo cuadrático imaginario, E una curva elíptica con multiplicación compleja por O_K y $h : E \to \mathbb{P}^1$ la función de Weber de E/H descrita como antes. Sea $\mathfrak{c}$ un ideal entero de O_K, entonces el campo*

$$K(j(E), h(E[\mathfrak{c}])),$$

es el campo de clase de rayos de K módulo $\mathfrak{c}$.

Demostración. Sea $L = K(j(E), h(E[\mathfrak{c}]))$, por el teorema de Weber-Fueter (teorema 9), L contiene al campo de clase de Hilbert. Con el fin de probar que L es el campo de clase de rayos de K módulo $\mathfrak{c}$, por el teorema $2(i\,v)$ y el teorema 1, necesitamos probar que $(\mathfrak{p}, L/K) = 1$ si y sólo si $\mathfrak{p} \in P(\mathfrak{c})$ para todos salvo un número finito de primos con grado de inercia igual a 1 en K.

Primeramente, supongamos que $\mathfrak{p}$ es un primo de grado 1 de K tal que $\mathfrak{p} \in P(\mathfrak{c})$. Esto significa que $\mathfrak{p} = \mu O_K$ para algún $\mu \in O_K$ tal que $\mu \equiv 1 (\bmod \mathfrak{c})$. En particular, $\mathfrak{p}$ es principal y por lo tanto $(\mathfrak{p}, H/K) = 1$. Luego podemos aplicar el lema 3, después de excluir un número finito de primos $\mathfrak{p}$, para obtener un $\pi \in O_K$ tal que $\mathfrak{p} = \pi O_K$ y el siguiente diagrama

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \xrightarrow{\phi} & \tilde{E} \end{array}$$

conmuta. Como $\pi O_K = \mathfrak{p} = \mu O_K$ existe una unidad $\xi \in O_K^*$ tal que $\pi = \xi\mu$. Notemos que $[\xi] \in \mathrm{Aut}(E)$ luego, $\left[\mu\right]$ y $[\pi]$ difieren por un automorfismo de E.

Sabemos que $(\mathfrak{p}, L/K)$ fija a $H = K(j(E))$, luego con el fin de probar que fija a a todo L, tenemos que mostrar que fija a $h(E[\mathfrak{c}])$. Sea $T \in E[\mathfrak{c}]$ cualquier punto de $\mathfrak{c}$-torsión. De la conmutatividad del diagrama tenemos que

$$\widetilde{T^{(\mathfrak{p},L/K)}} = \phi(\tilde{T}) = \widetilde{[\pi]\,T}.$$

Por otro lado, excluyendo los primos $\mathfrak{p}$ que dividen a $|E[\mathfrak{c}]|$ y aplicando el teorema 6 tenemos que $T^{(\mathfrak{p},L/K)} = [\pi]\,T$.

Ahora, usando que $(\mathfrak{p}, H/K) = 1$ y h está definido sobre H tenemos que

$$h(T)^{(\mathfrak{p},L/K)} = h(T^{(\mathfrak{p},L/K)}) = h([\pi]\,T) = h([\xi] \circ \left[\mu\right]\,T).$$

Como h es invariante bajo $\mathrm{Aut}(E)$ y $[\xi] \in \mathrm{Aut}E$ tenemos que

$$h([\xi] \circ \left[\mu\right]\,T) = h(\left[\mu\right]\,T) = h(T).$$

La ultima igualdad se sigue del hecho de que $T \in E[\mathfrak{c}]$ y $\mu \equiv 1 \pmod{\mathfrak{c}}$. Esto prueba que si $\mathfrak{p} \in P(\mathfrak{c})$ entonces $(\mathfrak{p}, L/K) = 1$.

Con el fin de probar el regreso, consideremos un primo $\mathfrak{p}$ con grado de inercia igual a 1 que satisface la igualdad $(\mathfrak{p}, L/K) = 1$. Entonces

$$(\mathfrak{p}, H/K) = (\mathfrak{p}, L/K)|_H = 1.$$

Excluyendo un número finito de primos podemos aplicar el lema 3 para dar un $\pi \in O_K$ tal que $\mathfrak{p} = \pi O_K$ y el diagrama

$$\begin{array}{ccc} E & \stackrel{[\pi]}{\to} & E \\ \downarrow & & \downarrow \\ \tilde{E} & \stackrel{\phi}{\to} & \tilde{E} \end{array}$$

conmuta. Además, podemos elegir algún $\sigma \in \mathrm{Gal}(\bar{K}/K)$ cuya restricción a K^{ab} es $(\mathfrak{p}, K^{ab}/K)$. En particular, $\sigma|_L = (\mathfrak{p}, L/K) = 1$, luego $\sigma|_H = 1$ pues $H \subset L$. Sea $T \in E[\mathfrak{c}]$ un punto de $\mathfrak{c}$-torsión. Usando la conmutatividad del diagrama y que σ se reduce a la p-ésima potencia de Frobenius tenemos que

$$\tilde{h}(\widetilde{[\pi]}\,\tilde{T}) = \tilde{h}(\widetilde{[\pi]\,T}) = \tilde{h}(\phi(\tilde{T})) = \tilde{h}(\widetilde{T^{\sigma}}) = \widetilde{h(T^{\sigma})}.$$

Como $\sigma|_H = 1 = \sigma|_L$, $h(T) \in L$ y h está definida sobre H se tiene que

$$\widetilde{h(T^{\sigma})} = \widetilde{h(T)^{\sigma}} = \widetilde{h(T)} = \tilde{h}(\tilde{T}).$$

Ahora, observemos que la reducción de h módulo $\mathfrak{P}$ es el mapeo

$$\tilde{h} : \tilde{E} \longrightarrow \widetilde{E/\mathrm{Aut}(E)} \cong \tilde{E}/\widetilde{\mathrm{Aut}(E)}.$$

De la anterior reducción y de la igualdad $\tilde{h}(\widetilde{[\pi]}\,\tilde{T}) = \tilde{h}(\tilde{T})$ se sigue que existe $[\xi] \in \mathrm{Aut}(E)$ tal que $\widetilde{[\pi]}\,\tilde{T} = \widetilde{[\xi]}\,\tilde{T}$. Por otra parte excluyendo un número finito de primos y usando el teorema 6 tenemos que $[\pi - \xi]\,T = O$.

A priori, el elemento particular ξ para el cual $[\pi - \xi]\,T = O$ podría depender de T. Pero como $E[\mathfrak{c}]$ es un $O_K/\mathfrak{c}$-módulo libre de rango 1, existe único $\xi \in O_K^*$ tal que $[\pi - \xi]$ anula a todo $E[\mathfrak{c}]$, lo cual implica que $\pi \equiv \xi \pmod{\mathfrak{c}}$. Luego,

$$\xi^{-1}\pi \equiv 1 \pmod{\mathfrak{c}},$$

implica que $\mathfrak{p} = \pi O_K = (\xi^{-1}\pi)O_K$ pues ξ es unidad. Esto prueba que $\mathfrak{p} \in P(\mathfrak{c})$, lo cual concluye la demostración.

□

Corolario 2. *Con la notación del teorema anterior*

$$K^{ab} = K(j(E), h(E_{tors})).$$

Demostración. Sea L/K una extensión abeliana finita y sea $\mathfrak{c}_{L/K}$ el conductor de L/K. Por la teoría de campos de clase (teorema 2), L está contenido en el campo de clase de rayos de K módulo $\mathfrak{c}_{L/K}$. Por el teorema 11

$$L \subset K(j(E), h(E[\mathfrak{c}_{L/K}])).$$

Tomando el compositum sobre todos los conductores dados $L \subset (j(E), h(E_{tors}))$, y luego la unión sobre todas las L's tenemos que $K^{ab} \subset K(j(E), h(E_{tors}))$. Pero el teorema 11 dice que $K(j(E), h(E_{tors}))$ es un compositum de extensiones abelianas, luego es abeliana y por lo tanto igual a K^{ab}. □

En particular, si $j(E) \neq 0, 1728$ y si tomamos una ecuación para E con coeficientes en el campo de clase de Hilbert de K, la extensión abeliana maximal de K es generada por las coordenadas x de los puntos de torsión.

8. Algunas generalizaciones

Como vimos en la sección 6, para el campo de los números racionales, el teorema de Kronecker-Weber nos proporciona una descripción explícita de todas las extensiones abelianas de $\mathbb{Q}$ con ayuda de la acción del grupo de Galois en las raíces de la unidad, la cual puede ser vista como ciertos valores de la función exponencial.

Vimos también (sección 7) que existe una teoría análoga para los campos cuadráticos imaginarios K cuyas extensiones son construidas con ayuda de la acción de $\mathrm{Gal}(\bar{K}/K)$ en los puntos de orden finito de una curva elíptica con multiplicación compleja.

8.1. **Variedades abelinas.** Algunos progresos han sido hechos en la solución del problema doce de Hilbert para los llamados CM-campos (campos con multiplicación compleja). Se dice que un campo F es *totalmente real* si es generado por las raíces de un polinomio, el cual se factoriza como producto de factores lineales sobre $\mathbb{R}$. Un *CM-campo* es una extensión cuadrática totalmente imaginaria $K = F(\sqrt{-a})$ de un campo totalmente real F donde $a \in F$ es totalmente positivo, es decir es positivo en cada encaje real de F. Esta teoría de multiplicación compleja multidimensional se basa en el estudio de variedades abelianas con multiplicación compleja por elementos de K (ver [4], [17], [18], [19], [20]).

Para un campo cuadrático real K una descripción de ciertas extensiones abelianas de este, es dada por la teoría de "multiplicación real de Shimura" (ver [18]). Sin embargo, en estos caso la situación es menos satisfactoria que el en caso de $\mathbb{Q}$ o de un campo cuadrático imaginario K, pues estas construcciones no generan todas las extensiones abelianas del campo base.

Una situación completamente diferente ocurre para el caso de campos de funciones cuando K es una extensión finita y separable de $\mathbb{F}_q(X)$. Aquí, existe una descripción completa de todas las extensiones abelianas de K en términos de los módulos elípticos de Drinfeld y de las funciones elípticas en característica positiva asociadas a éstos módulos [1].

La idea de describir las extensiones de K vía la acción de $\mathrm{Gal}(\bar{K}/K)$ en ciertos grupos y otros objetos algebraicos ha sido muy fructífera. Muchos ejemplos de construcciones de extensiones abelianas y no abelianas de un campo K son basadas en ésta idea. Una completa clasificación de estas extensiones en términos de representaciones de Galois

y ciertos objetos de Análisis y Geometría Algebraica (formas automorfas y motivos) son una importante meta a largo plazo del famoso Programa de Langlands [9].

8.2. **Conjeturas de Stark.** Un enfoque completamente distinto es el propuesto por H.M. Stark en [23], [24], [25], [26]. En dichos artículos, Stark desarrolla una serie de conjeturas que relacionan los valores de funciones L de Artin en $s = 0$ y $s = 1$ con ciertas cantidades algebraicas asociadas a extensiones de campos numéricos. El uso de éstas conjeturas proporciona generadores explícitos de campos de clase de rayos y por lo tanto resuelve el problema doce de Hilbert. A continuación presentamos un esbozo de ésta teoría la cual es desarrollada a detalle en [15] y [28].

Consideremos L/K una extensión abeliana de un campo numérico y S un conjunto finito de lugares de K que contiene a los lugares infinitos y los lugares finitos que se ramifican en L/K. Para cada elemento $\sigma \in \text{Gal}(L/K)$ definimos la *función zeta parcial* $\zeta_S(s,\sigma)$ por la serie de Dirichlet

$$\zeta_S(s,\sigma) = \sum_{(\mathfrak{a},S)=1,(\mathfrak{a},L/K)=\sigma} N\mathfrak{a}^{-s},$$

para $s \in \mathbb{C}$ tal que $\text{Re}s > 1$, donde $\mathfrak{a}$ corre sobre todos los ideales enteros de K que no son divisibles por los ideales primos contenidos en S y tales que el símbolo de Artin coincide con σ.

A un caracter χ sobre $\text{Gal}(L/K)$ podemos asociarle la función L de Artin dada por el producto de Euler

$$L_S(s,\chi) = \prod_{\mathfrak{p}\notin S} (1 - \chi(\sigma_\mathfrak{p}) N\mathfrak{p}^{-s})^{-1},$$

para $s \in \mathbb{C}$ tal que $\text{Re}s > 1$, donde $\mathfrak{p}$ corre sobre todos los ideales primos de K que no están contenidos en S. Estas funciones se pueden extender meromorficamente a todo el plano complejo y se tiene las siguientes relaciones entre ellas

$$\zeta_S(s,\sigma) = \frac{1}{[L:K]} \sum_{\chi\in\hat{G}} L_S(s,\chi)\bar{\chi}(\sigma), \quad L_S(s,\chi) = \sum_{\sigma\in Gal(L/K)} \zeta_S(s,\sigma)\chi(\sigma),$$

donde $\hat{G}$ denota el grupo de caracteres de $\text{Gal}(L/K)$.

Sea χ un caracter de $\text{Gal}(L/K)$. Si $\chi = 1$ el caracter trivial, definimos $r(1) = |S| - 1$, en otro caso, $r(\chi)$ es el número de lugares $v \in S$ tales que el grupo de descomposición G_v de v en L/K está contenido en el núcleo de χ, *i.e.* los lugares tales que $\chi|_{G_v} = 1$. Una demostración del siguiente resultado puede consultarse en [11] o [28].

Proposición 1. *El orden (grado) de anulación de la función L de Artin $L_S(s,\chi)$, en $s = 0$, es igual a $r(\chi)$.*

Supongamos que existe un lugar infinito v el cual se escinde completamente en L/K y fijemos w un lugar de L que divide a v. Supongamos también, que $|S| \geq 2$. De la proposición 1 tenemos que para todo χ $L_S(0,\chi) = 0$, luego las funciones zeta parciales ζ_S son todos cero en $s = 0$.

Definición 5. Sea L/K una extensión abeliana de un campo numérico y S un conjunto finito de lugares de K que contiene a los lugares infinitos y los lugares finitos que se ramifican en L/K. Diremos que $\epsilon \in K^*$ es una $S-unidad$ si es unidad en todos los primos $\mathfrak{p} \notin S$, $\mathfrak{p} \nmid \infty$ y es positiva para todos los lugares infinitos reales.

Conjetura 1 (Stark)**.** *Sea m el número de raíces de la unidad contenidas en L. Entonces existe una S-unidad $\epsilon = \epsilon(L/K,S,w) \in L$ tal que para toda $\sigma \in$Gal(L/K)*

$$\log|\sigma(\epsilon)|_w = -m\zeta'_S(0,\sigma),$$

o equivalentemente

$$L'_S(0,\chi) = -\frac{1}{m}\sum_{\sigma\in Gal(L/K)}\chi(\sigma)\log|\sigma(\epsilon)|_w\,,$$

para todo caracter χ de $Gal(L/K)$. Además, $L(\sqrt[m]{\epsilon})/K$ es una extensión abeliana y si $|S|\geq 3$, ϵ es una unidad.

Sea K un campo totalmente real distinto de $\mathbb{Q}$, v un lugar fijo de K e identificaremos K con su imagen $v(K)$ en $\mathbb{R}$. Sea $\epsilon(L/K,S,w)$ la unidad ϵ que aparece en la conjetura anterior. Notemos que estamos haciendo un abuso de notación pues $\epsilon(L/K,S,w)$ puede no ser única, sin embargo, bajo el supuesto de que w es un lugar real podemos hacer a ésta unidad única suponiendo que $w(\epsilon(L/K,S,w))>0$. Además, cuando S es elegido minimal[3], podemos simplificar $\epsilon(L/K,S,w)$ como $\epsilon(L/K,w)$.

De ahora en adelante supondremos que la conjetura 1 es verdadera para todas las extensiones abelianas finitas N/K en las cuales v se escinde completamente y cualquier elección del lugar w de N divide a v.

Sea K^{Stark} el subcampo de $\mathbb{C}$ generado sobre K por todas las unidades $\epsilon(N/K,w)$, donde N/K corre sobre todas las extensiones abelianas finitas de K en las cuales v se escinde completamente y w corre sobre todos los lugares infinitos de N que dividen a v. Para todo ideal primo $\mathfrak{p}$ de K definimos el entero $r_\mathfrak{p}$ como $r_\mathfrak{p}=2$ si $\mathfrak{p}$ no divide a 2 y $r_\mathfrak{p}=n_\mathfrak{p}+2$ en otro caso, donde $n_\mathfrak{p}=\left[K_\mathfrak{p}:\mathbb{Q}_2\right]$. Luego, tenemos el siguiente resultado.

Proposición 2. *Sean L/K una extensión abeliana finita de un campo totalmente real, v un lugar infinito de K y T un conjunto finito de ideales primos de K tales que para cada primo $\mathfrak{p}$ en T, el 2-rango del grupo de descomposición $G_\mathfrak{p}$ de $\mathfrak{p}$ en L/K es estrictamente menor que $r_\mathfrak{p}$. Entonces existe una extensión cuadrática N/L tal que*

i) *La extensión N/K es abeliana,*
ii) *Todos los lugares infinitos en K, salvo v, se vuelven complejos en N y*
iii) *Los ideales primos de L que dividen a los de T no se escinden en N/L.*

Bosquejo de la demostración. Sean $\mathfrak{p}$ un ideal primo en T y fijemos un ideal primo $\mathfrak{P}$ en L que divide a $\mathfrak{p}$ y $s_\mathfrak{p}$ denota el 2-rango del grupo de descomposición de $\mathfrak{p}$ en L/K. Por teoría de Galois tenemos que el número de extensiones cuadráticas de $K_\mathfrak{p}$ contenidas en $L_\mathfrak{P}$ es $2^{s_\mathfrak{p}}-1$. Por otro lado de la teoría de Kummer tenemos que el número de extensiones cuadráticas de $K_\mathfrak{p}$ es $2^{r_\mathfrak{p}}-1$. Como $s_\mathfrak{p}<r_\mathfrak{p}$, existe al menos una extensión cuadrática $E_\mathfrak{p}/K_\mathfrak{p}$, tal que $E_\mathfrak{p}$ no está contenida en $L_\mathfrak{P}$. Luego, existe un entero $\mathfrak{p}$-ádico $x_\mathfrak{p}$ en $K_\mathfrak{p}$ tal que $E_\mathfrak{p}=K_\mathfrak{p}(\sqrt{x_\mathfrak{p}})$. En particular, $x_\mathfrak{p}$ no es un cuadrado en $L_\mathfrak{P}$. Para cada ideal primo $\mathfrak{p}\in T$, escojamos un entero $\mathfrak{p}$-ádico $x_\mathfrak{p}$ y definimos

$$m_\mathfrak{p}=v_\mathfrak{P}(x_\mathfrak{p})+v_\mathfrak{P}(2)+1,$$

donde $v_\mathfrak{P}$ denota la valuación asociada a $\mathfrak{P}$. Note que $m_\mathfrak{p}$ no depende de la elección de $\mathfrak{P}$ pues $x_\mathfrak{p}$ es un elemento de $K_\mathfrak{p}$. Por el teorema de aproximación, existe un entero algebraico x en K tal que, $v(x)>0$, $v'(x)<0$ para todo lugar infinito v' de K distinto de v y $x\equiv x_\mathfrak{p}\,(\mathrm{mod}\,\mathfrak{p}^{m_\mathfrak{p}})$ para todo ideal primo $\mathfrak{p}\in T$. Ahora, veremos que $N=L(\sqrt{x})$ satisface las propiedades $(i)-(iii)$. Primero, es claro que N/K es abeliana ya que es el compositum de dos extensiones abelianas, a saber L/K y $K(\sqrt{x})/K$, por lo que la propiedad (i) se cumple. Como $\sqrt{v'(x)}$ es un número complejo para $v'\neq v$ mientras que $\sqrt{v(x)}$ es real

[3]Si S es minimal, S es el conjunto de todos los lugares infinitos de K con los lugares finitos ramificados en L/K.

de tiene que v es el único lugar infinito de K que sigue siendo real en N/K de donde tenemos que (iii) es satisfecha.

Finalmente, sea $\mathfrak{p}$ un ideal primo en T y supongamos que $\mathfrak{p}$ se escinde en N/L y sean $\mathfrak{P}$ y $\tilde{\mathfrak{P}}$ ideales primos de L y N, respectivamente, tales que dividen a $\mathfrak{p}$ y $\tilde{\mathfrak{P}}|\mathfrak{P}$. Entonces, los campos locales $N_{\tilde{\mathfrak{P}}}$ y $L_{\mathfrak{P}}$ son el mismo, luego x es un cuadrado en $L_{\mathfrak{P}}$. Ahora, considerando el polinomio $X^2 - x_{\mathfrak{p}} \in L_{\mathfrak{P}}[X]$ el cual tiene una raíz simple $\sqrt{x}$ módulo $\mathfrak{P}^{m_{\mathfrak{p}}}$. Por el lema de Hensel, este polinomio tiene una raíz en $L_{\mathfrak{P}}$. Pero ésto es una contradicción, pues $x_{\mathfrak{p}}$ no es un cuadrado en $L_{\mathfrak{P}}$ por lo tanto, $\mathfrak{p}$ no puede escindirse en N/L. Luego, se cumple (iii). ■

El siguiente teorema es una consecuencia de la conjetura 1 y su demostración puede consultarse en [25].

Teorema 12 (Stark)**.** *Sea* Γ *el grupo cociente*

$$\mathrm{Gal}(N/K)/\{1,\tau\},$$

tal que Γ *es el grupo de Galois de* L/K*. Supongamos que para todo caracter* ψ *de* $\mathrm{Gal}(N/K)$ *no inducido por un caracter de* Γ *se tiene que* $L'(0,\psi) \neq 0$*. Entonces,* $N = \mathbb{Q}(\epsilon)$ *y* $L = \mathbb{Q}(\epsilon^{-1} + \epsilon)$.

Una consecuencia de los teoremas anteriores es el siguiente resultado sobre extensiones abelianas reales de un campo numérico K.

Teorema 13. *La extensión abeliana maximal real de K está contenida en* K^{Stark}*. Equivalentemente, para toda extensión abeliana finita real existen unidades de Stark* $\epsilon_1, \cdots, \epsilon_r$ *tales que* $L \subset K(\epsilon_1, \cdots, \epsilon_r)$.

Bosquejo de la demostración. Supongamos que L/K es una extensión cíclica. Queremos construir una extensión cuadrática N/L que satisface las condiciones $(i) - (iii)$ de la proposición 2 y tal que pocas derivadas de las funciones L asociadas a estas extensiones se anulen en $s = 0$, pues de lo contrario, la conjetura 1 no seria útil. De la definición de $r(\chi)$ tenemos, que una manera de evitar ésto, es asegurarse de que ningún ideal primo en S se escinda en N/L.

Eligiendo S minimal, los ideales primos en S son exactamente los ideales primos que se ramifican en N/K. Sea $\mathfrak{p}$ uno de tales ideales primos. Si $\mathfrak{p}$ no se ramifica en L/K, $\mathfrak{p}$ se tiene que ramificar en N/L y por lo tanto no se escinde. Si $\mathfrak{p}$ es ramificado en L/K, queremos asegurarnos que $\mathfrak{p}$ no se va a escindir en N/L, por lo que consideramos a $\mathfrak{p}$ en T donde T es elegido como el conjunto de ideales primos de K que son ramificados en L/K. Para cada ideal primo $\mathfrak{p}$ en T, el 2-rango del grupo de descomposición en L/K es 1, luego podemos aplicar la proposición 2 y obtener una extensión cuadrática N/L que satisface las condiciones $(i) - (iii)$.

Fijemos un lugar infinito w en N que divide a v. Sea $\epsilon = \epsilon(N/K, w)$, τ el único automorfimos no trivial de la extensión cuadrática N/L y $\mathfrak{p}$ un ideal primo en S. Como $\mathfrak{p}$ no se escinde en N/L, $G_{\mathfrak{p}}$ contiene a τ. En particular, si χ es un caracter de $\mathrm{Gal}(N/K)$ tal que $\chi(\tau) \neq 1$ se tiene que $r(\chi) = 1$ y por la proposición 1, $L'_S(0,\chi) \neq 0$. Finalmente, aplicando el teorema 12 tenemos lo deseado.

Si L/K no es cíclico podemos descomponer a L/K como el compositum de extensiones cíclicas $L_1/K, \cdots, L_r/K$ y aplicar a cada una de ellas la construcción anterior para obtener extensiones cuadráticas N_i/L_i y lugares infinitos w_i tales que $\epsilon_i = \epsilon(N_i/K, w_i)$ satisfacen que $L_i = K(e_i + e_i^{-1})$. Luego hemos concluido la prueba, pues L es generado sobre K por elementos de la forma $\epsilon_i + e_i^{-1}$. ■

De hecho, hemos probado que

$$L = \mathbb{Q}(\epsilon_1 + \epsilon_1^{-1}, \cdots, \epsilon_r + \epsilon_r^{-1}).$$

8.3. **Toros no conmutativos.** El uso de los métodos de geometría no conmutativa para construir una teoría análoga a la de multiplicación compleja para campos cuadráticos reales, fue propuesto inicialmente por Yu.I. Manin en [7] y [8]. Esta linea de investigación es conocida como "el programa de multiplicación real".

La idea de Manin es remplazar las curvas elípticas por toros no conmutativos y la noción de isogenea por equivalencias de Morita. Manin observo, que así como las curvas elípticas con multiplicación compleja son las únicas curvas elípticas con endomorfismos adicionales no triviales [4], los toros no conmutativos $\mathbb{T}_\theta$ para los cuales el módulo θ es un punto de multiplicación real en $\mathbb{R}$, en un campo cuadrático real $K \subset \mathbb{R}$, tienen autoequivalencias de Morita no triviales, las cuales juegan el papel de los endomorfismos adicionales en las curvas elípticas con multiplicación compleja.

Uno de los principales problemas de extender la teoría de multiplicación compleja a la geometría no conmutativa, es que una curva elíptica junto a su modelo analítico como cociente tiene un modelo algebraico como curva definida por ecuaciones polinomiales, mientras que su análogo no conmutativo sólo tiene un buen modelo analítico pero no tiene un modelo algebraico completamente satisfactorio. Dicho modelo algebraico ayudaría a encontrar el análogo a los puntos de torsión de una curva elíptica en un toro no conmutativo.

Sin embargo, existe una aproximación al problema de clasificación de las extensiones de un campo cuadrático real trabajando directamente con el modelo analítico de toros no conmutativos. Esta aproximación consiste en reformular las conjeturas de Stark en términos de geometría no conmutativa. Dicha aproximación es presentada también por Manin en [8].

Una aproximación complementaria a ésta teoría es la de construir el análogo al espacio moduli de curvas elípticas, es decir, un espacio no conmutativo que parametrize a los toros no conmutativos salvo equivalencias de Morita. Esta teoría es referida a veces como la teoría de la "frontera invisible" de las curvas modulares, ya que ésta parametriza aquellas degeneraciones de la estructura de curvas elípticas que ya no son expresables por el modelo algebraico-geométrico pero que continúan existiendo en los toros no conmutativos. Nuevamente, el principal problema de ésta aproximación es encontrar el álgebra apropiada. Una descripción más detallada de ésta teoría y sus recientes avances puede consultarse en [10].

BIBLIOGRAFÍA

[1] V.G. Drinfeld, Elliptic modules, I, II. Math.USSR-Sbornik, 23,1976, 561-592; 31, 1977, 159-170.
[2] A. Knapp, *Elliptic Curves*, Princeton Univ. Press, 1992.
[3] S. Lang, *Elliptic Functions*. Addison-Wesley, 1973.
[4] S. Lang, *Complex Multiplication*, Springer-Verlag, 1983.
[5] S. Lang, *Algebraic Number Theory* Springer-Verlag, 1986.
[6] S. Lang, *Algebra* Springer-Verlag, 2002.
[7] Y.I. Manin, Von Zahlen und Figuren, in "Geometrie au XXe siècle. Historie et horizonts", Hermann (2005) 24-44.
[8] Y.I. Manin, Real Multiplication and noncommutative geometry, The legacy of Niels Henrik Abel, Springer (2005) 685-727.
[9] Y.I. Manin y A.A. Panchishkin, *Introduction to Modern Number Theory* Springer-Verlag, 2005.

[4] Entenderemos por endomorfismos triviales, a los inducidos vía multiplicación por un entero, *i.e.* las isogeneas $[m]$.

[10] M. Marcolli, Noncommutative geometry and arithmetic (ICM talk) to appear in the Proceedings of the ICM-2010, Hyderabad.
[11] J. Martinet, Character theory and Artin L-functions in *Algebraic number fields: L-functions and Galois properties*, Academic Press, 1977.
[12] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers* Springer-Verlag, 2004.
[13] J. Neukirch, *Algebraic Number Theory* Springer-Verlag, 1999.
[14] A. Robert, *Elliptic Curves*, Springer-Verlag, 1973.
[15] X-F. Roblot, Stark´s Conjectures and Hilbert's Twelfth Problem, Experiment. Math. vol 9:2 (2000), 251-260.
[16] J.P. Serre, Complex Multiplication in *Algebraic Number Theory*, J.W.S. Cassels and A. Fröhlich, eds. Academic Press, 1967, 292-296.
[17] J.P. Serre y J. Tate, Good reduction of abelian varietes, Annals of Math. 68 (1968), 492-517.
[18] G. Shimura, *Introduction to the Aritmetic Theory of Automorphic Functions*. Princeton Univ. Press, 1971.
[19] G. Shimura y Y. Taniyama, Complex multiplication of abelian varietes and its aplication to number theory. Nagoya Math. 43 (1971), 199-208.
[20] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton Univ. Press, 1998.
[21] J.H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.
[22] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.
[23] H. Stark, L-functions at s = 1, I: L-functions for quadratic forms, Adv. Math. 7 (1971), 301-343.
[24] H. Stark, L-functions at s = 1, II: Artin L-functions with rational characters, Adv. Math. 17 (1975), 60-92.
[25] H. Stark, L-functions at s = 1, III: Totally real fields and Hilbert's twelfth problem, Adv. Math. 22 (1976), 64-84.
[26] H. Stark, L-functions at s = 1, IV: First derivatives at $s = 0$, Adv. Math. 35 (1980), 197-235.
[27] J. Tate, Global class field theory in *Algebraic Number Theory*, J.W.S. Cassels and A. Fröhlich, eds. Academic Press, 1967, 173-203.
[28] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s=0*, Birkhäuser, Boston, 1984.
[29] L.C. Washington *Elliptic Curves Number Theory and Cryptography*, Chapman and Hall, 2008.