Arithmetic of CM Elliptic Curves

In Lecture 2, we explicitly constructed CM elliptic curves defined over the complex numbers. In Lecture 3, using the j-invariant, we showed CM elliptic curves can be defined over number fields. Today, we will further discuss the fields over which CM elliptic curves are defined and where isogenies among them are defined.

1 Galois Actions on Elliptic Curves

Let E be an elliptic curve defined over a number field K. Recall this means there exist $A, B \in K$ such that the elliptic curve E is defined by Weierstrass equation $y^2 = x^3 + Ax + B$. The absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ acts on the set of $\overline{K}$-points of E by its action on the coordinates. For any $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $P = (x, y) \in E(\overline{K})$, we write $P^\sigma = (\sigma(x), \sigma(y))$.

Let $\phi : E_1 \to E_2$ be an isogeny between elliptic curves E_1, E_2 defined over K. Recall a morphism ϕ is defined over K if for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have $\phi(P^\sigma) = (\phi(P))^\sigma$. Because an isogeny is determined by its kernel $\mathrm{Ker}\,\phi \subset E_1$, the field over which the isogeny ϕ is defined is the minimal field L such that for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ and $P \in \mathrm{Ker}\,\phi(\overline{\mathbb{Q}})$, the point $P^\sigma \in \mathrm{Ker}\,\phi(\overline{\mathbb{Q}})$.

Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then we can define an elliptic curve $E^\tau : y^2 = x^3 + \tau(A)x + \tau(B)$ and for any $P \in E(\overline{\mathbb{Q}})$, the point $P^\tau \in E^\tau(\overline{\mathbb{Q}})$. Another way to say an elliptic curve E is defined over K is that E is isomorphic to E^τ for any $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$for some isomorphism defined over K. Note that the map $E \to E^\tau$ given by $P \mapsto P^\tau$ is not algebraic in most cases. In other words, in general, an elliptic curve defined over a number field is not isogenous to its Galois conjugates. But we saw in Problem set 2 Problem 3 that CM elliptic curves are isogenous (over $\overline{\mathbb{Q}}$) to all of their Galois conjugates.

2 Field of Definition for $\mathrm{End}(E)$

Let E be an elliptic curve defined over a number field L. The endomorphism ring $\mathrm{End}_{\overline{L}}(E) \simeq \mathcal{O}$ where $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ is an order in an imaginary quadratic field. We want to determine over which field these endomorphisms are defined.

Lemma 2.1. *Let F be the field over which the endomorphisms are defined. Then $K \subset F$.*

Proof. Recall the set of holomorphic differentials $H^0(E, \Omega)$ is a 1-dimensional $\mathbb{C}$-vector space. Let $\Lambda \subset \mathbb{C}$ be a lattice such that $\mathbb{C}/\Lambda \simeq E(\mathbb{C})$ with $z \in \mathbb{C}$ corresponding to point $P_z \in E(\mathbb{C})$ and let $\iota : K \hookrightarrow \mathbb{C}$ be the embedding such that $\iota(\alpha)z = \alpha(P_z)$. Then the induced action α^* on $H^0(E, \Omega)$ is multiplication by α. Thus, if the endomorphism α commutes with Galois actions in $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, then $\alpha \in F$. □

The embedding $\iota : K \hookrightarrow \mathbb{C}$ in the proof of Lemma 2.1 is part of the CM data. To precisely describe the CM action, one should give $\mathcal{O}$ together with ι and this notion will be generalized to the notion *CM type* in the case of higher dimensional abelian varieties with complex multiplication.

Proposition 2.2. *Let E be an elliptic curve defined over a number field L. The endomorphism ring $\mathrm{End}_{\overline{L}}(E) \simeq \mathcal{O}$ where $\mathcal{O} \subset K = \mathbb{Q}(\sqrt{d})$ is an order in an imaginary quadratic field. Then for any $\alpha \in \mathcal{O}$, the endomorphism α is defined over the composition LK.*

Proof. From the proof of Lemma 2.1, there is an embedding $\iota : K \hookrightarrow \mathbb{C}$ such that the action of $\alpha \in \mathcal{O}$ on $V = H^0(E, \Omega)$ is multiplication by $\iota(\alpha)$. Recall from Lecture 1, since our discussion is over fields of characteristic 0, the map $\mathrm{End}_{\overline{L}}(K) \to \mathrm{End}(V)$ is injective. For any $\sigma \in \mathrm{Gal}(\overline{Q}/LK)$, since it fixes α^*, it also fixes α. We conclude the statement. □

3 Field of Definition for CM Elliptic Curves

We will restrict our discussion to the case of elliptic curves with CM by a maximal order. Let E be an elliptic curve defined over a number field L such that $\mathrm{End}_{\overline{L}}(E) \simeq \mathcal{O}_K$ where $\mathcal{O}_K$ is the ring of integers of an imaginary quadratic field K. We will discuss the field $K(j(E))$. Let's first state the conclusion and instead of discussing the proof, I will explain the statement and its implications.

Theorem 3.1. *The field $K(j(E))$ is the Hilbert class field of K.*

The *Hilbert class field* L of a number field K is the maximal unramified abelian extension of K. It is a Galois extension of K with Galois group $\mathrm{Gal}(L/K)$ isomorphic to the ideal class group $\mathcal{C}(K)$ (the group of fractional $\mathcal{O}_K$-ideals modulo the subgroup of principal fractional ideals) of K. The Principal ideal theorem gives an interesting property of the Hilbert class field, namely for any ideal $I \subset \mathcal{O}_K$, its extension $I\mathcal{O}_L \subset \mathcal{O}_L$ is a principal ideal.

For a number field K, the set of field extensions L/K are determined by the set of primes of K which splits completely in the extension. The Hilbert class field L is exactly the field extension L/K over which the set of split primes are all the principal ideals of K.

Recall the isomorphism classes of elliptic curves with CM by $\mathcal{O}_K$ are in bijection to lattices in $\mathbb{C}$ which are obtained from embeddings of fractional $\mathcal{O}_K$-ideals into $\mathbb{C}$ up to homothety. Let $\mathfrak{a} \subset K$ be a fractional $\mathcal{O}$ ideal and under an embedding $K \subset \mathcal{C}$ we make the following identification

$$\text{fractional } \mathcal{O}_K\text{-ideal } \mathfrak{a} \longleftrightarrow \text{lattice } \Lambda_{\mathfrak{a}} \longleftrightarrow \text{elliptic curve } E_{\mathfrak{a}}.$$

This gives a bijection between the set of these isomorphism classes of elliptic curves $\mathcal{S}$ with $\mathcal{C}(K)$ and thus $\mathcal{C}(K)$ acts on $\mathcal{S}$. Let L be the Hilbert class field of K, then there is a canonical isomorphism $\phi : \mathrm{Gal}(L/K) \to \mathcal{C}(K)$. This gives a $\mathrm{Gal}(\overline{K}/K)$ action on the set $\mathcal{S}$ and the theorem was proved by showing this action can be identified with the natural Galois action on $\mathcal{S}$ as we now describe.

Since $\overline{K}$-isomorphism classes of elliptic curves are determined by their j-invariants, we can describe the relationship between these two actions in the following way

$$(\phi^{-1}(\mathfrak{a}))(j(E_{\mathfrak{b}})) = j(E_{\mathfrak{a}^{-1}\mathfrak{b}})$$

where the left hand side action is the Galois action on the algebraic number $j(E_{\mathfrak{b}}) \in \overline{K}$.

Since the right hand side action: $\mathcal{C}(K)$ acting on $\mathcal{S}$ by $\mathfrak{a} : E_{\mathfrak{b}} \mapsto E_{\mathfrak{a}^{-1}\mathfrak{b}}$ is transitive, we conclude that the extension $K(j(E_{\mathfrak{a}}))/K$ is Galois with Galois group isomorphic to $\mathcal{C}(K)$. And the left hand Galois action shows that $\mathrm{Gal}(\overline{K}/L)$ acts trivially on $j(E_{\mathfrak{a}})$ identifying the field extensions L/K and $K(j(\mathfrak{a}))/K$.

In general, if E is an elliptic curve with CM by an order $\mathcal{O}$ of K, not necessarily the maximal order, then the field $K(j(E))$ is the ring class field of the order $\mathcal{O}$. This result is sometimes referred to as the **first main theorem of complex multiplication**.

The field extension $K(j(E))/K$ is abelian with Galois group $\mathrm{Gal}(K(j(E))/K) \simeq \mathcal{C}(\mathcal{O})$. Moreover, the field extension $K(j(E))/\mathbb{Q}$ is Galois and $\mathrm{Gal}(K(j(E))/\mathbb{Q}) \simeq \mathcal{C}(\mathcal{O}) \rtimes (\mathbb{Z}/2\mathbb{Z})$, a generalized dihedral group. In fact, if L/K is a finite abelian extension, then $L/\mathbb{Q}$ is a generalized dihedral extension if and only if $L \subset K(j(\mathcal{O}))$ for some order $\mathcal{O} \subset K$. So the first main theorem of complex multiplication helps us to describe abelian extensions of an imaginary quadratic field K which are generalized dihedral extensions of $\mathbb{Q}$. Next we will use CM elliptic curves to describe all abelian extension of K.

4 Torsion Fields of CM Elliptic Curves

Let K be an imaginary quadratic field, to describe all abelian extensions of K, we will use the torsion points of a CM elliptic curve.

Theorem 4.1. *Let E be an elliptic curve with CM by $\mathcal{O}_K$ defined over the Hilbert class field H of K. Consider the map $h : E \to E/\operatorname{Aut}(E) \simeq \mathbb{P}^1$ defined over H. By picking a parameter for $\mathbb{P}^1_H$, we get a function $h : E(\overline{H}) \setminus \{O\} \to \overline{H}$. Such a function is called a Weber function for E/H.*

Let L/K be a finite abelian extension, then there exists an ideal $\mathfrak{a} \subset \mathcal{O}_K$ such that $L \subset K(j(E), h(E[\mathfrak{a}]))$ where $E[\mathfrak{a}] = \{P \in E(\overline{L}) : \alpha P = O \text{ for all } \alpha \in \mathfrak{a}\}$.

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over H with CM by $\mathcal{O}_K$. If $j(E)$ is not equal to 0 or 1728, then its only nontrivial automorphism is $(x, y) \mapsto (x, -y)$. Thus, the function $(x, y) \mapsto x$ is a Weber function defined over H.

The theorem states that the maximal abelian extension of K is generated by the x-coordinates of all the torsion points of E. This is an implication of the second theorem of complex multiplication.