1. Talk on the main theorems of CM

We will start the CM-theory, by asking the famous question: *'Hilbert's* $12th$ *Problem'*.

'Hilbert's 12th Problem' is the question for finding special *transcendental functions*, whose values at some *special points* would generate all the abelian extensions of any number field K.

When $K = \mathbb{Q}$, Kronecker-Weber theorem gives an answer to the problem:

Theorem 1.1. *(Kronecker-Weber) For any abelian extension $K/\mathbb{Q}$, there exists a positive integer n such that*

$$K \subset \mathbb{Q}(\zeta_n) = \mathbb{Q}(\exp(\frac{2\pi i}{n})).$$

Here, the exponential function is the *transcendental function* and the special values are *n-th torsion points* of the unit circle.

When K is imaginary quadratic number field 'The CM-theory for elliptic curves' gives an answer to the problem:

Let K be an imaginary quadratic number field with ring of integers $\mathcal{O}_K = \mathbb{Z} + \tau\mathbb{Z}$. Complex analytically, we can construct an elliptic curve $E := \mathbb{C}/\mathcal{O}_K$. Then the value of j-function at τ (which is an algebraic number) generates the maximal unramified abelian extension H_K of K, i.e. $H_K = K(j(\tau))$. This gives an answer for unramified extension of imaginary quadratic fields, which is called 'The first main theorem for elliptic curves'. Moreover, we can also get the ray class fields $L_{\mathbf{m}}$ of conductor $m\mathcal{O}_K$ of K, by the values of Weber-function h at the m-torsion points of E, i.e. $L_{\mathbf{m}} = K(j(\tau), h(E[m])) = H_K(h(E[m]))$. This is 'the second main theorem for elliptic curves' and gives a complete solution to the problem.

Djordjo will give a talk on CFT and then Dino will give a talk on CM theory for elliptic curves. After these two talks these theorems will be more understandable.

'The theory of CM for Abelian Varieties' gives a partial answer to the problem for CM-fields (:= the imaginary quadratic extension of the totally real number fields). In this talk, we will see the generalization of the main theorem for elliptic curves for any abelian variety with CM. First I will define abelian variety then define CM-fields and the other ingredients to state the main theorem.

1.1. **Abelian Variety.**

Definition 1.2. *Let k be a field. An abelian variety over k is a connected complete (proper) group variety.*

Every abelian variety is smooth (group variety), projective (completeness) and commutative.

Now, let's ask some questions on the examples of abelian varieties.

• Is the group variety $\mathbb{C}^*$ an abelian variety? No, since $\mathbb{C}^*$ is not compact, it is not complete (not projective).

So now let's think about complex torus which is a complete variety.

• Is complex torus an abelian variety? If $\dim(A) = 1$, every complex torus is an elliptic curve and elliptic curves are the dimension 1 abelian varieties. If $\dim(A) > 1$, not every torus is isomorphic to an abelian variety because not every complex torus can be embedded in projective space.

Remark 1.3. *A complex torus $\mathbb{C}^g/\Lambda$ of dimension g is an abelian variety if and only if there exists a positive definite Riemann form on $\mathbb{C}^g/\Lambda$. Conversely, an abelian variety of dimension g is isomorphic to a complex torus over $\mathbb{C}$. (I will show in the talk 'Abelian Varieties over $\mathbb{C}$'.)*

Jacobian of a curve. Suppose C/k is an algebraic curve and that $C(k) \neq \emptyset$. The Jacobian variety of C is an abelian variety $J(C)$ such that for an extension k'/k, there is an (functorial) isomorphism $J(C)(k') \cong \mathrm{Pic}^0(X/k')$.

Definition 1.4. *An abelian variety A is said to be simple if it has no proper abelian subvarieties.*

The morphism of category of abelian varieties is a morphism of algebraic varieties complatible with group structures. Let A and B be abelian varieties. The set of homomorphisms from A to B is denoted by $\mathrm{Hom}_k(A, B)$ and which is a free $\mathbb{Z}$-module of finite rank. The endomorphism ring is denoted by $\mathrm{End}(A)$ and this is the important object in the theory of CM.

An *isogeny* is a surjective morphism with a finite kernel.

Now, let's define CM-field: A *CM-field* is a totally imaginary quadratic extension of a totally real number field.

Proposition 1.5. *The following conditions on a CM-field K are equivalent:*

(i) *K is a CM-field;*

(ii) *There exists an automorphism $\bar{\cdot} \neq \mathrm{id}$ of K such that $\rho \circ \bar{\cdot} = \bar{\cdot} \circ \rho$ for all $\rho : K \hookrightarrow \mathbb{C}$;*

(iii) *$K = F[\alpha]$ with F is totally real, $\alpha^2 \in F$, $\rho(\alpha^2) < 0$ for all $\alpha \hookrightarrow \mathbb{C}$.*

Proof. By taking F to be the fixed field of $\bar{\cdot}$ we get the equivalence of (i) and (ii). $(i) \Leftrightarrow (iii)$ Let α generate K over F. Then $\alpha^2 \in F$ and also $\rho(\alpha^2) < 0$ for all ρ since K is totally imaginary. Conversely, the condition (3) imply that K is totally imaginary quadratic extension of F. □

Now we can define the notion of complex multiplication:

Definition 1.6. *An abelian variety A of dimension $2g$ has complex multiplication by an order $\mathcal{O}$ in a CM-field K of degree $2g$ if there exists an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(A)$.*

Example Consider the elliptic curve $E : y^2 = x^3 + x$ over a field k. Assume $j \in k$ satisfies $j^2 = -1$. Let $K = \mathbb{Q}(i)$ and $\mathcal{O} = \mathbb{Z}[i]$. Then K has CM by $\mathcal{O}$ via the embedding ι given by $\iota(i)(x, y) = (-x, jy)$.

To classify the isogeny classes of abelian varieties with CM, we need the notion of CM-type.

Definition 1.7. *Let K be a CM-field of degree $2g$ and $L'/\mathbb{Q}$ be a normal field that contains a subfield isomorphic to K. Let L be a normal closure of K. A CM-type of K with values in L' is a subset $\Phi \subset \mathrm{Hom}(K, L')$ consisting of exactly one element from each of the g complex conjugate pairs $\{\phi, \overline{\phi}\} \subset \mathrm{Hom}(K, L')$.*

We say that a CM-type Φ is *primitive* if it is not induced from a CM-type of a strict CM-subfield.

If we have an abelian variety A/k with CM by K via ι, then we can define its *CM*-type Φ as the homomorphisms $K \to k$ appearing in the representation of K on the tangent space of A. We say that (A, ι) is of type Φ. (We will see on a later talk.)

Theorem 1.8. *Isogeny classes of abelian varieties with CM by a CM-field K are in bijection with the primitive CM-types of K.*

To be able to state the main theorem we also need to the notion of the type norm and the reflex field.

The *type norm* is the map

$$\begin{aligned} \mathrm{N}_\Phi : & K \to L' \\ & x \mapsto \prod_{\phi \in \Phi} \phi(x) \end{aligned}$$

and the field $K^r \subset L'$ generated by the image of N_Φ is CM-field is called the *reflex field* of (K, Φ). The reflex type of (K, Φ) is CM-type Φ^r of K^r with values in L' can be viewed as the set of 'inverses' of elements of Φ.

We also define type norm N_Φ on ideal groups. For a field K, let I_K be the group of fractional ideals of $\mathcal{O}_K$. Then

$$\begin{aligned} \mathrm{N}_\Phi : & I_K \to I_{K^r} \\ & \mathfrak{b} \mapsto \mathfrak{b}' \text{ such that } \mathfrak{b}'\mathcal{O}_{L'} = \prod_{\phi \in \Phi} \phi(\mathfrak{b}')\mathcal{O}_{L'} \end{aligned}$$

which is a well-defined map.

1.2. **Polarization & Field of Moduli.** Abelian varieties might have too many automorphisms for a moduli space exist. We define polarization on abelian varieties that solve this problem.

Let X be a divisor on an abelian variety A. If the map

$$\begin{aligned} \varphi_X : & A \to \mathrm{Pic}^0(A) = A^V \\ & a \mapsto \mathrm{Cl}(X_a - X) \end{aligned}$$

is an isogeny, then φ_X is called polarization of A. If this map is an isomorphism then it is called principal polarization of A.

Remark 1.9. *All abelian varieties are polarizable.*

We understand by a polarized abelian variety a couple (A, φ). Now I give a very important theorem which is base of the definition of field of moduli:

Theorem 1.10. *Let A be an abelian variety and φ be a polarization of A. Then there exists a field k_0 with the following properties:*

(M) k & σ being respectively a field definition for (A, φ) containing k_0 and isomorphism of k into a field. Then, the polarized abelian variety (A, φ) is isomorphic to $(A^\sigma, \varphi^\sigma)$ if and only if σ is identity on k_0.

We call the field k_0 with property (M), which is uniquely determined if char $k = 0$, the field of moduli of (A, φ).

If char $k = 0$, (A, φ) determines a point $j(A, \varphi)$ (represents an isomorphism class of (A, φ)) in the *coarse moduli space of of polarized abelian varieties*, (which we will define later). The field of moduli is the smallest field containing $K(j(A, \varphi))$.

Now we can state the first main theorem of CM:

The first main theorem of Complex Multiplication. Let (K, Φ) be a primitive CM-type with the reflex (K^r, Φ^r). Let A be an abelian variety over a field $k \supset K$ with CM by $\mathcal{O}_K$ via ι of type Φ, and φ a polarization of A. Let $K(j(A, \varphi)) \subset \overline{k}$ be the field of moduli of (A, φ). Then the composite CM_{K^r,Φ^r} of $K(j(A, \varphi))$ and K^r is the unramified class field over K^r corresponding to the ideal-group $H_{K,\Phi}$, where

$$\begin{aligned} H_{K^r,\Phi^r} &= \{\mathfrak{b} \in I_{K^r} : \exists \mu \in K^* \text{ s.t. } \mathrm{N}_{\Phi^r}(\mathfrak{b}) = (\mu) \text{ and } \mu\overline{\mu} = \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{b})\} \\ &\supset P_K = \{x\mathcal{O}_K : x \in K^*\} \end{aligned}$$

Moreover, the Artin isomorphism

$$\psi : I_{K^r}/H_{K^r,\Phi^r} \to \mathrm{Gal}(\mathrm{CM}_{K^r,\Phi^r}/K^r)$$

is given by

$$\psi(\mathfrak{b}) j(A, \varphi) = j(A/A[\iota(\mathrm{N}_{\Phi^r}(\mathfrak{b}))], \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{b})\varphi)$$

for all $\mathfrak{b} \in I_{K^r}$.

If $g = 1$, then K is an imaginary quadratic field; $\Phi = \{\mathrm{id}\}$; $K^r = K$ and $\Phi^r = \{\mathrm{id}\}$. So the set H_{K^r,Φ^r} is the group of principal ideals P_K. Let E be an elliptic curve over a field $k \supset K$ with CM by $\mathcal{O}_K$ via ι. Since each elliptic curve has a canonical polarization, we can forget about polarization. The field of moduli of E is the Hilbert Class Field $H_K = K(j(E))$ of K and we have the Artin isomorphism

$$\psi : \mathrm{Cl}(\mathcal{O}_K) \to \mathrm{Gal}(H_K/K)$$

is given by

$$\psi([\mathfrak{b}])j(E) = j(E/E[\mathfrak{b}])$$

for all $\mathfrak{b} \in I_K$.

The second main theorem of Complex Multiplication. Let (K, Φ) be a primitive CM-type with the reflex (K^r, Φ^r). Let A be an abelian variety over a field $k \supset K$ with CM by $\mathcal{O}_K$ via ι of type Φ, and φ a polarization of A. Let $\mathfrak{a}$ be an integral ideal of K and let a be the smallest positive integer divisible by $\mathfrak{a}$. Let $t \in A(\bar{t})$ be a point with annihilator $\mathfrak{a}$. Let $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{a}) = K(j(A, \varphi, t)) \subset \overline{k}$ be the field of moduli of (A, φ). Then $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{a})$ is the abelian extension of K corresponding to $I_{K^r}(a)/H_{K^r,\Phi^r}(\mathfrak{a})$, where

$$\begin{aligned} H_{K^r,\Phi^r}(\mathfrak{a}) = \{\mathfrak{b} \in I_K((a)) :& \exists \mu \in (K^r)^* \text{ s.t. } \mathrm{N}_\Phi(\mathfrak{b}) = \mu\mathcal{O}_{K^r}, \\ & \mu\overline{\mu} = \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{b}), \text{ and } \mu \equiv 1 \pmod{a}\} \end{aligned}$$

$$\supset P_K(a) = \{x\mathcal{O}_K : x \in K^*,\ x \equiv \pmod{a}\}.$$

Moreover, the Artin isomorphism

$$\psi : I_{K^r}(a)/H_{K^r,\Phi^r}(\mathfrak{a}) \to \mathrm{Gal}(\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{a})/K^r)$$

is given by

$$\psi(\mathfrak{b})j(A, \Phi, t) = j(A/A[\iota\mathrm{N}_{\Phi^r}(\mathfrak{b})], \mathrm{N}(\mathfrak{b})\varphi, t)$$

for all $\mathfrak{b} \in I_{K^r}(a)$.

Here j is a point in the moduli space of polarized abelian varieties together with a point of order a.

If we take $\mathfrak{a} = 1$, then $t = 0$ and we can leave out $\mathfrak{a}$, a, t from the notation and thus we get the first main theorem.

Moreover, if we take $g = 1$, we see that $H(\mathfrak{a}) = P_K(\mathfrak{a}) \cap I_K(a)$, where

$$P_K(\mathfrak{a}) = \{x\mathcal{O}_K : x \in K^*, x \equiv 1 \pmod{\mathfrak{a}}\}.$$

So we have that $\mathrm{CM}(\mathfrak{a})$ is the ray class field for the modulus $\mathfrak{a}$.

We haven't given the complete answer to Hilbert's 12th problem for CM-fields. In a later talk, we may see the analogue of the exponential function in terms of Weierstrass σ-function.

In this lecture series our aim is to understand the proofs of the main theorems and the following theorem:

For a simple abelian variety, the Frobenius element F_q in the ring $\mathrm{End}(A)$ is an algebraic integer. Weil showed that all complex values of this algebraic integer are $\sqrt{q}$ and we call algebraic integers with this property *Weil q-numbers.*

Theorem 1.11. *(Honda-Tate theory) There is a bijection*

$$\frac{\{\textit{simple abelian varieties over } \boldsymbol{F}_q\}}{\textit{isogeny}} \to \frac{\{\textit{Weil q-numbers}\}}{\textit{conjugation}}$$

$$A \mapsto F_q.$$