Introduction for the seminar on complex multiplication

Marco Streng

October 14, 2009

Abstract

We state the "main theorems of complex multiplication" and point out notions to be defined during the seminar. We mention Kronecker's Jugendtraum and Honda-Tate theory as motivation.

These are notes of an introductionary talk for a seminar on complex multiplication. Please email any errors or suggestions to marco.streng@gmail.com

1 Kronecker's Jugendtraum

Kronecker-Weber Theorem. *Let $K/\mathbf{Q}$ be a finite abelian Galois extension. Then there is a positive integer n such that we have*

$$K \subset \mathbf{Q}(\zeta_n) = \mathbf{Q}(t : t \in \mathbf{G}_m(\overline{\mathbf{Q}})[n]) = \mathbf{Q}(\exp(2\pi i \frac{1}{n})).$$

In particular, we have $K^{\mathrm{ab}} = \mathbf{Q}(t : t \in \mathbf{G}_m(\overline{\mathbf{Q}}))$.

Hilbert's twelfth problem (a.k.a. Kronecker's Jugendtraum) is, for any number field F, to find an analogue of $z \mapsto \exp(2\pi i z)$ when $\mathbf{Q}$ is replaced by F. Kronecker himself, with the theory of complex multiplication of elliptic curves, gave a full answer for the case where F is imaginary quadratic. With the theory of complex multiplication of abelian varieties, Shimura and Taniyama [3] generalized this to a partial answer for the case where F is a *CM field*.

Definition. A CM field is a field $K = K_0(\sqrt{r})$, where K_0 is a totally real number field and $r \in K_0$ is totally negative.

We denote the automorphism of K with fixed field K_0 by $x \mapsto \overline{x}$ and note that it equals complex conjugation for every embedding of K into $\mathbf{C}$.

For a CM field K, we will obtain a large part of K^{ab} by replacing $\mathbf{G}_m$ above by an *abelian variety with complex multiplication by K*. This is the first halve of the motivation for our seminar.

2 Abelian varieties and complex multiplication

Let k be a field. An *abelian variety* A/k is a proper connected group variety over k. It is known that every abelian variety is smooth, projective, and commutative. We use the notation $g = \dim(A)$ and k will always be the base field of A.

Examples.

- A 1-dimensional abelian variety is exactly the same as an *elliptic curve*.
- Every abelian variety over $k = \mathbf{C}$ is (as a complex manifold) isomorphic to a *complex torus*, i.e. a manifold of the form $\mathbf{C}^g/\Lambda$, for a lattice Λ of rank $2g$ in $\mathbf{C}^g$. A complex torus is an abelian variety if and only if it has a positive definite *Riemann form*, as we will see in a later talk.
- If C/k is a curve, then there exists an abelian variety $J(C)/k$ called the *Jacobian* such that for every field extension l/k with $C(l) \neq 0$, we have $J(C)(l) = \mathrm{Pic}^0(C_l)$.

We define the category of abelian varieties by setting

$$\mathrm{Hom}(A, B) = \{k\text{-variety morphisms (defined over } k) \text{ s.t. } 0 \mapsto 0\}.$$

It is known that all elements of $\mathrm{Hom}(A, B)$ are homomorphisms of group varieties, i.e. respect the group structure. An important object in the theory of complex multiplication is the *endomorphism ring* $\mathrm{End}(A) = \mathrm{Hom}(A, A)$.

Definition. We say that A (of dimension g) has *complex multiplication* or *CM* by an order $\mathcal{O}$ in a CM field K of degree $2g$ if there exists an embedding $\iota : \mathcal{O} \to \mathrm{End}(A)$.

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

Here is another important example of an endomorphism.

Example. Let $A/\mathbf{F}_q$ be an abelian variety over a finite field. We define the *Frobenius endomorphism* $F_q \in \mathrm{End}(A)$ as follows. Choose a projective model of A with coefficients in $\mathbf{F}_q$ (more intrinsic definitions exist, but this serves our purpose of illustration). Then F_q is the morphism from A to itself that sends a point $x = (x_0 : \cdots : x_n)$ to $x^q = (x_0^q : \cdots : x_0^q)$.

This example is important for (among other things) the second halve of our motivation: Honda-Tate theory.

3 Honda-Tate theory

An *isogeny* is a surjective morphism of abelian varieties with a finite kernel. An abelian variety is called *simple* if it is not isogenous to a product of lower-dimensional abelian varieties. It is known that every abelian variety is isogenous to a product of simple abelian varieties.

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 absolute values of this algebraic integer are $\sqrt{q}$, and we call algebraic integers with this property *Weil q-numbers*.

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

$$\begin{array}{ccc} \dfrac{\{\textit{simple abelian varieties over } \mathbf{F}_q\}}{\textit{isogeny}} & \to & \dfrac{\{\textit{Weil } q\textit{-numbers}\}}{\textit{conjugation}} \\ A & \mapsto & F_q. \end{array}$$

Weil's result implies that the map is well-defined. Tate showed that it is injective. Honda used the theory of complex multiplication to show that every element on the right has a power that is in the image of the map. Tate used this to show that the map is surjective.

The surjectivity result is constructive and we can look at algorithmic aspects during the seminar. The Frobenius endomorphism (as an algebraic integer) determines the number of rational points of the corresponding abelian variety. This implies that, by applying this construction to suitable Weil q-numbers, one can obtain abelian varieties of which the group of rational points is suitable for discrete logarithm based cryptography.

4 The Hilbert class field

Let K be any number field. Then (inside an algebraic closure of K), there is a largest unramified abelian Galois extension H_K of K and it is called the *Hilbert class field* of K.

Here 'unramified' not only means unramified at all finite primes, but also at all infinite primes (meaning that real embeddings stay real). As CM fields have no real embeddings, this is not relevant if K is a CM field.

There is a well defined bijection

$$\mathrm{Cl}_K \to \mathrm{Gal}(H_K/K)$$

given by the *Artin map*

$$\mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}.$$

Here the *Frobenius automorphism* $\mathrm{Frob}_{\mathfrak{p}}$ is the unique automorphism of H_K satisfying (for $\mathfrak{P}$ a prime of H_K lying over $\mathfrak{p}$)

$$\mathrm{Frob}_{\mathfrak{p}}(x) \cong x^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$$

for all $x \in K^*$ coprime to $\mathfrak{P}$. In other words, it is a lift of the $N(\mathfrak{p})$-th power Frobenius automorphism of the residue field of $\mathfrak{P}$.

5 The first main theorem for elliptic curves

Now suppose K is imaginary quadratic and let $\mathcal{O}_K$ be its maximal order. Let E be an elliptic curve over a field k of characteristic 0 with CM by $\mathcal{O}$ via $\iota : \mathcal{O}_K \to \mathrm{End}(A)$. Then ι induces an embedding of K into k via the tangent space of E at 0 (as we will see in another talk). We identify K with its images in k and $\mathrm{End}(A) \otimes \mathbf{Q}$.

Theorem. *With the notation and assumptions above, we have*

$$H_K = K(j(E)) \subset k.$$

Moreover, the Artin map $\psi : \mathrm{Cl}_K \to \mathrm{Gal}(H_K/K)$ is given by

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

for all ideals $\mathfrak{a} \subset \mathcal{O}_K$.

Here we define the $\mathfrak{a}$-torsion subgroup $E[\mathfrak{a}]$ of E by

$$E[\mathfrak{a}] = \cap_{\alpha \in \mathfrak{a}} E[\mathfrak{a}]$$

and note that quotients of elliptic curves by finite subgroups exist.

Complex analytically, we can take $E = \mathbf{C}/\mathcal{O}_K$ and note that $j(\mathbf{C}/(\mathbf{Z} + \tau\mathbf{Z})$ is a complex analytic function of τ. This gives the complex analytic description $H_K = K(j((\sqrt{D} + D)/2))$ of H_K and answers Hilbert's twelfth problem for unramified extensions of imaginary quadratic number fields.

6 What do we need for the higher dimensional analogue?

Moduli and polarizations

An important object in the previous theorem is the j-invariant, i.e. the moduli space of elliptic curves. Abelian varieties in general have too many automorphisms for a moduli space to exist. Actually, CM abelian varieties of dimension $g \geq 2$ always have infinitely many automorphisms, since the unit group $\mathcal{O}_K^*$ has rank $g - 1$.

To solve this problem, we look at abelian varieties together with a *polarization* φ. Polarizations will be defined in a later talk. For elliptic curves, we can forget about them, because every elliptic curve has a unique polarization of degree 1.

By $j(A, \varphi)$, we will mean the isomorphism class of (A, φ) or, equivalently, the point corresponding to (A, φ) in the *coarse moduli space of polarized abelian varieties* (which we will also define later). By $F(j(A, \varphi))$, we will mean the smallest field containing F over which the point in the moduli space is defined, or, equivalently, the *field of moduli* of (A, φ) as defined in [3].

CM types and type norms

Next, recall that (in the elliptic case), we generated an extension of K by taking elements from k. The connection between those two fields was given by an embedding $K \to k$ induced via the tangent space. In general, such a connection is given by *CM types* and the *type norm*.

Definition. Let K be a CM field of degree $2g$ and $L'/\mathbf{Q}$ a normal extension. A *CM type* Φ of K with values in L' is a set of g embeddings of K into L' of which no two are complex conjugate to each other (recall that complex conjugation is a well defined automorphism of K).

Suppose k has characteristic 0 and A/k has CM by K via ι. Then in some way (we will see the details in another talk, but it has to do with diagonalizing the representation of K on the tangent space of A) we assign to (A, ι) a *CM type* Φ of K with values in $\overline{k}$ and we say that (A, ι) is *of type* Φ.

We will also need the *reflex* and the *type norm* of a CM type. The type norm is the map

$$K \to L' : \quad x \mapsto \prod_{\phi \in \Phi} \phi(x).$$

The field $K' \subset L'$ generated by the image is a CM field (as we will see in a later talk) and is called the *reflex field* of (K, Φ). At some point, we will see the definition of the *reflex type* of (K, Φ), which is a CM type Φ' of K' with values in $\overline{K}$ and can be viewed as the set of 'inverses' of elements of Φ. We will see that the reflex field of (K', Φ') is a subfield of K.

We define the *type norm* N_Φ on unit and ideal groups as follows. For a field F, let I_F be the group of invertible fractional ideals of $\mathcal{O}_F$. The type norm N_Φ is given by

$$\begin{aligned} N_\Phi : K^* &\to (K')^* \\ x &\mapsto \prod_{\phi \in \Phi} \phi(x) \quad \text{and} \\ N_\Phi : I_K &\to I_{K'} \\ \mathfrak{a} &\mapsto \mathfrak{a}' \quad \text{such that } \mathfrak{a}'\mathcal{O}_{L'} = \textstyle\prod_{\phi \in \Phi} \phi(\mathfrak{a})\mathcal{O}_{L'}. \end{aligned}$$

The fact that the type norm is well defined on ideals needs a proof (which we do not give in this talk). It is easy to see that $N_\Phi(x)\overline{N_\Phi(x)} = N(x)$ and $N_\Phi(\mathfrak{a})\overline{N_\Phi(\mathfrak{a})} = N(\mathfrak{a})\mathcal{O}_{K'}$, where $N = N_{K/\mathbf{Q}}$ denotes the norm, taking positive values in $\mathbf{Q}$.

7 The main theorems of complex multiplication

The first main theorem

We can now formulate the main theorems of complex multiplication.

The first main theorem of complex multiplication. *Given a CM field F with a CM type Ψ, let (K,Φ) be the reflex of (F,Ψ), let A be an abelian variety over a field $k \supset F$ with CM by $\mathcal{O}_K$ via ι of type Φ, and let φ be a polarization of A. Let $\mathrm{CM}_{F,\Psi} = F(j(A,\varphi)) \subset \overline{k}$.*

Then $\mathrm{CM}_{F,\Psi}$ is the unramified abelian extension of F corresponding to $I_F/H_{F,\Psi}$, where

$$\begin{aligned} H_{F,\Psi} &= \left\{ \mathfrak{a} \in I_F : \begin{array}{c} \exists \mu \in K^* \ \text{ such that} \\ N_\Psi(\mathfrak{a}) = \mu\mathcal{O}_K, \\ \mu\overline{\mu} = N(\mathfrak{a}) \end{array} \right\} \\ &\subset P_F = \{x\mathcal{O}_F : x \in F^*\}. \end{aligned}$$

Moreover, the Artin isomorphism

$$I_F/H_{F,\Psi} \to \mathrm{Gal}(\mathrm{CM}_{F,\Psi}/F)$$

is given by

$$\psi(\mathfrak{a})j(A,\varphi) = j(A/A[\iota N_\Psi(\mathfrak{a})], N(\mathfrak{a})\varphi)$$

for all $\mathfrak{a} \subset \mathcal{O}_F$ in I_F.

Here, as in the elliptic case, we set

$$A[\iota(\mathfrak{c})] = \cap_{\gamma\in\mathfrak{c}} A[\iota(\gamma)]$$

for ideals $\mathfrak{c} \subset \mathcal{O}_K$ and it is possible to take quotients of abelian varieties by this finite subgroup (as we may see later in the seminar). We will see that $N(\mathfrak{a})\varphi$ induces a polarization on the quotient.

The case $g = 1$. If F is an imaginary quadratic field, then we can identify F and K via $\Psi = N_\Psi$. If we do that, then N_Φ is the identity map. Moreover, we can leave out the polarizations from the notation, since we can take φ to be the unique polarization on the elliptic curve A of degree 1. We then get the previous "first main theorem" back.

Existence. We will see in later talks that everything after 'let' in the theorem actually exists, so that the theory of complex multiplication actually constructs the abelian extension corresponding to $H_{F,\Psi}$ for given F, Ψ.

This result in the literature This theorem is due to Shimura and Taniyama and is "Main Theorem 1" on page 112 of their book [3].

Actually, Shimura and Taniyama [3] only state the fact that $\mathrm{CM}_{F,\Psi}$ is the class field corresponding to $H_{F,\Psi}$. The explicit Galois action is in the proof.

Also, Shimura and Taniyama [3] restrict to the case where Ψ is a primitive CM type of F. However, this restriction can be removed as shown by Shimura [2].

The second main theorem of complex multiplication

The second main theorem of complex multiplication is the following generalization of the first main theorem. It requires more knowledge of *class field theory* than just the Hilbert class field. Let $I_F(b)$ be the group of invertible fractional ideals of F that are coprime to b.

Our first formulation of the second main theorem of complex multiplication. *Given a CM field F with a CM type Ψ, let (K, Φ) be the reflex of (F, Ψ), let A be an abelian variety over a field $k \supset F$ with CM by $\mathcal{O}_K$ via ι of type Φ, and let φ be a polarization of A.*

Given an ideal $\mathfrak{b} \subset \mathcal{O}_K$. Let $t \in A(\overline{k})$ be a point with annihilator $\mathfrak{b}$ and let b be the smallest positive integer in $\mathfrak{b} \cap \mathbf{Z}$.

Let $\mathrm{CM}_{F,\Psi}(\mathfrak{b}) = F(j(A, \varphi, t)) \subset \overline{k}$.

Then $\mathrm{CM}_{F,\Psi}(\mathfrak{b})$ is the abelian extension of F corresponding to $I_F(b)/H_{F,\Psi}(\mathfrak{b})$, where

$$\begin{aligned} H_{F,\Psi}(\mathfrak{b}) &= \left\{ \mathfrak{a} \in I_F(b) : \begin{array}{l} \exists \mu \in K^* \ \text{ such that} \\ N_\Psi(\mathfrak{a}) = \mu \mathcal{O}_K, \\ \mu\overline{\mu} = N(\mathfrak{a}), \\ \mu \equiv 1 \pmod{b} \end{array} \right\} \\ &\subset P_F(b) = \{x\mathcal{O}_F : x \in F^*, x \equiv 1 \pmod{b}\}. \end{aligned}$$

Moreover, the Artin isomorphism

$$I_F(b)/H_{F,\Psi}(\mathfrak{b}) \to \mathrm{Gal}(\mathrm{CM}_{F,\Psi}(\mathfrak{b})/F)$$

is given by

$$\psi(\mathfrak{a}) j(A, \varphi, t) = j(A/A[\iota N_\Psi(\mathfrak{a})], N(\mathfrak{a})\varphi, t)$$

for all $\mathfrak{a} \subset \mathcal{O}_F$ in $I_F(b)$.

Here j is a point in the moduli space of polarized abelian varieties together with a point of order b. By the point t on the quotient abelian variety, we mean the image of t under the quotient morphism.

The first main theorem as a special case. If we take $\mathfrak{b} = 1$, then $t = 0$ on A and we can leave out $t, \mathfrak{b}$, and b from the notation. This gives us the first main theorem as a special case of the second.

Existence. Again, everything after 'let' really exists (as we will see) so that the theory of complex multiplication actually constructs the abelian extension corresponding to $H_{F,\Psi}(\mathfrak{b})$ for given $F, \Psi, \mathfrak{b}$.

The case $g = 1$. If F is an imaginary quadratic number field, and we identify F and K via $\Psi = N_\Psi$, then one sees

$$H(\mathfrak{b}) = P_F(\mathfrak{b}) \cap I_F(b),$$

where

$$P_F(\mathfrak{b}) = \{x\mathcal{O}_F : x \in F^*, x \equiv 1 \pmod{\mathfrak{b}}\}.$$

This shows that for F imaginary quadratic, we have that $CM(\mathfrak{b})$ is the *ray class field* for the modulus $\mathfrak{b}$ and that we have $F^{\mathrm{ab}} = \cup CM(\mathfrak{b})$.

The class fields obtained by complex multiplication. In general, we don't get all abelian extensions of F by complex multiplication, since $H(\mathfrak{b})$ is not all of $P_F(\mathfrak{b}) \cap I_F(b)$. Which fields we can obtain is studied in [2] and is an interesting subject for a talk in the seminar.

Kronecker's Jugendtraum. This is not actually an analogue of the map $z \mapsto \exp(2\pi i z)$ yet, but it comes very close. It does give $A(\overline{F})[\mathfrak{b}]$ as an analogue of $\mathbf{G}_m(\overline{Q})[n]$. Moreover, we may see in a later talk how to use this theorem to express the field $\mathrm{CM}_{F,\Psi}(\mathfrak{b})$ in terms of Weierstrass σ functions.

This result in the literature. The theorem as stated above is different from the original formulation as "Main Theorem 2" on page 118 of Shimura and Taniyama's book [3] in the sense that it gives $\mathrm{CM}_{F,\Psi}(\mathfrak{b})$ directly over K instead of over $\mathrm{CM}_{F,\Psi}$. We give a formulation in Section 9 below that looks more like the one in [3].

The statement as above follows from the proof of the result in [3]. The fact that we do not need to assume Ψ to be primitive is again in [2].

There is also an adelic formulation in [3] and [1]. We may give that formulation at a later stage in the seminar.

8 Frobenius morphisms of reductions of CM abelian varieties

The most important ingredient in the proof of the main theorem is the formula of Shimura and Taniyama that gives the Frobenius morphism of the reduction of a CM abelian variety.

Frobenius morphisms. Here is a more general version of the Frobenius morphism than the one we had before: if A/k is an abelian variety over a field of characteristic p and q is a power of p, and we assume A to be given as a projective variety, then let $A^{(q)}$ be the variety obtained by raising the coefficients of A to the q-th power. We get a morphism of abelian varieties

$$\begin{array}{rccc} F_q : A & \to & A^{(q)} \\ x & \mapsto & x^q \end{array}$$

by raising the coordinates of x to the q-th power. In the case $q = \#k$, we get the Frobenius *endo*morphism that we mentioned before.

Reduction. Now suppose that A/k is an abelian variety over a number field, again given by a projective model. Then we can get a *reduction* of A modulo a prime $\mathfrak{P}$ of k by reducing the coefficients of A and if this reduction is 'well behaved' in some way that we will see in a later talk, then A has *good reduction*. We can extend this notion to sets of abelian varieties and their 'Hom'-s. We will see that the 'Hom'-s are finitely generated as abelian groups, hence every finite set of abelian varieties has good reduction at almost all primes.

In fact, a possible subject for a later time in our seminar is the fact that every abelian variety with CM has *potential good reduction*, that is, a model over some field extension such that it has good reduction at every prime.

Theorem (Shimura-Taniyama [3, §13])**.** *Let A be an abelian variety over a number field k with complex multiplication by $\mathcal{O}_K$ via ι of type Φ and assume that A and its endomorphism ring have good reduction (and possibly some more assumptions?) at a prime $\mathfrak{P}$ of k.*

Let (F, Ψ) be the reflex of (K, Φ), assume $k \supset F$ and let $\mathfrak{p} = \mathfrak{P} \cap F$. Let $\widetilde{A}$ be the reduction of A modulo $\mathfrak{P}$ and let $q = N(\mathfrak{p})$.

Then we have

1. *The map $F_q : \widetilde{A} \to \widetilde{A}^{(q)}$ is a quotient of A by $A[\iota N_\Psi(\mathfrak{p})]$.*
2. *The endomorphism $F_{N(\mathfrak{P})} \in \mathrm{End}(A)$ is the reduction modulo $\mathfrak{P}$ of an endomorphism $\iota(\pi)$ for some $\pi \in \mathcal{O}_K$. Moreover, we have*

$$\pi\mathcal{O}_K = N_\Psi(N_{k/F}(\mathfrak{P})).$$

One of our goals in the seminar is to prove this result.

Sketch of the proof of the main theorem. Using the first part of this result, we can sketch the proof of the main theorem. If we don't worry about the polarization φ or the point t, then we see $j(\widetilde{A})^q = j(\widetilde{A}^{(q)}) = j(\widetilde{A}/\widetilde{A}[\iota N_\Psi(\mathfrak{p})])$. This shows the identity

$$\psi([\mathfrak{a}])j(A, \varphi, t) = j(A/A[\iota N_\Psi(\mathfrak{a})], \varphi', t)$$

already modulo details and modulo $\mathfrak{P}$, where φ' is the induced polarization on the quotient. One of our goals is to fill in the details and give the proof of the main theorem. We only need good reduction at all but finitely many primes for this.

Sketch of the proof of Honda's result. If we use the second part of the above theorem, then we can see how to obtain an abelian variety corresponding to a given Weil q-number if we can write it as a type norm. In fact, given a Weil q-number π, if we can write a power of π as a type norm of an ideal in a CM field, and show the existence of abelian varieties with CM of that type, and show that it has potential good reduction, then a power of π is a Frobenius endomorphism for the reduction of such an abelian variety, which is a result of Honda.

9 The second main theorem revisited

For the second formulation of the second main theorem, we look at the relative extension $CM(\mathfrak{b})/CM$ and its Galois group $(H_{F,\Psi} \cap I_F(b))/H_{F,\Psi}(\mathfrak{b})$. Let

$$M(b) = \{\mu \in K^*, \mu\overline{\mu} \in \mathbf{Q}^*, \mu \text{ coprime to } b\}/(\mathcal{O}_K^*)^{\mathrm{tor}}.$$

We find injective morphisms

$$N_\Psi : H_{F,\Psi} \cap I_F(b) \to M(b), \quad \text{and}$$

$$N_\Psi : (H_{F,\Psi} \cap I_F(b))/H_{F,\Psi}(\mathfrak{b}) \to M(b)/(M(b) \cap 1 + \mathfrak{b}).$$

Let N be the image of the second map. Note that every element of N has a representative $\mu \in \mathcal{O}_K$.

The case $g = 1$. If F is imaginary quadratic, then the maps N_Ψ are isomorphisms and the group $M(b)/(M(b) \cap 1 + \mathfrak{b})$ is naturally isomorphic to $(\mathcal{O}_F/\mathfrak{b})^*/\mathcal{O}_F^*$. For $g \geq 2$, it is an interesting question what N is and if we can find such a nice presentation of the group. We hope to see an answer during the seminar.

The normalized Kummer variety. The normalized Kummer variety of a polarized abelian variety $(A, \varphi)/k$ is a morphism of varieties $V : A \to Q$ that is a quotient of A by the action of $\mathrm{Aut}(A, \varphi)$ and satisfies some rationality conditions such as that Q is defined over $P(j(A, \varphi))$, where P is the prime field of k. We may give a definition later in the seminar, it is in [3]. If A has CM by K of a primitive CM type, then $\mathrm{Aut}(A, \varphi) = (\mathcal{O}_K^*)^{\mathrm{tor}}$.

Our second formulation of the main theorem of complex multiplication. *Given a CM field F with a CM type Ψ, let (K, Φ) be the reflex of (F, Ψ), let A be an abelian variety over a field $k \supset F$ with CM by $\mathcal{O}_K$ via ι of type Φ, and let $V : A \to Q$ be its normalized Kummer variety.*

Given an ideal $\mathfrak{b} \subset \mathcal{O}_K$, let $t \in A(\overline{k})$ be a point with annihilator $\mathfrak{b}$, and let b be the smallest positive integer in $\mathfrak{b} \cap \mathbf{Z}$.

Then $\mathrm{CM}_{F,\Psi}(\mathfrak{b}) = \mathrm{CM}_{F,\Psi}(V(t)) \subset \overline{k}$ is the same abelian extension of F as in the first formulation of the second main theorem.

Moreover, the Artin isomorphism

$$N \to \mathrm{Gal}(\mathrm{CM}_{F,\Psi}(\mathfrak{b})/\mathrm{CM}_{F,\Psi})$$

is given by

$$\psi(\mu)V(t) = V(\mu t)$$

for all $\mu \in N$.

Existence. Again, everything after 'let' really exists (as we will see) so that the theory of complex multiplication can actually construct the abelian extension

corresponding to $H_{F,\Psi}(\mathfrak{b})$.

The case $g = 1$. If A is an elliptic curve over a field of characteristic different from 2 and 3, then A has a model over $P(j(A))$ of the form $A : y^2 = x^3 + ax + b$. Let $n = \#\mathcal{O}_K^*/2$. We then have $Q = \mathbf{P}^1$ and V is the n-th power of the x-coordinate map.

In complex analytic terms, we can take this x to be

$$x_\tau(t) = \begin{cases} \frac{1}{g_3(\tau)}\wp(\tau,t)^3 & \text{if } g_2(\tau) = 0, \\ \frac{1}{g_2(\tau)}\wp(\tau,t)^2 & \text{if } g_3(\tau) = 0, \text{ and} \\ \frac{g_2(\tau)}{g_3(\tau)}\wp(\tau,t) & \text{otherwise,} \end{cases}$$

for every $t \in E(\mathbf{C}) = \mathbf{C}/(\mathbf{Z} + \tau\mathbf{Z})$.

For an imaginary quadratic field K of discriminant D and a positive integer b, let $\tau = \frac{1}{2}(\sqrt{D} + D)$. Recall that $\mathrm{CM}(b)$ is the ray class field of K for the modulus b. Then this shows that we have

$$\mathrm{CM}(b) = K(j(\tau), x_\tau(1/b)).$$

This gives a full solution to Kronecker's Jugendtraum for imaginary quadratic fields.

This result in the literature. In [3] ("Main Theorem 2 on page 118"), the fact that $\mathrm{CM}_{F,\Psi}(V(t))$ is the correct field is stated without the explicit Galois action, but the explicit Galois action is in the proof.

The assumption that Ψ is primitive is there, but can be removed as shown in [2].

References

[1] Serge Lang. *Complex Multiplication*, volume 255 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1983.

[2] Goro Shimura. On the class-fields obtained by complex multiplication of abelian varieties. *Osaka Math. J.*, 14:33–44, 1962.

[3] Goro Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998. Sections 1 – 16 essentially appeared before in Goro Shimura and Yutaka Taniyama, *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory*, Mathematical Society of Japan, 1961.