Complex Multiplication

Spring 2012 Junior Paper

David Corwin

0 Abstract

Class field theory describes the abelian extensions of a number field using the arithmetic of that field. The Kronecker-Weber theorem states that all abelian extensions of the rationals are contained in cyclotomic fields. As we know, cyclotomic fields can be generated by special values of the exponential function $e^{2\pi iz}$, and we call this the *theory of complex multiplication for G_m*. We would thus like to find other analytic functions whose special values generate abelian extensions of other number fields.

To see where to look, let us examine the exponential function more closely. It provides a group homomorphism from the Lie group $\mathbb{R}$ to the Lie group $\mathbb{R}/\mathbb{Z}$, or the unit circle in the complex plane, which is a real algebraic group. This map is also the universal covering map of the unit circle, and we thus call it a uniformization. It is the values of the exponential function at rational numbers that generate abelian extensions, and since the exponential is a homomorphism, this is the same as the torsion points of the unit circle. In other words, the coordinates of the torsion points generate abelian extensions of $\mathbb{Q}$.

We thus might like to take a general number field K, look at $K/\mathcal{O}_K$, and hope that (1) This can be seen as the torsion points of an algebraic group and (2) The torsion points generate the abelian extensions of K. In (1), we would take the full algebraic group to be $(K \otimes \mathbb{R})/\mathcal{O}_K$.

Unfortunately, in many cases, such an object would not turn out to be very nice. However, in the case of K an imaginary quadratic field, the quotient actually has a nice structure of an elliptic curve. This suggests that want to study torsion points of elliptic curves of the form $K \otimes \mathbb{R}/\mathcal{O}_K$, for K a quadratic imaginary field. As we have a group homomorphism $\mathbb{C} \to E$, where E is our

elliptic curve, given by holomorphic functions, the coordinates of torsion points will then come from the values of these holomorphic functions at rational points of $\mathbb{C} = \mathbb{R}^2$.

We thus begin the study of the complex multiplication of elliptic curves. Without motivation, we shall interpret this as the study of elliptic curves whose endomorphism rings contain orders in imaginary quadratic field. Afterward, we shall note that if K is replaced by a slightly more general number field, known as a CM field, we will get a (possibly higher-dimensional) abelian variety, and the study of the abelian variety will similarly yield information about class field theory.

We will sketch all of the proofs of the fundamental theorems concerning complex multiplication, making sure to at least capture the essential ideas behind the proofs. We hope to, most of all, motivate all of the steps in the proof. We will then explain how the proof in the case of abelian varieties of arbitrary dimension is very similar, but with more complications that must be dealt with.

The coverage of the theory for elliptic curves largely follows that of Silverman's textbook [9] as well as the similar notes by Ghath [1] and Rubin [6]. For abelian varieties, the discussion is based mostly on [4], with a bit of input from [3] and [7].

1 Notation

We summarize some of the notation defined in the text below.

For a number field K, we let Σ_K denote the set of finite places of K, Σ_K^∞ the set of infinite places, and $\overline{\Sigma_K}$ the set of all places. For each place v of K, we let K_v denote the completion at v, $\mathcal{O}_v$ its valuation ring, and U_v the group of units. For a prime p (or ℓ), we thus let U_p denote the p-adic units. We write valuations additively, always setting the valuation of a uniformizer to be 1. When we refer to an *absolute value* $||_v$, we are working multiplicatively, with the standard normalization relative to the given field. We let I_K denote the group of idèles of K, and if S is a finite set of places of K, we let $\mathbf{A}_K^{S,\times}$ denote the idèles supported outside S.

All fields, unless otherwise noted, have characteristic 0. If we say a field has "characteristic p," we are supposing $p > 0$ is a rational prime. If L/K is a Galois extension of fields, we let $G(L/K)$ denote its Galois group. If K is a field, then G_K denotes its absolute Galois group. If both are number fields, with w a place of L lying over a place v of K, we denote by $I(w/v) \subseteq D(w/v) =$

$G(L_w/K_v) \subseteq G(L/K)$ the decomposition and inertia groups, respectively, of w. If K is a field, then $\overline{K}$ denotes its algebraic closure (which is the same as the separable closure when K is perfect, the case we mostly consider). If $\mathfrak{p}$ is a prime of K, we let $(L/K, \mathfrak{p})$ denote the Frobenius of $\mathfrak{p}$ in $G(L/K)$, and we denote it by $(K, \mathfrak{p})$ when L is irrelevant.

We write V/K to denote that a variety V is defined over a field K. If σ is an automorphism of $\overline{(K)}$, then it sends V to $\sigma(V)$ by fibered product with $\mathrm{Spec}(K)$ over $\mathrm{Spec}(K)$, or equivalently, by applying σ to the coefficients of the equations used to define everything. If σ fixes K, then V is naturally isomorphic over K to $\sigma(V)$. If G/K is an algebraic group, we let $G(\overline{K})$ denote the K-rational points, and $E[m]$ denote the m-torsion points, over $\overline{(K)}$.

We shall freely use results from Silverman [10] without proof.

2 CM Elliptic Curves

2.1 Structure

Definition 2.1. An elliptic curve E/K is said to have *complex multiplication* by an imaginary quadratic field F if $\mathrm{End}_0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains a field isomorphic to F. Equivalently, $\mathrm{End}(E)$ is an order in F.

In characteristic 0, the containments above are automatically equal (while in characteristic p, the endomorphism ring might be slightly larger). For two elliptic curves E, E', we note $\mathrm{Hom}_0(E, E') := \mathrm{Hom}(E, E') \otimes_{\mathbb{Z}} \mathbb{Q}$. (Equivalently, it is the set of morphisms between the $\mathbb{Q}$-Hodge structures associated to E, E'.)

If R is an order in F, we say that E/K has *complex multiplication by R* if $\mathrm{End}(E)$ contains a copy of R. We shall restrict our attention to curves with complex multiplication by $\mathcal{O}_F$, with a remark at the end explaining how the results differ in the more general case. Thus, from now on, *complex multiplication by F* is synonymous with *complex multiplication by $\mathcal{O}_F$*.

2.2 Some O_F-modules

We recall briefly some facts from [10]. For an elliptic curve E/K with complex multiplication by F over F, we know that $\mathcal{O}_F$ acts linearly on $\mathrm{Tgt}_0(E)$ and

on $T_\ell(E)$ (equivalently, the étale homology $H_1(E, \mathbb{Z}_\ell)$), which are K- and $\mathbb{Z}_\ell$-modules of dimensions 1 and 2, respectively. Tensoring the latter with $\mathbb{Q}$, we get a $\mathbb{Q}_\ell$-linear action on $V_\ell(E)$.

As long as ℓ does not equal the characteristic of K, the action of $\mathcal{O}_F$ on $T_\ell(E)$ is faithful (and similarly, that of F on $V_\ell(E)$). In particular, $T_\ell(E)$ is a free $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-module of rank 1. If $\mathrm{End}(E)$ is larger than $\mathcal{O}_F$, $T_\ell(E)$ is still a faithful $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-module (and the same holds if we tensor everything with $\mathbb{Q}$).

Furthermore, if K has characteristic 0 and embeds in $\mathbb{C}$, we have the homology $H_1(E, \mathbb{Z})$, which is free of rank 2. Then $\mathcal{O}_F$ acts on this, making it into a module of rank 1, and F acts on $H_1(E, \mathbb{Q})$, which is free of rank 1. Note that the tangent space $\mathrm{Tgt}_0(E)$ of $E/\mathbb{C}$ is naturally isomorphic to $H_1(E, \mathbb{R})$, giving the latter a complex structure, as well as making it a free $F \otimes_{\mathbb{Q}} \mathbb{R}$-module of rank 1. Furthermore, $T_\ell(E) \cong_{\mathcal{O}_F} \mathbb{Z}_\ell \otimes_{\mathbb{Z}} H_1(E, \mathbb{Z})$.

Finally, dual to the action on the tangent space is the K-linear action on the holomorphic differentials, which is true as a differential is holomorphic iff it is translation invariant. In characteristic 0, every element acts faithfully (and in general, an element does not act faithfully iff it is inseparable). Note that, in particular:

Remark 2.2. An element of $\mathcal{O}_F$ is defined over KF as an endomorphism. Assuming K contains all conjugates of F, the action on the differential fixes an embedding $F \to K$. The Galois group acts on an element of F as if it were a true element of F, and not an endomorphism of an elliptic curve.

2.3 Classification

We would now like to classify such curves, up to isomorphism over $\mathbb{C}$. First, notice that if we take Γ to be any fractional ideal of $\mathcal{O}_F$, then $(\mathbb{R} \otimes_{\mathbb{Q}} F)/\Gamma$ is an elliptic curve with complex multiplication by F. Furthermore, it is clear that two fractional ideals differing by a principal ideal give isomorphic elliptic curves, as the lattices they define are proportional by an element of $\mathbb{C}^\times$. We would like to show that this gives a bijection between the set of ideal classes of $\mathcal{O}_F$ and the isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}_F$.

Proposition 2.3. *(1) Every elliptic curve with complex multiplication by $\mathcal{O}_F$ arises in the manner above*
(2) If two elliptic curves are isomorphic, then any two ideals defining them are in the same ideal class

In particular, there is a bijection between the ideal classes of $\mathcal{O}_F$ and the (isomorphism classes of) elliptic curves with complex multiplication by $\mathcal{O}_F$.

Proof. Note that any elliptic curve can be represented by a lattice generated by 1 and $\tau \in \mathcal{H}$. Then it is clear that $\tau \in F$. We can then scale the lattice by an integer m so that $m\tau \in \mathcal{O}_F$. Then since $\mathcal{O}_F$ sends the lattice to itself, the lattice is now an ideal of $\mathcal{O}_F$, which shows that the lattice is an ideal. This proves (1).

Then if two curves are isomorphic, meaning the lattices are related by scaling, then this factor must be in $F^\times$, so the two ideals are in the same class. □

We let $\mathcal{E}_F$ denote the set of isomorphism classes of elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_F$.

Note that, if we want to associate an ideal to E more intrinsically, $H_1(E, \mathbb{Z})$ is an $\mathcal{O}_F$-module, and ideal classes correspond bijectively to isomorphism classes of rank 1 projective (torsion-free) modules over $\mathcal{O}_F$.

Now that we have established a bijection between isomorphism classes of such elliptic curves and the ideal class group of $\mathcal{O}_F$, we recall class field theory gives us an isomorphism between the latter set and $G(H/F)$, where H is the Hilbert class field of H. We will now proceed to show that there is a direct bijection between $G(H/F)$ and these isomorphism classes, given by the Galois action on these curves.

Also note that given this bijection, we can think of it as a simply-transitive action of $Cl(\mathcal{O}_F)$ on $\mathcal{E}_F$. It takes a few simple details to check that the action can be described by multiplying a lattice $\Gamma \subseteq \mathbb{C}$ by an ideal $\mathfrak{a}$, i.e. $\mathfrak{a}\Gamma \subseteq \mathbb{C}$.

We prefer, however, to let ideals act by their inverse. Thus if $[\mathfrak{a}]$ denotes an ideal class, and E an elliptic curve with CM and lattice Γ, we let $[\mathfrak{a}] * E$ denote the elliptic curve with lattice $\mathfrak{a}^{-1}\Gamma$. If $E = \mathbb{C}/\mathcal{O}_F$, then we let the ideal class $[\mathfrak{a}]$ correspond to the elliptic curve $[\mathfrak{a}] * E$. *Note that this differs from the convention used until this point.*

3 Galois Action

We recall that over a field K, automorphisms of K act on the set of isomorphism classes of elliptic curves over K by acting on their coefficients. We also recall that if K is algebraically closed, we can associate to each elliptic curve E/K an element $j(E) \in K$, and that the j-invariant classifies elliptic curves up to isomorphism over K. As the j-invariant is defined as a polynomial in the

coefficients of E, the action of automorphisms translates to an action on teh j-invariant.

By symmetry, if σ is an automorphism of $\mathbb{C}$ and E a CM elliptic curve over $\mathbb{C}$, then $\sigma(E)$ has the same CM. Since there are finitely many isomorphism classes of elliptic curves with CM by a given ring over $\mathbb{C}$, there are finitely-many possible j-invariants. In particular, $j(E)$ has finitely many conjugates over $\mathbb{Q}$, hence is algebraic of degree at most $Cl(\mathcal{O}_F)$. Furthermore, as we can take K above to be $\overline{\mathbb{Q}}$, we can work with isomorphism over $\overline{\mathbb{Q}}$ instead of $\mathbb{C}$.

4 Algebraic Description of the Ideal Action

For each elliptic curve $E \in \mathcal{E}_F$, we have a map $f_E : G_F \to Cl(\mathcal{O}_F)$ given by $\sigma \mapsto [\mathfrak{a}]$ such that $\sigma(E) \cong [\mathfrak{a}] * E$. We would like to show that this is independent of E and is a homomorphism. The latter follows fairly easily from the former:

Proposition 4.1. *For $E \in \mathcal{E}_F$, define a map $f_E : G_F \to Cl(\mathcal{O}_F)$ by $\sigma \mapsto \sigma(E)$. Suppose that f_E is independent of E (and we denote it by f). Then this map is a homomorphism from G_F to $Cl(\mathcal{O}_F)$.*

Proof. Let $\sigma, \tau \in G_F$, and let E correspond to the trivial element of $Cl(\mathcal{O}_F)$. Then

$$\begin{aligned} f_E(\sigma \circ \tau) * E &= E^{\sigma\circ\tau} \\ &= (f_E(\tau) * E)^{\sigma} \\ &= f_{E^\tau}(\sigma) * (f_E(\tau) * E) \\ &= f_{E^\tau}(\sigma) f_E(\tau) \end{aligned}$$

Since $f_E = f_{E^\tau}$, the map f is a homomorphism. □

We would like to show that the action of the ideal class group of F commutes (in some sense) with the Galois action on our elliptic curve, which will give us what we want. We run into a difficulty because the ideal action is defined analytically, while the Galois action is algebraic. We will resolve this difficulty in the current section. First, we give an intuitive account, then sketch a rigorous proof. We will give a complete proof in the section on abelian varieties, as the theory is almost identical.

Let $\mathfrak{a}$ be an integral ideal of F, and write E as $\mathbb{C}/\Gamma$, for a lattice Γ. Then $\mathfrak{a}^{-1}\Gamma$ is a sublattice of Γ, meaning that $E' := \mathbb{C}/\mathfrak{a}^{-1}\Gamma$ is a quotient of E by

$\mathfrak{a}^{-1}\Gamma/\Gamma$. These are the points of E that vanish under the action of $\mathfrak{a}$, or $E[\mathfrak{a}]$. Notice that $E' = [\mathfrak{a}] * E$.

We can thus simply take the quotient by this subgroup, as described in [10], Chapter III, 4.12. Note that because all CM elliptic curves and morphisms between them are defined over $\overline{\mathbb{Q}}$, we know that if we have what we want analytically, we also have what we want algebraically.

Furthermore, we remark that if $\mathfrak{a}$ is a non-integral fractional ideal, we can still define $E \to E' = [af] * E$, but this morphism will only be in $\mathrm{Hom}_0(E, E')$, not $\mathrm{Hom}(E, E')$.

We now would like to point out that while the isomorphism class of E' above depends only on the class of $\mathfrak{a}$, the quotient map $f : E \to E'$ depends on the ideal $\mathfrak{a}$ itself. Following Milne [4], we formalize this by calling a pair $(E', f : E \to E')$ inducing the above on complex points an $\mathfrak{a}$-*multiplication*. However, we remark that an $\mathfrak{a}$-multiplication is unique up to isomorphism (an isomorphism of the pair (E,f)), so it might be more appropriate to call it *the* $\mathfrak{a}$-multiplication.

Alternatively, we can give the following more abstract definition of an $\mathfrak{a}$-multiplication (which has the advantage of working in characteristic p):

Definition 4.2. For an elliptic curve E with complex multiplication by F and a fractional ideal $\mathfrak{a}$ of F, we call an elliptic curve $E^{\mathfrak{a}}$ and a map $f^{\mathfrak{a}} : E \to E^{\mathfrak{a}}$ an $\mathfrak{a}$-*multiplication* if $a : E \to E$ factors through $f^{\mathfrak{a}}$ iff $a \in \mathfrak{a}$. Note that we allow ourselves to consider $\mathfrak{a}$ non-integral, in which case $f^{\mathfrak{a}}$ but in this case, "factors through" means that the associated morphism $E^{\mathfrak{a}} \to E$ is an actual homomorphism.

It is clear from this definition that the natural projection $E \twoheadrightarrow E/E[\mathfrak{a}]$ is an $\mathfrak{a}$-multiplication.

We also note that an isogeny $f : E \to E'$ that commutes with F is automatically an $\mathfrak{a}$-multiplication for some $\mathfrak{a}$. We only need note that E, E' can be uniformized as $H_1(E, \mathbb{R})/H_1(E, \mathbb{Z}), H_1(E', \mathbb{R})/H_1(E', \mathbb{Z})$, respectively, and that the subset of F sending $f_*^{-1}(H_1(E', \mathbb{Z})) \subseteq H_1(E, \mathbb{R})$ into $H_1(E, \mathbb{Z})$ is a fractional ideal of F. Conversely, every $\mathfrak{a}$-multiplication is an isogeny that commutes with F (equivalently, with $\mathcal{O}_F$). Of course, it is only in characteristic p that we have to worry about commuting with F.

Furthermore, the cokernel of the mapping $f_* : H_1(E, \mathbb{Z}) \to H_1(E', \mathbb{Z})$ is the degree of the isogeny, which is the same as $[\mathcal{O}_F : \mathfrak{a}]$ (note that this can be defined in an obvious way even if $\mathfrak{a}$ is not integral).

We then have the following properties, which are intuitively obvious from the complex analytic theory, and not too hard to prove algebraically. We state them without proof, noting that the proof recalls the fact that $\mathrm{Hom}_{\mathcal{O}_F}(\mathfrak{a}, \mathfrak{b}) \cong_{\mathcal{O}_F} \mathfrak{b}\mathfrak{a}^{-1}$.

Proposition 4.3. *(1) An isogeny $f : E \to E'$ is an $\mathfrak{a}$-multiplication if every $a \in \mathfrak{a}$ factors through f, and its degree is (at least) $[\mathcal{O}_F : \mathfrak{a}]$*
(2) Multiplication by $\alpha \in F$ is an (α)-multiplication
(3) $f^{\mathfrak{a}}$ factors through $f^{\mathfrak{a}'}$ iff $\mathfrak{a}' \subseteq \mathfrak{a}$
(4) A composition of an $\mathfrak{a}$-multiplication with an $\mathfrak{a}'$-multiplication is an $\mathfrak{a}\mathfrak{a}'$-multiplication
(5) If $f : E \to E'$ is an $\mathfrak{a}$-multiplication, then precomposition with $f \circ \alpha \in \mathrm{Hom}(E, E')$ iff $\alpha \in \mathfrak{a}^{-1}$, and this determines an isomorphism from $\mathfrak{a}^{-1}$ to $\mathrm{Hom}(E, E')$ as $\mathcal{O}_F$-modules. By (4), this means that $\mathrm{Hom}(E^{\mathfrak{a}}, E^{\mathfrak{b}}) \cong \mathfrak{a}\mathfrak{b}^{-1}$ (note the error in [4], 1.33(a)!)

Remark 4.4. We make a remark about canonicity. The notion of $\mathfrak{a}$-multiplication is unique *up to isomorphism*, so anything that is invariant under isomorphism can make use of *the* $\mathfrak{a}$-multiplication. However, this is not the case for everything, and we will need to note this later on. Notice that when we define an $\mathfrak{a}$-multiplication of E by choosing a uniformization $\mathbb{C}/\Gamma \to E$, the choice of uniformization is itself canonical only up to isomorphism, which is where the ambiguity appears. We could, however, define $[af] * E$ as $H_1(E, \mathbb{R})/\mathfrak{a}^{-1}H_1(E, \mathbb{Z})$.

Also note that if $\alpha \in F^\times$, then $\alpha : E \to E$ is an (α)-multiplication, so in some sense, the embedding $F^\times \hookrightarrow \mathrm{End}_0(E)$ gives us an isomorphism $E \cong E^{(\alpha)}$.

We briefly remark that taking quotients in the case of abelian varieties of arbitrary dimension is more difficult. We will thus take a different approach to define $\mathfrak{a}$-multiplications in the section on abelian varieties, one that we could have taken here. In [9], this approach is taken in the case of elliptic curves.

5 The J-Invariant is Integral

In terms of showing that j is integral, it is clear that is suffices to show that an elliptic curve with complex multiplication has good reduction. To do this, we show that the action on the Tate module is abelian, so up to finite index, the inertia group is pro-p. Then ℓ-adic groups are locally (up to finite index) pro-ℓ, so we are done.

Theorem 5.1. *If E is an elliptic curve with complex multiplication, then $j(E)$ is an algebraic integer.*

Proof. According to [10] Chapter VII, the j-invariant is integral iff E has potentially good reduction at all primes. To show it has potentially good reduction, note that, by the criterion of Néron-Ogg-Shafarevich, good reduction at $\mathfrak{p}$ is equivalent to the inertia group acting trivially on the Tate module $T_\ell(E)$ (or $V_\ell(E)$) for some $(\ell) \neq \mathfrak{p} \cap \mathbb{Z}$, hence potentially good reduction is equivalent to acting through a finite quotient.

But after passing to an extension, Galois group elements act $\mathcal{O}_F$-linearly, hence $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-linearly. As $T_\ell(E)$ is a rank 1-module over this, and we can choose ℓ that does not split in F (hence $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is a field, and $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is the ring of integers in it), the Galois group acts as multiplication by elements of $(\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^\times$, as the module is free of rank 1). But this group is locally a pro-ℓ group by the ℓ-adic logarithm, and we know from local class field theory (which we can apply because we now know the action is abelian) that the inertia group is locally pro-p (where $(p) = \mathfrak{p} \cap \mathbb{Z}$), so after passing to a finite extension, the inertia group must act trivially, as the action is continuous. □

Note that in [9], there is a more elementary, albeit longer, proof of this fact.

Because of the above fact, and because $\mathbb{Q}(i\sqrt{163})$ has class number 1, we find that $j(\frac{1+i\sqrt{163}}{2}) \approx e^{\pi\sqrt{163}}$ is an integer. Notice that we derived this remarkable fact about an infinite series using a significant amount of algebra.

6 The J-Invariant Generates the Hilbert Class Field

We just have a little bit more work to show that this homomorphism is surjective and is the one given by class field theory.

We recall that the Artin reciprocity isomorphism is given by sending a prime ideal to its Frobenius element. We thus require a method of relating the quotient map $E \to [\mathfrak{p}] * E$ to the action of the Frobenius element. In brief, we do this by reducing modulo $\mathfrak{p}$. Then the Frobenius action of Galois reduces the Frobenius modulo $\mathfrak{p}$, which is an algebraic map in addition to a Galois-theoretic map. We then note that the map above will be inseparable modulo $\mathfrak{p}$, hence will factor through the Frobenius element, and this will essentially give us what we want. We make this precise below:

Theorem 6.1. *Let H denote the Hilbert class field of F. Then $H = F(j(E))$, for any $E \in \mathcal{E}_F$, hence $f : G_F \to Cl(\mathcal{O}_F)$ factors through $G(H/F)$. Further-*

more, the induced map $G(H/F) \to Cl(\mathcal{O}_F)$ is Artin reciprocity isomorphism (and hence $\{j(E) \mid E \in \mathcal{E}_F\}$ is a full set of conjugates over F).

Proof. Let L be a field over which all the j-invariants are defined. We will hope to show that $L = H$, but for the moment, we only know it is an extension of F. We have an induced map $G_F \to Cl(\mathcal{O}_F)$, which factors through $G(L/F)$. Note that the map $G(L/F) \to Cl(\mathcal{O}_F)$ is injective, since if an automorphism induces a principal ideal, then it acts trivially on the j-invariants, hence fixes L.

Suppose p is a rational prime that splits completely in F and for which everything else works nicely, i.e. there is a prime $\mathfrak{P}$ of L over p such that all of $\mathcal{E}_F$ has good reduction over L, there is no ramification in L, isomorphic reduction implies isomorphic curves (equivalently, none of the differences between the j-invariants of curves in $\mathcal{E}_F$ are in primes over p). Let $\mathfrak{p}$ be a prime of F over p.

Then the $\mathfrak{p}$-multiplication $E \to [\mathfrak{p}] * E$ has degree p, hence so does its reduction. If we can show that its reduction is inseparable, then it must be the Frobenius map, as an inseparable map factors through the Frobenius map.

Let us first derive a few consequences, assuming we know this fact. We recall that the set of primes of degree 1 over $\mathbb{Q}$, with a finite set of primes thrown out, has density 1. Thus their Frobenius elements saturate $G(L/K)$. This shows that the map $G(L/K) \to Cl(\mathcal{O}_F)$ is in some sense the Artin map, but of course, we don't actually know that L is the appropriate field. Of course, this does tell us that a prime splits completely in L iff it is principal, which shows that $L = H$. Then the above shows that the map is the Artin reciprocity map.

Now, why is the map $E \to \mathfrak{p} * E$ inseparable? If it were principal, then the map would be (after composing with an isomorphism between $\mathfrak{p} * E$ and E) multiplication by an element in $\mathfrak{P}$, hence would induce the trivial map on the tangent space modulo $\mathfrak{P}$, hence would be inseparable. However, we don't know this. Of course, we can do the following. We know by the density theorem that there is another prime $\mathfrak{a}$ of F such that $\mathfrak{p}\mathfrak{a}$ is principal, and $\mathfrak{a}$ is prime to p. Then the composition of an $\mathfrak{a}$-multiplication with a $\mathfrak{p}$-multiplication gives us, after composing with an isomorphism between $\mathfrak{a}\mathfrak{p} * E$ and E, multiplication by an element of $\mathfrak{p}$, hence an inseparable map. Hence, if we show that an $\mathfrak{a}$ multiplication is separable, this shows that a $\mathfrak{p}$-multiplication must be inseparable.

We prove this latter fact by noting we can also find $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}$ is principal and prime to p. Thus it induces a nontrivial map on the tangent space modulo $\mathfrak{P}$, hence is separable, so an $\mathfrak{a}$-multiplication is separable. □

6.1 The Case of Non-Maximal Orders

Just for this subsection, we relax the assumption that our CM elliptic curves have CM by $\mathcal{O}_F$, and suppose that E has CM by R, an order in F. Then it's not too hard to conclude that isomorphism classes of elliptic curves with CM by R are in bijection with $Cl(R)$ (see [5], Chapter I, §12, for the theory of class groups of orders). This can be viewed as a quotient of a certain ray class group, hence corresponds to an abelian extension. We then might expect that the j-invariants of these isomorphism classes constitute a set of conjugates for this abelian extension, and the Galois group acts via the Artin isomorphism as the class group. This is indeed the case, and the proof is almost identical, involving reduction modulo a prime.

Since we now are considering abelian extensions with ramification, can we use these to generate all the abelian extensions of F? I.e., does $\{j(\tau) \mid \tau \in F\}$ generate F^{ab}. The answer lies in the theory of $Cl(R)$ for orders R of F (hence is not a question of complex multiplication), and the answer is no. However, if we adjoin all of these j-values and all of the roots of unity, we get an extension that differs from F^{ab} by a product of groups of order 2, as mentioned in [7].

7 Torsion Points and Ray Class Fields

So far, what we have done does not have any analogue in the theory of complex multiplication for G_m. In that case, $\mathbb{Q}$ has class number 1, and there is only one isomorphism class of the multiplicative group. We would now like to generate ray class fields (i.e. not just the Hilbert class field) using torsion points. For a modulus $\mathfrak{m}$ of F, we let $L_{\mathfrak{m}}$ denote the ray class field of modulus $\mathfrak{m}$ and $Cl_{\mathfrak{m}}(\mathcal{O}_F) := \mathbb{I}_F^{\mathfrak{m}}/\iota(F_{\mathfrak{m},1})$ the ray class group

We hope that, as in the case of G_m, the points $E[\mathfrak{m}]$ generate the ray class field $F_{\mathfrak{m}}/F$. Furthermore, supposing this, we might hope that the Galois action of $G(F_{\mathfrak{m}}/F)$ on these points corresponds to an action of the ideals.

We thus divide what we're looking for into two things:
(1) Show that the torsion points generate the ray class fields
(2) Show that the Galois action on the torsion points is the same (via the Artin isomorphism) as the action of ideals

From what we have seen in generating the Hilbert class field, we might expect that something like (2) will allow us to conclude (1). First, we make a point about (1):

7.1 Weber Functions

Let us forget about non-principal ideals for the moment, or equivalently, we are looking for the action of $G(F_{\mathfrak{m}}/H)$. Then $F^{\times}$ acts on these points, and $F_{\mathfrak{m},1}$ acts trivially on $E[\mathfrak{m}]$, suggesting we are going in the right direction. The problem is that class field theory relates $G(F_{\mathfrak{m}}/H)$ to *ideals*, not elements of $F^{\times}$, so we want the units of F to act trivially. We recall that the units are the same as automorphisms of E, so we essentially want to generate the ray class field not using the torsion points themselves but using something invariant under the action of automorphisms. We are thus led to the notion of Weber functions.

In other words, we would somehow like to express the quotient of E by its automorphisms.

When F is not either $\mathbb{Q}[i]$ or $\mathbb{Q}[i\sqrt{3}]$, the only automorphism is $[-1]$. Thus the map sending a point of E to its x-coordinate under some Weierstrass model serves precisely this purpose. Furthermore, two points have the same x-coordinate iff they are related by an automorphism. In the case of the two special F, we can take x^2 and x^3, respectively. We thus hope that these will generate the ray class field.

Note, however, that this depends on the Weierstrass model. We can fix this by taking some multiple of x (or x^2, x^3) that depends on the Weierstrass model. As mentioned in [10], change of variables between Weierstrass equations can only take very specific forms. We are thus led to conclude that if our Weierstrass equation is $y^2 = 4x^3 - g_2x - g_3$, then

$$\frac{g_2g_3x}{\Delta}$$

is independent of model, with similar formulas in the two exceptional cases. We call this the *Weber function* of E. We denote the Weber function by h.

Notice that the Weber function is invariant under isomorphism of elliptic curves. This is very powerful, as we do not have to worry whether any of our isomorphisms are canonical when we are looking only at the Weber function. In fact, we could have motivated the Weber function by saying that we needed something more instrinsic, since, after all, the coordinates of points of E depend on an embedding $E \hookrightarrow \mathbb{P}^2$. This is also useful because $\mathfrak{a}$-multiplications are defined up to isomorphism, but the Weber function is invariant under isomorphism.

Finally, note that in each of the cases above, it is easy to see that IF $h(P) = h(P')$ where $P, P' \in E(K)$, then there is an automorphism of E taking P to P'. We can think of the Weber function as the quotient map $E \to E/\mathrm{Aut}(E)$.

Remark 7.1. As this is a function on E, we can of course think of it as a periodic function on $\mathbb{C}$. This was originally used when complex multiplication was formulated in terms of analytic functions.

7.2 The Theorem for Torsion Points

We will respond to (2) in this section. In the proof in the last section, we showed that a certain $\mathfrak{a}$-multiplication was the same as a Frobenius map when reduced modulo a prime. To bring this back up to our global field, we used only primes that did not divide the product of the differences of the j-invariants of elliptic curves with complex multiplication by $\mathcal{O}_F$. Thus, if two elliptic curves were isomorphic modulo a prime, they were also isomorphic globally. In order to avoid losing information on torsion points when reducing modulo a prime, we recall [10], Chapter VII, 3.1, which states that at a good prime relatively prime to m, then reduction is injective on $E[m]$. We therefore see that without much more effort, we can prove the following theorem:

Theorem 7.2. *Let $\mathfrak{m}$ be an integral ideal of $\mathcal{O}_F$. Then $F(j(E), h(E[\mathfrak{m}])$ is the ray class field $L_\mathfrak{m}$ of F, and the action of G_F on these values of the Weber function corresponds, inversely via the Artin reciprocity isomorphism, so the action of $\mathbb{I}_F^\mathfrak{m}/\iota(F_{\mathfrak{m},1})$.*

Proof. First, we make a note about how a non-principal ideal acts on the torsion points. We recall that if $a \in F^\times$, then multiplication by a is an (a)-multiplication. Therefore, we replace endomorphisms of E by multiplications corresponding to the ideals they generate. Since $\mathfrak{a}$-multiplications are unique up to isomorphism, this is not a problem when we are considering values of the Weber function. However, see the remark below.

We sketch the ideas of the proofs.

As with the Hilbert class field, we have a map from G_F to a class group. This time, we care about the isomorphism class of the elliptic curve as well as the torsion points, so only elements of $\iota(F_{\mathfrak{m},1})$ act trivially. Thus our homomorphism is to $Cl_\mathfrak{m}(\mathcal{O}_F)$.

Next, we use an almost identical argument as in Theorem 6.1, but this time we only use primes $\mathfrak{p}$ that are prime to $\mathfrak{m}$. This ensures that the reduction modulo our prime of $E[\mathfrak{m}]$ is injective, while only throwing out finitely-many primes. Thus we find, first of all, that the values of the Weber function generate precisely $L_\mathfrak{m}$, and furthermore, that the Galois action is given by the Artin isomorphism. □

Remark 7.3. We note that, while the above is dependent on the Weber function, we can formulate this theorem in a way that avoids use of the Weber function. This will essentially mean that we will have an $\mathfrak{a}$-multiplication that agrees with σ on the $\mathfrak{m}$-torsion and such that $(L_{\mathfrak{m}}/F, \mathfrak{a}) = \sigma$. The reason this can still exist is because an $\mathfrak{a}$-multiplication is defined only up to isomorphism. In the section on abelian varieties, we will in fact formulate the fundamental theorem in exactly this manner.

8 Adelic Formulation

We remark that the results above depend in a certain sense on $\mathfrak{m}$. However, we recall class field theory can be formulated by taking the inverse limit over all the $\mathfrak{m}$, allowing us to express the Artin reciprocity law as an isomorphism between a certain group and all of ${G_F}^{ab}$. This approach involves adeles. In the case of complex multiplication, we can certainly take the inverse limit over all the $\mathfrak{m}$. More specifically, though, we would like to blend this with the adelic formulation of class field theory. This would allow us to describe the action of ${G_F}^{ab}$ on all of the torsion points at once. If we are to do this, we thus need to describe the action of the ideles on the torsion points of E.

Note that the torsion points are in correspondence with $H_1(E, \mathbb{Q})/H_1(E, \mathbb{Z})$. If we choose a uniformization that identifies F with $H_1(E, \mathbb{Q})$ and $H_1(E, \mathbb{Z})$ with a fractional ideal $\mathfrak{a}$ of F, then the torsion points correspond to $F/\mathfrak{a}$.

Since F is totally imaginary, the (idelic) Artin map depends only on the finite ideles. One can show that a torsion module is the direct sum of its $\mathfrak{p}$-primary components for primes $\mathfrak{p}$. Since both correspond to Laurent tails at $\mathfrak{p}$, the $\mathfrak{p}$-primary component is equal to $F_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}$, hence

$$F/\mathfrak{a} \cong \oplus_{\mathfrak{p}} F_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}.$$

Of course, there is also a map from the finite adeles $\mathbf{A}_{F,f}$ to this direct sum by mapping each component, so this allows the adeles to act on it. Note that if x is an idele, then x maps $\mathfrak{a}$ to $(x)\mathfrak{a}$, where (x) is the ideal generated by x. Thus x determines a map $F/\mathfrak{a} \to^x F/(x)\mathfrak{a}$.

Thus a choice of uniformization determines an action of the ideles on the torsion points of E.

We then have the following theorem:

Theorem 8.1. *Let E be an elliptic curve and $f : \mathbb{C}/\mathfrak{a} \to E$ a uniformization.*

Let s be an idele of F and σ an automorphism of $cl(F)$ whose restriction to F^{ab} is the Artin map applied to s. Then there is a unique uniformization

$$f' : \mathbb{C}/s^{-1}\mathfrak{a} \to \sigma(E)$$

such that s^{-1} agrees with σ on torsion points.

Proof. First, we quickly remark that f' is unique, as the torsion points are dense.

The most difficult part of this is unraveling the definition of the idelic Artin map. If L/F is an abelian extension, then L is contained in some ray class field $L_{\mathfrak{m}}$. The idelic Artin map then sends uniformizers at primes unramified in $L_{\mathfrak{m}}$ (not dividing $\mathfrak{m}$) to the corresponding Frobenius elements, and the rest is covered by declaring that $F^{\times}$ is in the kernel of the Artin map.

We suppose we are considering a model defined over H. We will choose $m \geq 3$ and then show the maps agree on $E[m]$. The result follows by noting that m was arbitrary. Let L be a field containing all of $E[m]$ and H. Now we chooose a prime ideal $\mathfrak{p}$ of F of degree 1 over $\mathbb{Q}$ that is prime to m, unramified, such that E has good reduction at a prime $\mathfrak{P}$ of L above $\mathfrak{p}$, and whose Frobenius elements in $G(L/K)$ is the restriction of σ to L. (This exists by Chebotarev Density.)

Let π be an idele whose component at $\mathfrak{p}$ is a uniformizer, and whose other components are trivial. Then we know that π is sent to the same element as s under the Artin map to $G(L_m/K)$ (as L contains the ray class field L_m), so $s = \pi a u$, where $a \in F^{\times}$ and u is congruent to 1 modulo m and is a unit at every prime.

Thus the ideal generated by s is in the same ideal class as $\mathfrak{p}$, so $\mathbb{C}/s^{-1}\mathfrak{a}$ really is isomorphic to $\sigma(E)$. We have a natural uniformization $\mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \to \sigma(E)$ (the $\mathfrak{p}$-multiplication), and composing with multiplication by a, we get a uniformization $\mathbb{C}/s^{-1}\mathfrak{a} \to \sigma(E)$.

Then the reduction argument in the previous section shows that using the "natural" uniformization, π acts as σ, hence πa acts as σ on $E[m]$, when acting under the uniformization above. Then note that u acts trivially on $E[m]$, so this proves the result for $E[m]$.

Then we just remark that a depended on m. One thus needs to make remark about the dependence on $\mathfrak{p}$ to show that f' is independent of m, taking into account units of $\mathcal{O}_F$ that are in $F_{m,1}$. This step then completes the proof. □

We also remark that the adelic formulation is mostly a formalism at this point, as it is merely a way of rephrasing the above action. It is most useful in the Langlands formulation, in which adelic points of algebraic groups appear frequently.

9 Abelian Varieties

We will now describe the theory of complex multiplication on abelian varieties, which is a generalization of that for elliptic curves. The theory is similar in many ways: we (roughly) describe the class field theory of a field of endomorphisms of our abelian variety using torsion points of that abelian variety, and abelian varieties with torsion structure will correspond to generalized ideal classes. The proofs are also similar: we reduce to a residue field, and then we end up with an inseparable endomorphism resulting from an ideal- (or idele-)theoretic construction, which then must be equal to a certain Frobenius endomorphism, giving us the connection between our abelian variety and the Artin reciprocity map.

On the other hand, we will see that the results (and hence the proofs) are more difficult to state. This is true for a few reasons
(1) The geometry of higher-dimensional algebraic varieties is more difficult (i.e. we cannot use the theory of curves)
(2) The endomorphism ring can be more more complicated than an order in an imaginary quadratic field (and hence the need to introduce the notion of a CM-type)

For (1), we will mainly need to a cite a few basic (and fairly intuitive) results from the theory of abelian varieties. As for (2), the endomorphism ring, when tensored with $\mathbb{Q}$ has many embeddings into $\mathbb{C}$, and we will need to take these all into account, developping the notion of a CM-type. Furthermore, the endomorphisms might not even form a field, but rather a product of fields, and we will have to develop an auxiliary field, known as the reflex field, which is the field whose class field theory is reflected in the arithmetic of the abelian variety.

We will very soon classify abelian varieties with CM, and it is here that (2) will appear. This classification will immediately make apparent the need for the notion of CM-type. Afterward, we will see that the proofs are very similar to those in the case of elliptic curves, differing only in that we will constantly have to make reference to algebraic construction related to CM types, and that we will not be able to use the theory of curves.

First, we discuss basic properties of CM abelian varieties.

10 Abelian Varieties with Complex Multiplication

In the case of elliptic curves, we know the endomorphism ring (over $\mathbb{Q}$ for this discussion) an algebra of degree at most 4 because it acts faithfully on the rational cohomology, and it is a field since it acts faithfully on the one-dimensional vector space of holomorphic 1-forms, hence of degree at most 2. We then say an elliptic curve has *complex multiplication* when this maximal degree is attained.

In the case of abelian varieties of dimension g, we know that the endomorphisms act faithfully on the cohomology, which is of rank $2g$, as well as on the holomorphic 1-forms, which is of rank g (but possibly over a field larger than $\mathbb{Q}$). However, the endomorphism ring, for a gth power of an elliptic curve, for example, contains at least $\mathrm{GL}_g(\mathbb{Q})$, which is of dimension g^2 over $\mathbb{Q}$, hence can grow much larger than $2g$. But such an algebra is fairly uninteresting to us, at least as class field theory goes.

However, for a semisimple K-algebra, there is a notion of *reduced* degree, which can be defined as the smallest dimension of a faithful representation of that algebra. The concrete idea is that a semisimple algebra decomposes as a sum of simple algebras, which are matrix algebras over a division ring over K. Each matrix algebra thus has dimension n^2 for some positive integer n, and then the reduced degree considers n instead of n^2. Thus $\mathrm{M}_n(D)$ has degree $n[D:K]$, which makes sense given the above definition, as it acts faithfully on D^n.

We therefore know that the reduced degree of $\mathrm{End}_0(A)$ as a $\mathbb{Q}$-algebra *is* less than $2g$ (assuming it is semisimple, which one can show using properties of the Rosati involution). We thus wish to define an abelian variety with complex multiplication as one such that the reduced degree of its endomorphism algebra is equal to $2g$.

Before going forward, one remark is in order. One can show without much trouble that the largest étale subalgebra of a semisimple algebra has degree equal to the reduced degree. Thus we could say that every étale subalgebra of $\mathrm{End}_0(A)$ has degree at most $2g$ over $\mathbb{Q}$, and complex multiplication is when we have an étale subalgebra of largest possible degree. In some sense, we could have simply taken this as the definition from the start, since it's not surprising to think that we are most interested in étale algebras as endomorphism rings.

Definition 10.1. For an abelian variety A of dimension g, the any étale subalgebra of the endomorphism ring has rank at most $2g$ over $\mathbb{R}$ in characteristic 0. When this rank is achieved, we say the abelian variety has *complex multiplication* or is a *CM abelian variety.*

10.1 CM-Algebras

While in the case of elliptic curves, this is always an order in a field, it can only be described as an order in an etale algebra (finite product of separable field extensions) over $\mathbb{Q}$ in the general case. More specifically, we have the following:

Definition 10.2. A *CM-field* E is a totally imaginary degree 2 extension of a totally real field (hence obtained by adjoining the square root of a totally negative element). A *CM-algebra* E is a finite product of CM-fields (often viewed as a $\mathbb{Q}$-algebra).

Note that this means that E has a unique complex conjugation, which, as in [4], we denote by ι_E. This is the unique automorphism fixing the product of the totally real subfields of E.

We then note:

Fact 10.3. If A is a CM abelian variety, then the largest étale subalgebra of $\mathrm{End}_0(A)$ is automatically a CM-algebra E, and $E \cap \mathrm{End}(A)$ is an order in E.

From now on, we suppose that all CM abelian varieties have $\mathcal{O}_E$, the maximal order, as part of their endomorphisms. This serves to simplify certain proofs and avoid recourse to rings that are not Dedekind or a product of Dedekind domains.

When we talk about an abelian variety A with CM by E, we are thinking of E as a subring of $\mathrm{End}_0(A)$*, not as a ring on its own. In other words, we are fixing an embedding* $E \hookrightarrow \mathrm{End}_0(A)$.

Furthermore, if we refer to a CM abelian variety A/K and an automorphism σ of $\overline{(K)}$, then we assume the embedding $E \hookrightarrow \mathrm{End}_0(\sigma(A))$ comes from composition of σ with $E \hookrightarrow \mathrm{End}_0(A)$. In particular, if σ fixes K, then σ commutes with the action of E on $A = \sigma(A)$.

This is important, as we could theoretically twist the embedding by an automorphism of $E/\mathbb{Q}$.

10.2 Lattice Ideals

We make some quick remarks on the algebraic number theory of $\mathcal{O}_E$, since this is not particularly standard material. We note that $\mathcal{O}_E$ is simply the product

of the integer rings of the direct factors of E, and most of the number theory is basically the product of the number theory of each of the direct factors. We note that there are numerous ideals of $\mathcal{O}_E$ corresponding to only a subset of the direct factors of E. We thus note the following definition:

Definition 10.4. We call an ideal $\mathfrak{a} \subseteq \mathcal{O}_E$ a *lattice ideal* if it contains an element of $E^\times$. Equivalently, it is a lattice in $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{R}$. Equivalently, it is an ideal whose rank over $\mathbb{Z}$ is the same as that of $\mathcal{O}_E$.

We extend this definition to include multiples of lattice ideals by elements of $E^\times$, which we call *fractional lattice ideals* or simply *fractional ideals* of E.

We note that the theory of fractional lattice ideals is almost identical to the theory of fractional ideals for Dedekind domains. In particular, we get an ideal class group, and these correspond to isomorphism classes of certain modules over $\mathcal{O}_E$. Furthermore, $\mathrm{Hom}_{\mathcal{O}_E}(\mathfrak{a}, \mathfrak{b}) \cong_{\mathcal{O}_E} \mathfrak{b}\mathfrak{a}^{-1}$.

10.3 Some O_E-modules

This section is nearly copied from the section on elliptic curves. For an abelian variety A/K with complex multiplication by E over K, we know that $\mathcal{O}_E$ acts linearly on $\mathrm{Tgt}_0(A)$ and on $T_\ell(A)$ (equivalently, the étale homology $H_1(A, \mathbb{Z}_\ell)$), which are K- and $\mathbb{Z}_\ell$- modules of dimensions g and $2g$, respectively. Tensoring the latter with $\mathbb{Q}$, we get a $\mathbb{Q}_\ell$-linear action on $V_\ell(E)$.

As long as ℓ does not equal the characteristic of K, the action of $\mathcal{O}_E$ on $T_\ell(A)$ is faithful (and similarly, that of E on $V_\ell(A)$). In particular, $T_\ell(A)$ is a free $\mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-module of rank 1. If $\mathrm{End}(A)$ is larger than $\mathcal{O}_E$, $T_\ell(A)$ is still a faithful $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$-module (and the same holds if we tensor everything with $\mathbb{Q}$).

Furthermore, if K has characteristic 0 and embeds in $\mathbb{C}$ (which is true of any finitely-generated field of characteristic 0), we have the homology $H_1(A, \mathbb{Z})$, which is free of rank $2g$. Then $\mathcal{O}_E$ acts on this, making it into a module of rank 1, and E acts on $H_1(A, \mathbb{Q})$, which is free of rank 1. Note that the tangent space $\mathrm{Tgt}_0(A)$ of $A/\mathbb{C}$ is naturally isomorphic to $H_1(A, \mathbb{R})$, giving the latter a complex structure, as well as making it a free $E \otimes_{\mathbb{Q}} \mathbb{R}$-module of rank 1. Furthermore, $T_\ell(E) \cong_{\mathcal{O}_F} \mathbb{Z}_\ell \otimes_{\mathbb{Z}} H_1(E, \mathbb{Z})$.

Finally, dual to the action on the tangent space is the K-linear action on the holomorphic differentials. This is true because a differential is holomorphic iff it is translation invariant, so the differentials are in bijection with the cotangent space. In characteristic 0, every element acts faithfully (and in general,

an element does not act faithfully iff it is inseparable). Note that the holomorphic differentials are naturally isomorphic to the (1,0) part of the Hodge decomposition of the de Rham cohomology.

11 Classification of CM Abelian Varieties and CM Types

11.1 Isogeny Classes and CM Types

The notion of a CM type is essential to the theory of complex multiplication of abelian varieties. We will motivate this by attempting to classify isogeny classes of abelian varieties with complex multiplication, showing that the classification is given by CM types.

We know that every element of $\mathcal{O}_E$ satisfies a separable polynomial, hence is diagonalisable in its actions on $H_1(A, \mathbb{C})$ and $\mathrm{Tgt}_0(A)$. Furthermore, from the basic theory of abelian varieties, the representation of $\mathcal{O}_E$ on $H_1(A, \mathbb{C})$ is isomorphic to the sum of the representation on $\mathrm{Tgt}_0(A)$ and its complex conjugate. Since $H_1(A, \mathbb{Q})$ is a free $E = \mathcal{O}_E \otimes \mathbb{Q}$-module of rank 1, the representation on $H_1(A, \mathbb{C})$ is the sum of all the $\mathbb{Q}$-embeddings of E into $\mathbb{C}$. Thus the representation on $\mathrm{Tgt}_0(A)$ is the direct sum of half of the embeddings, which are representatives for the embeddings modulo complex conjugation on $\mathbb{C}$. We make the following definition:

Definition 11.1. A CM-type Φ on a CM-algebra E is a set of half of the embeddings of E into $\mathbb{C}$ such that the full set of embeddings is given by composing the set with complex conjugation on $\mathbb{C}$.

We have thus shown above that an abelian variety with complex multiplication by E determines a CM-type. Furthermore, as this only depends on the representation of E on the tangent space, it is invariant under isogeny.

To show that sogeny classes of abelian varieties are classified by their CM-type, we wish to show that two abelian varieties with complex multiplication by E and the same CM-type are isogenous. Suppose A is an abelian variety with CM-type Φ.

We note that $H_1(A, \mathbb{Z})$ is a locally free $\mathcal{O}_E$-module of rank 1. It then contains a free submodule of finite index, so we can replace A by an abelian variety such that $H_1(A, \mathbb{Z})$ is free over $\mathcal{O}_E$, without changing the isogeny class.

Suppose that $H_1(A,\mathbb{Z})$ is generated by $\gamma \in H_1(A,\mathbb{Z})$ over $\mathcal{O}_E$. Then γ determines an isomorphism $E \cong H_1(A,\mathbb{Q})$, hence between $E \otimes_{\mathbb{Q}} \mathbb{R}$ and $H_1(A,\mathbb{R})$. Note that the CM-type Φ determines an isomorphism $E \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C}^{\Phi}$, and because $\mathrm{Tgt}_0(A)$ determines the complex structure on $H_1(A,\mathbb{R})$, we get a complex isomorphism

$$H_1(A,\mathbb{R}) \cong E \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C}^{\Phi}$$

Then $H_1(A,\mathbb{Z})$ corresponds to $\mathcal{O}_E \subseteq E \otimes_{\mathbb{Q}} \mathbb{R}$, so A is isomorphic to $(E \otimes_{\mathbb{Q}} \mathbb{R})/\mathcal{O}_E$, where $E \otimes_{\mathbb{Q}} \mathbb{R}$ has complex structure determined by Φ. It follows that all abelian varieties with the same CM-type are isogenous.

Conversely, a CM-type Φ determines an isomorphism $E \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C}^{\Phi}$. The image of $\mathcal{O}_E$ under this isomorphism is a lattice, and the quotient is an abelian variety with CM-type Φ. We thus have established the following:

Theorem 11.2. *Isogeny classes of abelian varieties with CM by a CM-algebra E are in bijection with CM-types Φ of E. The bijection associates to an abelian variety A the CM-type coming from the representation of E on $\mathrm{Tgt}_0(A)$, and it associates to a CM-type Φ the variety $\mathbb{C}^{\Phi}/\mathcal{O}_E$.*

We next make the following *important* remark about varieties defined over fields of characteristic 0 other than $\mathbb{C}$.

Remark 11.3. Suppose A has complex multiplication by E and is defined over a field K that contains all the conjugates of E. Then the representation of E on $\mathrm{Tgt}_0(A)$ must decompose into one-dimensional representations. Given an embedding $K \hookrightarrow \mathbb{C}$, we can view A as an abelian variety over $\mathbb{C}$, and the above theory shows that this representation of E on $\mathrm{Tgt}_0(A)$ must come from a CM-type. Once we have our embedding $K \hookrightarrow \mathbb{C}$, we can think of our CM-type as a set of homomorphisms from E into K, rather than $\mathbb{C}$.

Remark 11.4. More abstractly, if we have an abelian variety A/K with CM by E, we can, without choosing an embedding $K \hookrightarrow \mathbb{C}$, define its CM-type as the homomorphisms $E \to K$ appearing in the representation of E on $\mathrm{Tgt}_0(A)$. The possibility of choosing an embedding $K \hookrightarrow \mathbb{C}$ allows us to conclude that these are half of the possible embeddings, with the full set giving by some complex conjugation.

11.2 Isomorphism Classes

In the case of elliptic curves, all elliptic curves with CM by the same field are isogenous. In the case of abelian varieties, we have shown that isogeny classes are classified by CM types. In the case of elliptic curves, isomorphism classes with CM by the maximal order are in bijection with ideal classes. We note that when we restrict ourselves to a particular isogeny class, this is still the case.

Fact 11.5. For a given CM-type Φ on a CM-algebra E, the isomorphism classes of abelian varieties with CM-type Φ and $\mathcal{O}_E$ as endomorphism ring are in bijection with isomorphism classes of rank 1 locally free modules over $\mathcal{O}_E$, or equivalently, classes of lattice ideals (ideals that are lattices in $E \otimes_{\mathbb{Z}} \mathbb{R}$).

Note that, as in the case of elliptic curves, given an abelian variety, we can recover the module as $H_1(A, \mathbb{Z})$, with the natural action by $\mathcal{O}_E$.

12 Ideal Multiplication for Abelian Varieties

We would like to extend $\mathfrak{a}$-multiplications to abelian varieties A with complex multiplication by E, when $\mathfrak{a}$ is a fractional ideal of E. We can define this quite simply over $\mathbb{C}$ by supposing $A = \mathbb{C}^g/\Gamma$, with g the dimension of A and Γ a lattice, then letting $A^{\mathfrak{a}} = \mathbb{C}^g/\mathfrak{a}^{-1}\Gamma$ and $f^{\mathfrak{a}} : A \to A^{\mathfrak{a}}$ the naturally-induced quotient.

As in the case of elliptic curves, we would like give an algebraic description of this action that will, in particular, allow us to show that it commutes with the Galois action (in an appropriate sense). This is the main difference from the case of elliptic curves. We will first restate all the properties of $\mathfrak{a}$-multiplications (but in the case of abelian varieties), then explain how they can be given an algebraic definition.

Definition 12.1. For an abelian variety A with complex multiplication by E and a fractional ideal $\mathfrak{a}$ of E, we call an abelian variety $A^{\mathfrak{a}}$ and a map $f^{\mathfrak{a}} : A \to A^{\mathfrak{a}}$ an $\mathfrak{a}$-*multiplication* if $a : A \to A$ factors through $f^{\mathfrak{a}}$ iff $a \in \mathfrak{a}$. Note that we allow ourselves to consider $\mathfrak{a}$ non-integral, in which case $f^{\mathfrak{a}}$ but in this case, "factors through" means that the morphism $A' \to A$ is actually in $\mathrm{Hom}(A', A)$.

Thus an isogeny $a \in \mathrm{End}_0(A)$ is an (a)-multiplication. In a sense, if we think of multiplication by a as an multiplication by its ideal, then we should think of $\mathfrak{a}$-multiplications as a way to multiply by non-principal ideals. The only caveat then is that it might not be an endomorphism, but a homomorphism into another variety.

Note that we could define this instead by saying that all $a \in \mathfrak{a}$ factors through $f^{\mathfrak{a}}$, and that furthermore, $\mathfrak{a}$ is universal for this property.

We also note that an isogeny $f : A \to A'$ that commutes with E is automatically an $\mathfrak{a}$-multiplication for some $\mathfrak{a}$. We only need note that, as in the case of elliptic curves, A, A' can be uniformized.

Furthermore, the cokernel of the mapping $f_* : H_1(A, \mathbb{Z}) \to H_1(A', \mathbb{Z})$ is the degree of the isogeny, which is the same as $[\mathcal{O}_E : \mathfrak{a}]$.

We once again have the following properties, which follow fairly easily from either the complex-analytic theory or the abstract definition (to be given below):

Proposition 12.2. *(1) An isogeny $f : A \to A'$ is an $\mathfrak{a}$-multiplication if every $a \in \mathfrak{a}$ factors through f, and its degree is (at least) $[\mathcal{O}_E : \mathfrak{a}]$*
(2) Multiplication by $\alpha \in E^\times$ is an (α)-multiplication
(3) $f^\mathfrak{a}$ factors through $f^{\mathfrak{a}'}$ iff $\mathfrak{a}' \subseteq \mathfrak{a}$
(4) A composition of an $\mathfrak{a}$-multiplication with an $\mathfrak{a}'$-multiplication is an $\mathfrak{a}\mathfrak{a}'$-multiplication
(5) If $f : A \to A'$ is an $\mathfrak{a}$-multiplication, then precomposition with $f \circ \alpha \in \mathrm{Hom}(A, A')$ iff $\alpha \in \mathfrak{a}^{-1}$, and this determines an isomorphism from $\mathfrak{a}^{-1}$ to $\mathrm{Hom}(A, A')$ as $\mathcal{O}_E$-modules. By (4), this means that

$$\mathrm{Hom}_{\mathcal{O}_E}(A^\mathfrak{a}, A^\mathfrak{b}) \cong \mathfrak{a}\mathfrak{b}^{-1}$$

, where $\mathrm{Hom}_{\mathcal{O}_E}$ denotes those isogenies commuting with $\mathcal{O}_E$. (note the error in [4], 1.33(a)!)

Proof. We note how to prove (5). Note that

$$H_1(A', \mathbb{Z}) \cong_{\mathcal{O}_E} \mathfrak{a}^{-1} \otimes_{\mathcal{O}_E} H_1(A, \mathbb{Z}).$$

Thus

$$\mathrm{Hom}_{\mathcal{O}_E}(H_1(A, \mathbb{Z}), H_1(A', \mathbb{Z})) \cong_{\mathcal{O}_E} \mathfrak{a}^{-1},$$

and since E gives the complex structure on $H_1(A, \mathbb{R})$, a $\mathbb{Z}$-linear map commuting with E is compatible with the complex structure, hence a morphism of abelian varieties, so this indeed gives the set of isogenies from A to A' commuting with $\mathcal{O}_E$. □

Remark 12.3. The same remarks about canonicity apply as in the case of elliptic curves.

Furthermore, as in the case of elliptic curves, we have the following:

Proposition 12.4. *The map from $Cl(\mathcal{O}_E)$ defined by $[\mathfrak{a}] \mapsto A^\mathfrak{a}$ is a bijection from $Cl(\mathcal{O}_E)$ to the set of abelian varieties with CM by $\mathcal{O}_E$ and the same CM-type as A.*

Proof. Similar to the case of elliptic curves. In brief, if the ideal classes are the same, then there is an element of $E^\times$ relating them, giving an isomorphism between the two varieties, and if the two isomorphic, then they are their lattices (and hence ideals) are related by an element of $E^\times$. □

12.1 Algebraic Definition

We next remark how to define an $\mathfrak{a}$-multiplication. We would like to create the quotient $A/A[\mathfrak{a}]$, although this is harder in the higher-dimensional case. We thus do the following.

12.1.1 First Approach

We take a set of generators, $\alpha_1, \cdots, \alpha_n$ of A. This defines a morphism $\alpha_i : A \to A^n$. We then note that the image is a sub-group variety of an abelian variety, and is also connected, hence an abelian variety. It is fairly clear that if $\alpha \in \mathfrak{a}$, then $\alpha = \sum_i r_i \alpha_i$ for $r_i \in \mathcal{O}_E$, hence there is a map $A^n \to A$ given by the r_i whose composition with α_i is α. Furthermore, if $A \to A'$ is another morphism with the same property, then we have a factoring $A \to A' \to A^n$ that gives α^i

12.1.2 Second Approach

This is more or less the approach followed in [9], in the case of elliptic curves.

We motivate the approach as follows. We note that the definition is easy in the complex-analytic case because the space $\mathbb{C}^g$ is larger and hence "gives us room to budge." (Note: I should probably try to find a better phrase.)

In other words, the notion of different isomorphism classes of $\mathcal{O}_E$-modules is something somewhat abstract (say, for the person who only knows vector spaces). We might like to think of these, therefore, in terms of something more concrete, such as vector spaces, or more generally (but not too generally!), free modules. When resorting to complex analysis, these are simply different lattices that live inside the vector space $\mathbb{C}^g$, or even more specifically, $E = \mathbb{Q}^{2g}$. But how can we access these in a purely algebraic way? We would like to get some "room" without having to resort to complex analysis.

We then respond to this need for concreteness: we can express $\mathfrak{a}$ using a finite presentation ${\mathcal{O}_E}^m \to^g {\mathcal{O}_E}^n \to \mathfrak{a}$ of $\mathcal{O}_E$-modules. We note that g can be expressed by an $n \times m$ matrix, and this encodes everything about the $\mathcal{O}_E$-module $\mathfrak{a}$. How can we translate this into purely algebraic constructions in the theory of abelian varieties? We can use the matrix of g to give a map $A^m \to^g A^n$, or, using its transpose, we get a map $A^n \to^{g^T} A^m$.

It is not too hard to see that complex analytically, the kernel of g^T is an algebraic group that is precisely $A^{\mathfrak{a}}$. Furthermore, this construction is completely algebraic! In particular, it is not too hard to see that if A and all of its endomorphisms are defined over K, then this kernel inherits a natural action of G_K. If we think of the embedding $\mathfrak{a} \hookrightarrow \mathcal{O}_E$ as giving us an exact sequence

$$\mathcal{O}_E{}^m \to^g \mathcal{O}_E{}^n \to^h \mathcal{O}_E \to \mathcal{O}_E/\mathfrak{a} \to 0,$$

then it is not too hard to see that the composition $A \to^{h^T} A^n \to^{g^T} A^m$ is trivial, hence we get a map from A to $A^{\mathfrak{a}}$, as desired.

12.1.3 Third Approach

There is another definition, related to a certain intuitive idea. We note that if we think of A as being like $\mathcal{O}_E$, then we can intuitively think of $A^{\mathfrak{a}}$ as somehow being like $\mathfrak{a}^{-1}$. This makes sense when we recall the similarity between $\mathrm{Hom}(A^{\mathfrak{a}}, A^{\mathfrak{b}}) \cong_{\mathcal{O}_E} \mathfrak{a}\mathfrak{b}^{-1}$ and $\mathrm{Hom}_{\mathcal{O}_E}(\mathfrak{a}^{-1}, \mathfrak{b}^{-1}) \cong_{\mathcal{O}_E} \mathfrak{a}\mathfrak{b}^{-1}$. Thus, in order to get the abelian variety that is "like" $\mathfrak{a}^{-1}$, we might want to look at $\mathrm{Hom}(\mathfrak{a}, A)$ and hope for some way to make it into a variety, not just a group.

The simplest way to do so is to describe its functor of points. We suppose A is defined over K note that $\mathcal{O}_E$ acts on A, hence acts on the group $A(T)$ for any K-algebra T (or more generally, any K-scheme T, but we do not need this as a functor of points is determined by its effect on affine schemes). Thus, it makes sense to talk about $\mathrm{Hom}_{\mathcal{O}_E}(\mathfrak{a}, A(T))$, and we define a new group variety A^M over K by

$$A^M(T) := \mathrm{Hom}_{\mathcal{O}_E}(M, A(T))$$

for any $\mathcal{O}_E$-module M. The only question then is to show that this is a representable functor. As it turns out, showing that this is representable is precisely the argument of our "Second Approach."

Note that we have only defined our algebraic group A^M up to isomorphism. This makes sense, since it only depended on M *qua* $\mathcal{O}_E$-module, and the isomorphism class of $\mathfrak{a}$ as an $\mathcal{O}_E$-module is the same its ideal class. We now note that the above construction is a contravariant functor in M. In particular, if $M = \mathfrak{a} \subseteq \mathcal{O}_E$, an ideal of $\mathcal{O}_E$ (i.e., we have a fixed $\mathcal{O}_E$-module injection $M \hookrightarrow \mathcal{O}_E$), this gives us a morphism $A \to A^{\mathfrak{a}}$.

13 Reduction Modulo A Prime

Let A/K be an abelian variety, with K the field of fractions of a discrete valuation ring R. We say that A has good reduction if there is an abelian scheme $\mathcal{A}$ (smooth and proper) over R whose fiber at the generic point of R is isomorphic to A, and whose special fiber, denoted A_0, is therefore an abelian variety over the residue field k of R. Concretely, if we have a set of equations for $\mathcal{A}$, we reduce modulo the prime of R to get the model over k. A set of equations that works will be such that its matrix is invertible in R, causing the scheme to be smooth.

We note that for an R-algebra S, $A(S \otimes_R K) = \mathcal{A}(S)$ (a universal property of the model over R), giving us a reduction map $A(S \otimes_R K) = \mathcal{A}(S) \to A_0(S \otimes_R k)$. In particular, this works for S the valuation ring of any algebraic extension L of K.

The most common case will be when R is the localization of a number field K or p-adic field at a prime ideal $\mathfrak{p}$. In this case, we will say that A has good reduction at $\mathfrak{p}$.

We note that, as in the case of elliptic curves, there is a reduction map on endomorphisms (which follows from universal properties of $\mathcal{A}$). As in the case of elliptic curves, the reduction map is injective on endomorphisms, but the endomorphism ring of the abelian variety over k might be larger than that over the the field of characteristic 0. However, the action on the Tate module will still be faithful (though certain elements might have nontrivial kernels).

As in the case of elliptic curves, abelian varieties with complex multiplication have potentially good reduction at all primes. The proof is nearly identical, as the criterion of Néron-Ogg-Shafarevich extends to abelian varieties.

14 Shimura-Taniyama Formula

We suppose, for the rest of this section, that A is an abelian variety with complex multiplication by a CM-algebra E over a number field K, that $\mathfrak{P}$ is a prime of K at which A has good reduction, and that $k = \mathcal{O}_K/\mathfrak{P}$. We let q denote $|k|$, and let A_0 denote the reduction of A modulo $\mathfrak{P}$.

As in the case of elliptic curves, we would like to describe the action of the Galois group G_F on torsion points (for some field F in K, which we are leaving vague at the moment), and we do that by considering Frobenius elements, which

are dense in the Galois group. Thus, given a Frobenius element $\sigma = (F, \mathfrak{p})$, we would like to show that there is an $\mathfrak{a}$-multiplication

$$f : A \to \sigma(A)$$

such that:
(1) f reduces to the $p^{[\mathcal{O}_F:\mathfrak{p}]}$-power Frobenius modulo a prime $\mathfrak{P}$ of K above $\mathfrak{p}$
(2) $\mathfrak{a}$ related in a nice (class field-theoretic) way to σ.

Note that $\sigma(A)$ is not necessarily isomorphic to A. Because we prefer to work with endomorphisms, we can do the following. We note that

$$\sigma(f) : \sigma(A) \to \sigma^2(A)$$

will also be an $\mathfrak{a}$-multiplication (recall that E is identified as a subring of the endomorphisms of $\sigma(A)$ via σ). Then

$$\sigma^{f(\mathfrak{P}/\mathfrak{p})}(f) \circ \cdots \circ \sigma(f) \circ f : A \to \sigma^{f(\mathfrak{P}/\mathfrak{p})} A = (K, \mathfrak{P})(A) = A$$

is an $\mathfrak{a}^{f(\mathfrak{P}/\mathfrak{p})}$ multiplication inducing the Frobenius qth-power on A_0. Thus, in order to find $\mathfrak{a}$, we would like to find the ideal generated by the element of $\mathcal{O}_E$ that reduces to the Frobenius endomorphism modulo $\mathfrak{P}$.

14.1 Commutants

Before doing the above, we must show that there actually is an element of $\mathcal{O}_E$ that reduces to the Frobenius endomorphism modulo $\mathfrak{P}$.

In the case of elliptic curves, we prove that the Frobenius map comes from an element of E by showing noting that it commutes with all of the other endomorphisms. We will do the same here, and we just require a bit of preliminaries on which endomorphisms are in the center of the ring of endomorphisms.

Basically, if an endomorphism commutes with all others, it (in particular) commutes with those of E, so it is E-linear on the various E-modules arising from the elliptic curve (usually some sort of cohomology). Since these are of dimension 1, such an endomorphism must be an element of E. We just need a little more work to extend this result to characteristic p (when there might be more endomorphisms than E) and to actual endomorphisms of A (as opposed to those tensored with $\mathbb{Q}$).

Proposition 14.1. *There exists an element $\pi \in \mathcal{O}_E$ inducing the qth-power Frobenius endomorphism on the reduction modulo $\mathfrak{P}$, A_0, of A.*

Proof. The Frobenius morphism commutes with all other endomorphisms as they are defined over K, hence their reductions are defined over k, and the Frobenius is an Galois group element that fixes k. Therefore, its action on the Tate module $V_\ell(A)$ (for a good ℓ) is $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-linear, hence is multiplication by an element of $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ because the former is a module of rank 1 over the latter. It is thus an element of E as $\mathrm{End}_0(A_0) \cap (E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell) = E$. Furthermore, $\mathrm{End}(A_0) \cap E$ is an order in E, and since $\mathrm{End}(A)$ is the maximal order, it maps surjectively onto $\mathrm{End}(A_0) \cap E$, so this Frobenius endomorphism is in the image of $\mathcal{O}_E = \mathrm{End}(A)$. □

14.2 The Formula

The Shimura-Taniyama formula is a description of this element of $\mathcal{O}_E$, which we call π.

Theorem 14.2 (Shimura-Taniyama Formula)**.** *The element π in the above proposition generates the following ideal:*

$$\prod_{\phi \in \Phi} \phi^{-1}(\mathrm{N}_{K/\phi(E)}(\mathfrak{P})),$$

where $\Phi \subseteq \mathrm{Hom}(E, K)$ is the CM-type of A (see Remark 11.4).

We first remark how we would prove this proposition in the case of CM elliptic curves, then move on to the general case of abelian varieties. Note that we implicitly used something of this form when proving Theorem 6.1, and other accounts of complex multiplication for elliptic curves use it explicitly.

For this paragraph and the next, we let E/K denote an elliptic curve with complex multiplication by $\mathcal{O}_F$, the ring of integers in an imaginary quadratic field. Let $\mathfrak{P}$ be a prime of K at which E has good reduction (and a couple other properties we won't worry about) know from the above that there is a $\pi \in \mathcal{O}_F$ that reduces to the Frobenius modulo $\mathfrak{P}$. Then F embedds in K by the action on the tangent space (equivalently, on the holomorphic differentials), and we would like to show that $(\pi) = \mathrm{N}_{K/F}(\mathfrak{P})$.

If p is inert in F, then we are done, for then π is a power of $p\mathcal{O}_F$, and since we know its degree is $q = p^{2f(\mathfrak{P}/p\mathcal{O}_F)}$, we are done. Suppose, on the other hand, that $p\mathcal{O}_F = \mathfrak{pq}$, with $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$ and $\mathfrak{p}$ the prime lying under $\mathfrak{P}$ in the embedding $F \hookrightarrow K$. Then $(\pi) = \mathfrak{p}^n\mathfrak{q}^m$. To analyze each prime individually, let h be the class number of $\mathcal{O}_F$, so that $\mathfrak{p}^{nh} = (\gamma_1)$ and $\mathfrak{q}^{mh} = (\gamma_2)$, hence $(\pi)^h = (\gamma_1\gamma_2)$. Then π^h induces a purely inseparable map modulo $\mathfrak{P}$. However, γ_2 is not in $\mathfrak{p}$, hence not in $\mathfrak{P}$ in its action on the differential, so its reduction modulo $\mathfrak{P}$ is separable! Therefore, $(\gamma_2) = (1)$, and our result follows.

In the case of abelian varieties, the vector space of holomorphic differentials has dimension greater than 1, so the same arguments get more complicated: first, we cannot easily detect separability or inseparability, and second, there are multiple embeddings from our endomorphism ring into K, hence multiple primes that lie below $\mathfrak{P}$. We recall that the theory of the module of differentials nicely relates differentials with the concept of separability, and we use it to prove the following lemma, which will allow us to make similar arguments in the case of abelian varieties:

Lemma 14.3. *Let k be algebraically closed of characteristic p and $\alpha : A \to B$ an isogeny over k. Suppose $\alpha^*(k(B))$ contains $k(A)^q$, where $q = p^m$, and let d be the dimension of the kernel of the induced map on tangent spaces. Then the degree of α is at most q^d.*

Note that in the case of elliptic curves, for $d = 0$ this is the fact that inseparable morphisms are zero on the tangent space, and for $d = 1$, this is the fact that the qth power Frobenius has degree q.

Proof. Let L/K denote the extension $k(A)/\alpha^*(k(B))$. The condition that K contains L^q implies that the field extension is purely inseparable, generated by taking qth roots of elements of K.

We thus have an exact sequence

$$\Omega_{K/k} \otimes_K L \to^{\alpha^*} \Omega_{L/k} \to \Omega_{L/K} \to 0$$

by [2], p.186. In the case of abelian varieties, the (algebraic) differential 1-forms are isomorphic to the tensor product of the cotangent space with the function field, hence dual to the tensor product with the tangent field. This shows that the cokernel of the first map in the above exact sequence is dual to the kernel of the induced map on tangent spaces, so $\dim_L \Omega_{L/K} = d$.

Then the basic theory of purely inseparable extensions shows that L can be generated by d elements over K, each of which is a qth root of an element of K, so the extension has degree at most q^d. □

We now finish the proof of the Shimura-Taniyama formula.

Proof. Because degree is unchanged under reduction, we know that π has degree q^g (as the Frobenius does), hence $|\mathrm{N}_{K/\mathbb{Q}}(\pi)| = q$, so π factors as a product of primes of F lying over p. Thus

$$(\pi) = \prod_{v|p} \mathfrak{p}_v^{m_v}$$

where m_v are non-negative integers.

The expression $\prod_{\phi\in\Phi} \phi^{-1}(\mathrm{N}_{K/\phi(E)}(\mathfrak{P}))$ is also a product over $v \mid p$. For such v, let

$$\Phi_v := \{\phi \in \Phi \mid \phi^{-1}(\mathfrak{P}) = \mathfrak{p}_v\}.$$

Then what we wish to show is that

$$\mathfrak{p}_v^{m_v} =^? \prod_{\phi\in\Phi_v} \phi^{-1}(\mathrm{N}_{K/\phi(E)}(\mathfrak{P})).$$

Since both are powers of the same prime ideal, we just have to show the exponent is the same, which amounts to showing that

$$\begin{aligned}
\mathrm{N}_{E/\mathbb{Q}}\mathfrak{p}^{m_v} &=^? \mathrm{N}_{E/\mathbb{Q}}\Big(\prod_{\phi\in\Phi_v} \phi^{-1}(\mathrm{N}_{K/\phi(E)}(\mathfrak{P}))\Big) \\
&= \prod_{\phi\in\Phi_v} \mathrm{N}_{E/\mathbb{Q}}(\phi^{-1}(\mathrm{N}_{K/\phi(E)}(\mathfrak{P}))) \\
&= \prod_{\phi\in\Phi_v} \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P}) \\
&= \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P})^{d_v} \\
&= q^{d_v},
\end{aligned}$$

where $d_v = |\Phi_v|$.

Of course, since $\sum_{v|p} d_v = g$, and the degree of π is $\mathrm{N}_{E/\mathbb{Q}}(\pi)$ the product of each side of the above is q^g, so we only have to show that $\mathrm{N}_{E/\mathbb{Q}}\mathfrak{p}^{m_v}$ *divides* q^{d_v}.

We would love to interpret $\mathrm{N}_{E/\mathbb{Q}}(\mathfrak{p}^{m_v})$ as the degree of $\mathfrak{p}^{m_v}$ and use Lemma 14.3, but we do not know whether this ideal is principal (and hence actually defines a morphism of A). Of course, to prove what we want, we can raise each side to the power h, the class number of $\mathcal{O}_E$, and suppose that $\mathfrak{p}^{hm_v} = (\gamma_v)$. Then since $\prod_v (\gamma_v) = (\pi)^h$, each γ_v^* (modulo $\mathfrak{P}$) sends $k(A_0)$ to a subfield containing $k(A_0)^{q^h}$. If we can show that d_v is the dimension of the kernel of γ_v on the tangent space, we are done by Lemma 14.3.

We recall that the tangent space of K is, as a $E \otimes_{\mathbb{Q}} K$-module, $\oplus_{\phi\in\Phi} K_\phi$. We know that the tangent space of $\mathcal{A}$, the abelian scheme over $\mathcal{O}_{\mathfrak{P}}$, is an $\mathcal{O}_{\mathfrak{P}}$

with action of $\mathcal{O}_E$ that induces the above tangent space when we change base. By a result in commutative algebra, for all but finitely many p, this gives an isomorphism $\mathrm{Tgt}_0(\mathcal{A}) \cong_{\mathcal{O}_E \otimes_{\mathbb{Z}} \mathcal{O}_{\mathfrak{P}}} \oplus_{\phi \in \Phi} \mathcal{O}_\phi$, where $\mathcal{O}_\phi$ is $\mathcal{O}_{\mathfrak{P}}$ with $\mathcal{O}_E$-action by ϕ. Then $\mathcal{O}_\phi$, when reduced modulo $\mathfrak{P}$ is in the kernel of γ_v iff $\phi(\gamma_v) \in \mathfrak{P}$, or equivalently, $\phi^{-1}(\mathfrak{P}) = \mathfrak{p}_v$, i.e. $\phi \in \Phi_v$. Thus this dimension is in fact d_v, and we are done. □

14.3 Reflex Norms and the Reflex Field

We would like to put the formula from the last section on a more theoretical footing.

We note that the expression $\prod_{\phi \in \Phi} \phi^{-1}(\mathrm{N}_{K/\phi(E)}(\mathfrak{P}))$ is a product of embeddings, hence appears to be a kind of "norm." Before considering ideals, we consider the map

$$a \mapsto \prod_{\phi \in \Phi} \phi^{-1}(\mathrm{N}_{K/\phi(E)}(a))$$

as a map from $K^\times$ to $K^\times$. For reasons that will become apparent later, we denote this $\mathrm{N}_{\mathrm{K},\Phi}(\mathrm{a})$.

For each $\phi \in \Phi$, let V_Φ denote the $E \otimes_{\mathbb{Q}} K$-module K_ϕ which is K as a K-module, and has action of E given by $\phi : E \hookrightarrow K$, and let $V_{K,\Phi} = \oplus_{\phi \in \Phi} K_\phi$. We have already noted that the tangent space has this structure.

Each element $r \in K$ acts on V_ϕ as an E-linear map, and its determinant is $\phi^{-1}(\mathrm{N}_{K/\phi(E)}(r))$. Thus the E-linear determinant of the action of r on $V_{K,\Phi}$ is $\mathrm{N}_{\mathrm{K},\Phi}(\mathrm{r})$.

We can now use the properties of determinant under base change. If K'/K is an extension, we know that

$$V_{K',\Phi} \cong V_{K,\Phi} \otimes_K K'$$

as a $E \otimes_{\mathbb{Q}} K' = (E \otimes_{\mathbb{Q}} K) \otimes_K K'$-module. Then it follows that

$$\mathrm{N}_{\mathrm{K}',\Phi} = \mathrm{N}_{\mathrm{K},\Phi} \circ \mathrm{N}_{\mathrm{K}'/\mathrm{K}}$$

More interestingly, we would like to see if it is possible to find a field F smaller than K such that there exists an $E \otimes_{\mathbb{Q}} F$-module $V_{F,\Phi}$ whose tensor product over F with K gives $V_{K,\Phi}$. The idea is that we might find one over which the action of E is not diagonalizable.

By the invariance of trace under base change, we know that $\mathrm{Tr}_K(e \mid V_{K,\Phi}) = \sum_{\phi \in \Phi} \phi(e)$ must be contained in F for all $e \in E$. Can we take F to be the set of such traces? (If so, then this F is "smallest")

We choose an algebraic closure of K and let $G(\bar{(}K)/\mathbb{Q})$ act on homomorphisms from any ring, such as E, into K. Notice that the subgroup of $G(\overline{K}/\mathbb{Q})$ sending the set Φ to itself fixes all of these traces. Conversely, such an automorphism that fixes all of these traces must take Φ to itself by linear independence of characters. This gives us a characterization of the field of traces as the fixed field of a specific group. We will use E^* to denote this field.

Next, we recall that we can descend from K to a smaller field using Galois descent. Suppose that K is Galois over E^*. Then one can let $\sigma \in G(K/E^*)$ act on $V_{K,\Phi}$ by sending K_ϕ isomorphically onto $K_{\sigma\phi}$ for $\phi \in \Phi$. Then this mapping is clearly E-linear and $G(K/E^*)$-linear over K, meaning we can in fact descend to E^*.

Definition 14.4. We call the E^* defined above the *reflex field*. For $F = E^*$, we denote $V_{F,\Phi}$ simply by V_Φ, and $\mathrm{N}_{\mathrm{F},\Phi}$ by N_Φ, which is called the *reflex norm*.

Recall that, as mentioned before, for any K/E^*, we have

$$\mathrm{N}_{\mathrm{K},\Phi} = \mathrm{N}_\Phi \circ \mathrm{N}_{\mathrm{K}/\mathrm{E}^*}.$$

Finally, we remark how to extend this construction to ideals. The obvious condition should be that the reflex norm of a principal ideal is the ideal generated by the reflex norm of one of its generators. Then, one can make the reasonable request that the norm send primes lying over a given rational prime p to others lying over p. Because we can find a uniformizer at any given prime that does not lie in any other prime ideal over p, this determines the map uniquely.

Finally, we can summarize the Shimura-Taniyama formula as saying that $\mathrm{N}_{\mathrm{K},\Phi}(\mathfrak{P}) = (\pi)$.

Remark 14.5. Alternatively, one can note that we actually have a map $\mathrm{N}_\Phi : (\mathrm{E}^* \otimes_{\mathbb{Q}} \mathrm{R})^\times \to (\mathrm{E} \otimes_{\mathbb{Q}} \mathrm{R})^\times$ for each $\mathbb{Q}$-algebra R. (As a brief remark, this gives a map on functors of points, hence between two algebraic tori over $\mathbb{Q}$ corresponding to E^*, E respectively.) Upon taking R the ring of adeles, we get a map from the finite adeles of E^* to the finite adeles of E, and then one notes that this factors through when we send an idele to the ideal it generates, hence given us a norm map on ideals.

15 Main Theorem for Abelian Varieties

We have done essentially everything we need in order to extend complex multiplication to abelian varieties. The statements and proofs will be almost identical to those in the case of elliptic curves; the main difference is that we will be dealing with the class field theory of E^*, not of E, and we will send objects from E to E^* using the reflex norm.

Before doing so, we make a remark about the problem of explicitly generating class fields of number fields, which is what complex multiplication is supposed to be about:

Remark 15.1. We note that if E is a CM-field, then not only do we get a reflex field E^*, but we get a CM-type for E^*, known as the *reflex type*. Furthermore, reflex field and reflex type of E^* with its reflex type is the CM-field and CM-type! In other words, given a CM-field E, we can always find a field E' of which E is the reflex field for some CM-type on E'. This means we have a way of generating the class field theory of E.

We recall from Proposition 14.1 that there is an endormorphism inducing the Frobenius map. Now, suppose σ is a global automorphism inducing Frobenius modulo some prime and fixing the reflex field. Then A and $\sigma(A)$ are isogenous (as they have the same CM-type), and we would like to show that there is an isogeny $A \to \sigma(A)$ inducing Frobenius modulo a prime $\mathfrak{P}$ of good reduction. We thus have the following prosposition:

Proposition 15.2. *Suppose A, A' are isogenous CM abelian varieties (equivalently, with the same CM-type), A_0, A_0' their reductions modulo a prime of good reduction. Then the reduction map*

$$\mathrm{Hom}_{\mathcal{O}_E}(A, A') \to \mathrm{Hom}_{\mathcal{O}_E}(A_0, A_0')$$

is an isomorphism.

Proof. We know that A, A' correspond to two ideal classes represented by integral ideals $\mathfrak{a} \subseteq \mathfrak{a}'$ of $\mathcal{O}_E$, so the projection $(E \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{a} \to (E \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{a}'$ is a $\mathfrak{b} = \mathfrak{a}\mathfrak{a}'^{-1}$-multiplication from A to A', which we denote by f. Then precomposition with f gives an isomorphism from $\mathfrak{b}^{-1} \subseteq E \hookrightarrow \mathrm{End}_0(A)$ to $\mathrm{Hom}_{\mathcal{O}_E}(A, A')$ by Proposition 12.2, as from $\mathfrak{b}^{-1} \subseteq E \hookrightarrow \mathrm{End}_0(A_0)$ to $\mathrm{Hom}_{\mathcal{O}_E}(A_0, A_0')$.

As these isomorphisms commute with reduction, the reduction map is an isomorphism, and we are done. □

We can now state and prove the fundamental theorem in ideal-theoretic terms.

Theorem 15.3 (Fundamental Theorem of Complex Multiplication)**.** *Fix an integer $m \geq 3$ sufficiently large* and an abelian variety A/K with CM by E. Then for each automorphism $\sigma \in G(\overline{K}/E^*)$, there is an $\mathfrak{a}$-multiplication $f^\sigma : A \to \sigma(A)$ agreeing with σ on $A[m]$ such that*
(1) $\mathfrak{a}$ is determined in $Cl_m(\mathcal{O}_E)$
(2) This class only depends on the restriction of σ to the ray class field L_m of E^*, and

$$\mathfrak{a} = \mathrm{N}_\Phi(\mathfrak{b}),$$

where $(\mathfrak{b}, L_m/E^*) = \sigma\,|_{L_m}$.

Proof. Let K be a field over which all of the m-torsion points of all CM abelian varieties isogenous to A are defined. (We can even suppose that all of these varieties have good reduction at every prime of K by the Néron-Ogg-Shafarevich Criterion, but this is not necessary, since we can always throw out finitely many primes.)

Since σ fixes E^*, we know that A and $\sigma(A)$ are isogenous, and suppose f is an $\mathfrak{a}$-multiplication between them (which exists by the proof of Proposition 15.2). We can precompose with an element of $\mathcal{O}_E$ that makes f be an $\mathfrak{a}$-multiplication for $\mathfrak{a}$ prime to m (but $\mathfrak{a}$ still integral). Thus it makes $A[m]$ isomorphically onto $\sigma(A)[m]$.

Since $A[m], \sigma(A)[m]$ are $\mathcal{O}_E/(m)$-modules of rank 1, and σ and f commute with $\mathcal{O}_E$, there is $a \in \mathcal{O}_E$ such that $f \circ a$ agrees with σ on $A[m]$. We then replace f by $f\circ$, noting that we replace $\mathfrak{a}$ by $\mathfrak{a}(a)$.

Furthermore, composition of f with $\mathfrak{a}^{-1}(a^{-1})$ gives an isomorphism between $\mathfrak{a}^{-1}(a^{-1})$ and $\mathrm{Hom}_{\mathcal{O}_E}(A, \sigma(A))$. An element of $\mathfrak{a}^{-1}(a^{-1})$ gives an identical action on $A[m]$ iff it is congruent to 1 modulo m, meaning that $\mathfrak{a}$ is determined by σ modulo $\iota(E_{m,1})$.

In addition, if we have σ, σ', with corresponding isogenies f, g, then $\sigma(g) \circ f$ gives an isogeny agreeing with $\sigma' \circ \sigma$ on $A[m]$, so this gives us a homomorphism from G_{E^*} to $Cl_m(\mathcal{O}_E)$, which is clearly trivial on G_K.

Next, we use the Shimura-Taniyama formula in a fundamental way. Let $\mathfrak{P}$ be a prime of K over a prime $\mathfrak{p}$ of E^*, such that everything has good reduction, is prime to m, and nothing is ramified (we are being vague, but it is very easy to see that we can do this and only throw out finitely many primes). Suppose, furthermore, that $(K/E^*, \mathfrak{P}) = \sigma \mid K$. Then, in the notation of Section 14, we know that σ induces the $p^{f(\mathfrak{p}/p)}$th-power Frobenius modulo $\mathfrak{P}$. Let f be the

$\mathfrak{a}$-multiplication inducing this Frobenius (which exists by Proposition 15.2). We then have that

$$\sigma^{f(\mathfrak{P}/\mathfrak{p})}(f) \circ \cdots \circ \sigma(f) \circ f : A \to \sigma^{f(\mathfrak{P}/\mathfrak{p})} A = (K, \mathfrak{P})(A) = A$$

reduces to the qth-power Frobenius. This isogeny is an $\mathfrak{a}^{f(\mathfrak{P}/\mathfrak{p})}$-multiplication, so by the Taniyama-Shimura formula, we know that

$$\begin{aligned} \mathfrak{a}^{f(\mathfrak{P}/\mathfrak{p})} &= \mathrm{N}_{\mathrm{K},\Phi}(\mathfrak{P}) \\ &= \mathrm{N}_{\Phi}(\mathrm{N}_{\mathrm{K}/\mathrm{E}^*}(\mathfrak{P}) \\ &= \mathrm{N}_{\Phi}(\mathfrak{p}^{\mathrm{f}(\mathfrak{P}/\mathfrak{p})}) \\ &= (\mathrm{N}_{\Phi}(\mathfrak{p}))^{\mathrm{f}(\mathfrak{P}/\mathfrak{p})} \end{aligned}$$

It follows that $\mathfrak{a} = N_{\Phi}(\mathfrak{p})$.

Furthermore, by the analogue of [10], Chapter VII, Proposition 3.1 for abelian varieties, reduction is injective on $A[m]$, so f agrees with σ on $A[m]$, so $\mathfrak{a}$ represents the class in $Cl_m(\mathcal{O}_E)$ associated to σ.

This means that the map $\sigma \to Cl_m(\mathcal{O}_E)$ is given by the composition of the Artin map for E^* composed with the extension of N_{Φ} to the ray class groups (*which exists since the norm preserves elements congruent to 1 modulo m for sufficiently large m). From this we find that the map factors through G_{L_m}, and we are done. □

15.1 Adelic Version

As in the case of elliptic curves, there is an adelic version of the main theorem. We remind the reader that $\mathrm{N}_{/\Phi}$ extends to a homomorphism from the ideles of E^* to those of E. We then have the following.

Theorem 15.4 (Fundamental Theorem of Complex Multiplication via Ideles)**.** *Let A/K be a CM abelian variety and $f : \mathbb{C}^g/\mathfrak{a} \to A$ a uniformization. Let s be an idele of E^* and σ an automorphism of $\overline{(K)}$ whose restriction to the maximal abelian extension of E^* is the Artin map applied to s. Let $r = \mathrm{N}_{\Phi}(\mathrm{s})$. Then there is a unique uniformization*

$$f' : \mathbb{C}/r^{-1}\mathfrak{a} \to \sigma(A)$$

such that r^{-1} agrees with σ on torsion points.

The proof that the ideal version implies the adelic version is almost the same as in the case of elliptic curves, involving an identical factorization for ideles of E^*.

16 Shimura Varieties and Complex Multiplication

We have a Galois (or equivalently class group) action on the isomorphism classes of elliptic curves with complex multiplication. We know that there is a variety, known as the modular curve $\Gamma(1)$, parametrizing these. We thus might expect an action on the points of the modular curve corresponding to CM elliptic curves. More generally, we recall that higher level modular curves correspond to "level structure," or torsion points, and we know that pairs of elliptic curves and torsion points have everything to do with complex multiplication, and we would similarly get an action. More generally, in the case of abelian varieties, the kind of data involved in the fundamental theorem of complex multiplication is, once again, the same as moduli data.

We should also recall the adelic description of modular curves. We express modular curves (or Shimura varieties, in general) as quotients of the adelic points of an algebraic group, and quotients by smaller and smaller open subgroups of the ideles (or adelic points of a reductive algebraic group) correspond to higher and higher level structures. Given that complex multiplication involves an adelic action, and smaller and smaller open subgroups correspond to higher and higher level structure, we expect to find a relation between these two descriptions. In fact, this description can be used to define the Galois action on Shimura varieties.

17 Honor Code

I pledge my honor that this paper represents my own work in accordance with university rules and regulations.

/David Corwin/

References

[1] Ghate, Eknath. Complex Multiplication. http://www.math.tifr.res.in/ eghate/cm.pdf

[2] Matsumura, Hideyuki. *Commutative Algebra.* Addison-Wesley, 1980.

[3] Milne, James. Complex Multiplication. http://www.jmilne.org/math/CourseNotes/cm.html.

[4] Milne, James. The Fundamental Theorem of Complex Multiplication. http://www.jmilne.org/math/articles/2007c.pdf.

[5] Neukirch, Jurgen. *Algebraic Number Theory*. Springer-Verlag, 1999.

[6] Rubin, Karl. Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer. Inventiones Mathematicae, 1981, Volume 64, Number 3, Pages 455-470.

[7] Serre, Jean-Pierre. Complex Multiplication in *Algebraic Number Theory*, ed. Cassels-Frohlich. Sandiego, CA: Academic Press.

[8] Serre, Jean-Pierre. *Abelian l-Adic Representations and Elliptic Curves*. Redwood City, CA: Addison-Wesley, Advanced Book Program, 1989.

[9] Silverman, Joseph H. *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, 1994.

[10] Silverman, Joseph H. *The Arithmetic of Elliptic Curves*. Dordrecht: Springer, 2009.