Complex multiplication*

Avi Zeff

1. The Shimura-Taniyama formula

Our next goal is to show that although a priori they are only defined over $\mathbb{C}$, every Shimura variety has a canonical model over some number field E. This is essentially equivalent to the statement that some $\mathrm{Aut}(\mathbb{C}/E)$, i.e. some finite index subgroup of $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, acts naturally on the points of the Shimura variety. Thus if we hope to find models over number fields the first thing to do is to describe the action of some $\mathrm{Aut}(\mathbb{C}/E)$ on the points of a Shimura variety. In the case where the Shimura variety has an interpretation as the moduli space of abelian varieties with some additional structure, this description is given by the theory of complex multiplication.

Given a complex abelian variety A of dimension g, there is a canonical way of viewing its $\mathbb{C}$-points as $\mathbb{C}^g/\Lambda$ for a lattice Λ. Namely, its tangent space $\mathrm{Lie}(A)$ at the identity is a complex vector space of dimension g, and the exponential map $\exp : \mathrm{Lie}(A) \to A(\mathbb{C})$ is surjective. Its kernel is some g-dimensional $\mathbb{Z}$-lattice Λ in $\mathrm{Lie}(A)$, so that canonically $A(\mathbb{C}) = \mathrm{Lie}(A)/\Lambda \simeq \mathbb{C}^g/\Lambda$. The N-torsion points in $A(\mathbb{C})$ are then in bijection with $\Lambda/N\Lambda$, since $\mathrm{Lie}(A)$ is torsion-free, and so $T_f(A) = \varprojlim_N A(\mathbb{C})[N] \simeq \Lambda \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$, $V_f(A) = T_f(A) \otimes \mathbb{Q} \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{A}_f$. Endomorphisms $a : A \to A$ of A induce endomorphisms $da : \mathrm{Lie}(A) \to \mathrm{Lie}(A)$ fixing Λ.

To talk about abelian varieties with complex multiplication, our next goal, we first need to introduce CM fields. A CM field E is a number field such that there exists a totally real subfield F of E such that E/F is an imaginary quadratic extension. If E is a CM field over F, then every embedding $j : F \hookrightarrow \mathbb{R}$ corresponds to two conjugate embeddings $\varphi_j, \overline{\varphi}_j$ of E into $\mathbb{C}$. A CM type Φ for E is a choice of one of φ_j or $\overline{\varphi}_j$ for each j. For example, if E is just an imaginary quadratic extension over the totally real field $\mathbb{Q}$, then a CM type for E is just a choice of embedding into $\mathbb{C}$.

Given a complex abelian variety A of dimension g and an action $i : E \to \mathrm{End}^0(A) = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ for a CM field E of degree $2g$ over $\mathbb{Q}$, we say that (A, i) is of CM-type Φ if for every $x \in E$, the action $di(x)$ on $\mathrm{Lie}(A)$ decomposes as

$$di(x) = \sum_{\varphi \in \Phi} \varphi(x).$$

(Note that although only integral elements of E actually act on A, all elements of E act on $\mathrm{Lie}(A)$ by $(qx)(v) = q \cdot x(v)$ for $x \in \mathcal{O}_E$ and $q \in \mathbb{Q}$.)

Given any A and $i : E \to \mathrm{End}^0(A)$ for E CM, (A, i) will always be of some CM type Φ. Indeed, since Λ is a $\mathbb{Z}$-lattice in $\mathrm{Lie}(A)$, tensoring with $\mathbb{R}$ gives all of $\mathrm{Lie}(A)$, and so tensoring with $\mathbb{C}$ gives $\Lambda \otimes_{\mathbb{Z}} \mathbb{C} = \mathrm{Lie}(A) \oplus \overline{\mathrm{Lie}(A)}$, where $x \in E$ acts on the second factor by $\overline{di(x)}$. This is a complex vector space of dimension $2g$. On the other hand, if we tensor with $\mathbb{Q}$ instead we obtain an algebra of dimension $2g$ over $\mathbb{Q}$, which also has an action of E

*These notes are based on chapters 10-11 of [1].

and so is one-dimensional over E. Therefore $\Lambda \otimes_{\mathbb{Z}} \mathbb{C} = (\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$ is an E-module and so decomposes as a sum of copies of $\mathbb{C}$ each with an E-algebra structure, i.e. an embedding $\varphi : E \to \mathbb{C}$. Since $\mathrm{Lie}(A)$ and $\overline{\mathrm{Lie}(A)}$ are submodules compatible with the E-action, each contains half of these copies of $\mathbb{C}$ with a φ-action; if φ occurs in $\mathrm{Lie}(A)$, then $\overline{\varphi}$ occurs in $\overline{\mathrm{Lie}(A)}$, so $\mathrm{Lie}(A)$ comes with a CM-type for E.

If A is simple, then any number field with the correct degree acting on A must be a CM field, but in general this is not true. For example, if C is an elliptic curve with complex multiplication by E, then $C \times C$ has an action (up to isogeny) of $M_2(E)$, and therefore of any field embedding into $M_2(E)$. But this includes all quadratic extensions of E, which need not be CM.

Just as it is possible to associate to any abelian variety with suitable action a CM type, we can also associate to a CM type an abelian variety of that type.

For a CM type (E, Φ), write $\mathbb{C}^\Phi$ for a direct sum of copies of $\mathbb{C}$ indexed by Φ, each with the corresponding E-action, and also write Φ for the morphism $\mathcal{O}_E \to \mathbb{C}^\Phi$ sending $x \mapsto (\varphi(x))_\varphi$.

Proposition 1.1. *With the notation above, the image $\Phi(\mathcal{O}_E) \subset \mathbb{C}^\Phi$ is a lattice, and the quotient $\mathbb{C}^\Phi/\Phi(\mathcal{O}_E)$ is an abelian variety A_Φ of CM-type (E, Φ), with the map $i_\Phi : E \to \mathrm{End}^0(A_\Phi)$ given by the action of φ on the φ'th factor. Moreover any other pair (A, i) of CM-type (E, Φ) is E-isogenous to (A_Φ, i_Φ).*

Proof. To show that the image of $\mathcal{O}_E$ is a lattice, we just need to show that tensoring with $\mathbb{R}$ gives all of $\mathbb{C}^\Phi$. By linearity this reduces to showing that for each φ we have $\varphi(\mathcal{O}_E) \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{C}$; fixing the embedding φ, we can think of this as just $\mathcal{O}_E \otimes_{\mathbb{Z},\varphi} \mathbb{R}$, which is the same thing as $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Q} \otimes_{\mathbb{Q},\varphi} \mathbb{R} = E \otimes_{\mathbb{Q},\varphi} \mathbb{R} \simeq E \otimes_{F,\varphi} \mathbb{R} \simeq \mathbb{C}$ since E is imaginary quadratic over F.

To show that the quotient is an abelian variety, it suffices to write down a Riemann form; one can work out that $(u, v) \mapsto \mathrm{Tr}_{E/\mathbb{Q}}(\alpha u v^*)$ works, where $*$ is the unique nontrivial automorphism of E over F and α is a totally imaginary element of E, i.e. one such that $\alpha^* = -\alpha$. By construction (A_Φ, i_Φ) is of CM-type (E, Φ).

Finally, suppose that (A, i) is of CM type (E, Φ), so that $\mathrm{Lie}(A)$ is isomorphic as an $E \otimes_{\mathbb{Q}} \mathbb{C}$-module to $\mathbb{C}^\Phi$. There is a canonical lattice Λ such that $A(\mathbb{C}) = \mathrm{Lie}(A)/\Lambda$, and so $A(\mathbb{C})$ is isomorphic to $\mathbb{C}^\Phi/\Lambda$, and the image of $\mathbb{Q}\Lambda$ is stable under the action of E via Φ. Therefore it must be equal to $\Phi(E)$ up to multiplication by some invertible scalar in $E \otimes_{\mathbb{Q}} \mathbb{R}$. After rescaling the isomorphism $\mathrm{Lie}(A) \simeq \mathbb{C}^\Phi$ by this scalar, we can assume $\mathbb{Q}\Lambda = \Phi(E)$, so there is some lattice Λ' in E mapping to Λ; but any such lattice is contained in $\frac{1}{N}\mathcal{O}_E$ for N sufficiently large, and so there is an isogeny $\mathbb{C}^\Phi/\Phi(\mathcal{O}_E) \to \mathbb{C}^\Phi/\Phi(N\Lambda') = \mathbb{C}^\Phi/N\Lambda$ defined over E. But multiplication by N gives an isogeny $A(\mathbb{C}) = \mathrm{Lie}(A)/\Lambda \simeq \mathbb{C}^\Phi/\Lambda \to \mathbb{C}^\Phi/N\Lambda$ over E, and so A is E-isogenous to $\mathbb{C}^\Phi/\Phi(\mathcal{O}_E) = A_\Phi$. □

We can also define CM types for abelian varieties defined over any (sufficiently large) subfield k of $\mathbb{C}$ in the same way. We say that a complex variety V has a model over k if there exists a variety V_0 and an isomorphism $(V_0)_{\mathbb{C}} \xrightarrow{\sim} V$, where $(V_0)_{\mathbb{C}}$ denotes the base change to $\mathbb{C}$ along $\mathrm{Spec}\,\mathbb{C} \to \mathrm{Spec}\,k$.

Proposition 1.2. *Let (A, i) be an abelian variety of CM-type (E, Φ) over $\mathbb{C}$. Then (A, i) has a model over $\overline{\mathbb{Q}}$, unique up to isomorphism, which is also an abelian variety with CM-type (E, Φ).*

Proof. To see uniqueness, it suffices to observe that the functor sending abelian varieties over $\overline{\mathbb{Q}}$ to their base change to $\mathbb{C}$ is fully faithful. The torsion points on $A(k)$ are Zariski dense for abelian varieties A and any algebraically closed field k, and over any such k the N-torsion points are isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{2\dim A}$, so any map of abelian varieties $A_{\mathbb{C}} \to B_{\mathbb{C}}$ is defined by its restriction to torsion points, all of which are defined over $\overline{\mathbb{Q}}$. Thus any automorphism of $\mathbb{C}/\mathbb{Q}$ fixes the morphism on torsion points and thus on the whole variety, i.e. every morphism $A_{\mathbb{C}} \to B_{\mathbb{C}}$ is actually defined over $\overline{\mathbb{Q}}$ and therefore this functor is fully faithful.

It remains to show existence, i.e. that if (A, i) is of CM-type (E, Φ) then it actually does arise from some model over $\overline{\mathbb{Q}}$. Consider the ring R generated over $\overline{\mathbb{Q}}$ by the coefficients of the polynomials defining A and i. There are finitely many of these, so R is finitely generated over $\overline{\mathbb{Q}}$. Any maximal ideal $\mathfrak{m}$ of R has residue field a finite extension of $\overline{\mathbb{Q}}$, i.e. $\overline{\mathbb{Q}}$ itself since it is algebraically closed; call the reduction of (A, i) modulo $\mathfrak{m}$ a specialization of (A, i). Then any such specialization (A', i') is also of CM-type (E, Φ), since passing from $\mathbb{C}$ to R to $\overline{\mathbb{Q}}$ does not change the eigenvalues of the action of some generator of E on the tangent space of A. By Proposition 1.1, the base change $(A', i')_{\mathbb{C}}$ is therefore isogenous to (A, i) over E since both have CM-type (E, Φ). The kernel H of this isogeny is a subgroup of the torsion points of $A'(\mathbb{C})$, which as above are all defined over $\overline{\mathbb{Q}}$ and so we can quotient by the kernel to get a pair $(A'/H, i)$ which is a model over $\mathbb{Q}$ for (A, i). □

Note that a model over $\overline{\mathbb{Q}}$ implies a model over some number field: A is defined over $\overline{\mathbb{Q}}$ by some polynomials, the coefficients of which all lie in $\overline{\mathbb{Q}}$ and thus are each in some number field. Taking the compositum of these fields gives a number field over which A is defined.

Proposition 1.2 implies for example that any elliptic curve over $\mathbb{C}$ of CM-type must have algebraic j-invariant, since the curve must be defined over $\overline{\mathbb{Q}}$ and the j-invariant is an algebraic function of the coordinates.

We say that an abelian variety A over a number field K has good reduction at a prime $\mathfrak{p}$ of K if it extends to an abelian scheme $\mathcal{A}$ over $\mathcal{O}_{K,\mathfrak{p}}$. Let $\bar{A} = \mathcal{A} \times_{\mathcal{O}_{K,\mathfrak{p}}} k$ be the special fiber of $\mathcal{A}$, i.e. the fiber over the finite field $k = \mathcal{O}_K/\mathfrak{p}$. This is called the reduction of A modulo $\mathfrak{p}$, and turns out to be independent of the choice of $\mathcal{A}$. There is an isomorphism of Tate modules $V_f(A) \simeq V_f(\bar{A})$ and an inclusion of endomorphism rings $\mathrm{End}(A) \hookrightarrow \mathrm{End}(\bar{A})$ compatible with this isomorphism, since both arise from the reduction.

There is a criterion for having good reduction over number fields, namely the Néron–Ogg–Shafarevich criterion: an abelian variety A over a number field K has good reduction at a prime $\mathfrak{p}$ of K if there is a prime ℓ different from the characteristic of $\mathcal{O}_K/\mathfrak{p}$ such that the inertia group at $\mathfrak{p}$ acts trivially on $T_\ell A$.

Proposition 1.3. *Let (A, i) be an abelian variety of CM-type (E, Φ) over a number field $K \subset \mathbb{C}$, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. After possibly replacing K by a finite extension, A will have good reduction at $\mathfrak{p}$.*

Proof. We apply the Néron–Ogg–Shafarevich criterion. In our case, $V_\ell A \simeq H_1(A_{\mathbb{C}}, \mathbb{Q}) \otimes \mathbb{Q}_\ell$ is a free $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of rank 1, since $H_1(A_{\mathbb{C}}, \mathbb{Q})$ is one-dimensional over E. Thus the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ factors through this action, i.e. the action of some subgroup of $(E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^\times$, which will automatically be compact. Any such subgroup will be a finite extension of a pro-ℓ subgroup. On the other hand I is a finite extension of a pro-p group for p the characteristic

of $\mathcal{O}_K/\mathfrak{p}$, so the image of I in this subgroup is finite; and by replacing K by a finite extension we can kill the image of I, so by applying the criterion we conclude that A has good reduction at $\mathfrak{p}$. □

Lemma 1.4. *Let (A, i) be an abelian variety of CM-type (E, Φ) over a number field $K \subset \mathbb{C}$ having good reduction at $\mathfrak{p}$ to $(\bar{A}, \bar{i})$ over $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_q$. Then the Frobenius $\pi = \pi_{\bar{A}}$ of $\bar{A}$ lies in $\bar{i}(E)$.*

Proof. It suffices to show the claim after tensoring with $\mathbb{Q}_\ell$, since whether $\pi \in \bar{i}(E)$ is determined by applying linear functionals which are independent of the base ring. Since $V_\ell A$ is a free $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of rank 1, so is $V_\ell \bar{A}$, and since π acts on $V_\ell \bar{A}$ and commutes with the action of $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ it is in $\mathrm{End}_{E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell} V_\ell \bar{A} = \bar{i}(E) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. □

In particular, given such a pair (A, i) with good reduction at $\mathfrak{p}$, identifying E with its image under $\bar{i}$ we get an element $\pi \in E$, which by the Weil conjectures for abelian varieties over finite fields is a q-integer, i.e. an algebraic integer satisfying $|\pi| = \sqrt{q}$ for every embedding into $\mathbb{C}$.

We'd like to be able to pin down π. As an element of E, up to a unit this is the same thing as specifying $\mathrm{ord}_v(\pi)$ for every place v of E. In fact, $\mathrm{ord}_v(\pi) = 0$ for $v \nmid p$ and π is determined up to a root of unity by specifying its valuation only at v dividing p, by the following lemma.

Lemma 1.5. *Let π and π' be q-integers in a number field E, with $\mathrm{ord}_v(\pi) = \mathrm{ord}_v(\pi')$ for every $v|p$, where $p = \mathrm{char}\, \mathbb{F}_q$. Then $\pi' = \zeta\pi$ for some root of unity ζ in E, and $\mathrm{ord}_v(\pi) = \mathrm{ord}_v(\pi') = 0$ for every finite place $v \nmid p$.*

Proof. Consider the automorphism of $\mathbb{Q}[\pi]$ sending $\pi \mapsto q/\pi$. In particular q/π is also an algebraic integer, so $\mathrm{ord}_v(q/\pi) = \mathrm{ord}_v(q) - \mathrm{ord}_v(\pi) \geq 0$ for every v and so $\mathrm{ord}_v(\pi) = 0$ for every finite $v \nmid p$ for any algebraic integer π and in particular also for π'. Therefore $\mathrm{ord}_v(\pi) = \mathrm{ord}_v(\pi')$ for every v, and since both are q-integers $|\pi|_v = |\pi'|_v$ for every place (finite or infinite) of v, i.e. $|\pi'/\pi|_v = 1$ for every v; this is true only for roots of unity. □

Indeed, we cannot hope to do better than specifying π up to a root of unity, because different choices of (A, i) with the same CM-type, though in the same isogeny class, may have different Frobenius elements; all these Frobenii will differ only by roots of unity, but we cannot eliminate all ambiguity. Up to this ambiguity, though, we can specify π as follows.

In the situation above, for each prime v of E over p let $H_v = H_{v,\mathfrak{p}}$ be the set of embeddings $E \hookrightarrow K$ such that the inverse image of $\mathfrak{p}$ is the prime ideal corresponding to v.

Theorem 1.6 (Shimura-Taniyama)**.** *Suppose that (A, i) is any abelian variety of CM-type (E, Φ) over a number field K containing all conjugates of E, and $\mathfrak{p}$ is a prime of K over p with residue field $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_q$ such that A has good reduction at $\mathfrak{p}$. Then for every place v of E over p, we have*

$$\mathrm{ord}_v(\pi) = \mathrm{ord}_v(q) \cdot \frac{|\Phi \cap H_v|}{|H_v|}.$$

We hope that such a formula is compatible with complex conjugation, and ours is: we have $\pi\bar{\pi} = q$ and so

$$\mathrm{ord}_v(\pi) + \mathrm{ord}_v(\bar{\pi}) = \mathrm{ord}_v(q)$$

and

$$\mathrm{ord}_v(\bar{\pi}) = \mathrm{ord}_{\bar{v}}(\pi),$$

and similarly

$$\Phi \cap H_{\bar{v}} = \overline{\Phi} \cap H_v.$$

Therefore our formula gives

$$\mathrm{ord}_v(q) = \mathrm{ord}_v(\pi) + \mathrm{ord}_v(\bar{\pi}) = \mathrm{ord}_v(q) \cdot \frac{|\Phi \cap H_v| + |\Phi \cap H_{\bar{v}}|}{|H_v|},$$

which in turn is just

$$\mathrm{ord}_v(q) \cdot \frac{|(\Phi \cup \overline{\Phi}) \cap H_v|}{|H_v|} = \mathrm{ord}_v(q)$$

as desired. In fact the formula of the theorem is the only one which is compatible with complex conjugation in this sense.

Any finitely generated $\mathcal{O}_E$-module M can be written uniquely as $\bigoplus_i \mathcal{O}_E/\mathfrak{p}_i^{r_i}$ for ideals $\mathfrak{p}_i$ and integers $r_i \geq 1$. Write $|M|_{\mathcal{O}_E}$ for the ideal $\prod_i \mathfrak{p}_i^{r_i}$, which is well-defined by the uniqueness of this decomposition.

In particular if A is an abelian variety of dimension g over $\mathbb{F}_q$ with a homomorphism $i : \mathcal{O}_E \to \mathrm{End}(A)$ for E a number field of degree $2g$ over $\mathbb{Q}$, this makes $\mathrm{Lie}(A)$ into an $\mathcal{O}_E$-module. It turns out that $|\mathrm{Lie}(A)|_{\mathcal{O}_E}$ is the ideal generated by the Frobenius (π_A).

In the situation of Theorem 1.6, since replacing A with an isogenous variety does not change the validity of the theorem we may do so to assume that $i(\mathcal{O}_E) \subseteq \mathrm{End}(A)$. By assumption A has good reduction at $\mathfrak{p}$, and so extends to an abelian scheme $\mathcal{A}$ over $\mathcal{O}_{K,\mathfrak{p}}$. This is smooth of relative dimension g and so the tangent space T over $\mathcal{O}_{K,\mathfrak{p}}$ is a free $\mathcal{O}_{K,\mathfrak{p}}$-module of rank g, with the corresponding action of $\mathcal{O}_E$, whose base change to K recovers $\mathrm{Lie}(A)$ and to $\mathbb{F}_q$ recovers $\mathrm{Lie}(\bar{A})$.

If p is unramified in E, then $T \otimes_{\mathcal{O}_{K,\mathfrak{p}}} K \simeq K^{\Phi}$ since (A, i) has CM-type (E, Φ), and this isomorphism restricts to an isomorphism of $\mathcal{O}_E$-module $T \xrightarrow{\sim} \mathcal{O}_{K,\mathfrak{p}}^{\Phi}$, i.e. T is a direct sum of copies of $\mathcal{O}_{K,\mathfrak{p}}$ indexed by $\varphi \in \Phi$ with the action by $\varphi : \mathcal{O}_E \to \mathcal{O}_K \subset \mathcal{O}_{K,\mathfrak{p}}$. Thus $\mathrm{Lie}(\overline{A}) = T \otimes_{\mathcal{O}_{K,\mathfrak{p}}} \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}$ is a direct sum of copies of $\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p} \simeq \mathbb{F}_q$ each with the action of $\mathcal{O}_E$ by $\varphi/\mathfrak{p} : \mathcal{O}_E \to \mathcal{O}_K \hookrightarrow \mathcal{O}_{K,\mathfrak{p}} \twoheadrightarrow \mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}$, and so as $\mathcal{O}_E$-modules the φ'th factor is (the preimage under φ of) the norm $\mathrm{Nm}_{K/\varphi(E)}\,\mathfrak{p}$, and so $|\mathrm{Lie}(\bar{A})|_{\mathcal{O}_E}$, which we observed earlier is just $(\pi_{\bar{A}})$, is the product of these ideals. For v a place of E over p, the only φ which contribute a nontrivial term to ord_v are those which are the preimage of $\mathfrak{p}$ under some embedding of E into K, i.e. those in H_v, so

$$\mathrm{ord}_v(\pi) = \sum_{\varphi \in \Phi \cap H_v} \deg(\mathfrak{p}/\varphi(v)).$$

We've assumed p is unramified in E, so $\mathrm{ord}_v(p) = 1$ for $v|p$ and so $\mathrm{ord}_v(q) = \deg(\mathfrak{p}/p)$, so $\deg(\mathfrak{p}/\varphi(v)) = \frac{\deg(\mathfrak{p}/p)}{\deg(\varphi(v)/p)}$. The denominator is just $|H_v|$ and is independent of φ, so this is

$$\mathrm{ord}_v(\pi) = \mathrm{ord}_v(q) \cdot \frac{|\Phi \cap H_v|}{|H_v|}$$

as claimed.

Without the assumption that p is unramified, the proof becomes more complicated but will still work. However it is actually not necessary: the unramified case suffices to prove the main theorem of complex multiplication (Theorem 2.2), which in turn implies Theorem 1.6.

2. The main theorem

We now turn to describing the action of complex multiplication. In the dimension 1 case, elliptic curves, curves with complex multiplication by a CM field E generate the maximal abelian extension E^{ab} of E, by describing the action of $\mathrm{Gal}(E^{\mathrm{ab}}/E)$ on the curve and its torsion points and then applying class field theory. We now want to extend this theory to higher-dimensional abelian varieties. In this case we need to introduce a reflex field E^*, which is the same as E in the one-dimensional case, such that complex multiplication by E corresponds to the action of $\mathrm{Gal}(E^{*\mathrm{ab}}/E^*)$. We then interpret this description in terms of the action of $\mathrm{Aut}(\mathbb{C}/E^*)$ on the complex points of a certain Shimura variety.

To define the reflex field, we need the following equivalence.

Proposition 2.1. *Let (E, Φ) be a CM type. The following conditions on a subfield E^* of $\overline{\mathbb{Q}}$ are equivalent:*

(a) the set of $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which fix E^* are exactly those which fix Φ;

(b) E^* is generated over $\mathbb{Q}$ by $\sum_{\varphi\in\Phi} \varphi(a)$ for $a \in E$;

(c) E^* is the smallest subfield k of $\overline{\mathbb{Q}}$ such that there exists a k-vector space V with an action of E such that

$$\mathrm{Tr}_k(a|V) = \sum_{\varphi\in\Phi} \varphi(a)$$

for every $a \in E$.

Any of these conditions uniquely specifies a number field E^*; we call this field the reflex field of (E, Φ).

Proof. First, suppose that σ fixes Φ; then certainly it fixes everything of the form $\sum_\varphi \in \Phi\varphi(a)$ for $a \in E$, and conversely if σ fixes such a sum then it must be permuting the φ, so conditions (a) and (b) are equivalent. If k is a field as in (c), then it contains every element as in (b) and so contains the field specified by (b). On the other hand the field from (b) does in fact have such an action: there is a representation of $E^\times$ with character the sum of the $\varphi \in \Phi$ (since (a) and (b) are equivalent), which extends by zero to an action of E with trace $\sum_{\varphi\in\Phi} \varphi(a)$, so the field from (b) satisfies the condition of (c) and is contained in any other such field, so is the smallest such field. □

By condition (c), there exists an E^*-vector space V with an action of E such that

$$\mathrm{Tr}_{E^*}(a|V) = \sum_{\varphi\in\Phi} \varphi(a)$$

for every $a \in E$; we could equivalently regard V as an $E^* \otimes_{\mathbb{Q}} E$-vector space, or as an E-vector space with an E-linear action of E^*. The reflex norm is the homomorphism $N_{\Phi^*} : \mathrm{Res}_{E^*/\mathbb{Q}}(\mathbb{G}_\mathrm{m}) \to \mathrm{Res}_{E/\mathbb{Q}}(\mathbb{G}_\mathrm{m})$ sending

$$a \mapsto \det_E(a|V)$$

for every $a \in E^*$. Since V is unique up to an isomorphism of $E \otimes_{\mathbb{Q}} E^*$-algebras, this homomorphism depends only on E and Φ (since E^* depends only on them).

If (A, i) is an abelian variety of CM-type (E, Φ) over $\mathbb{C}$. We know (by Proposition 1.2) that (A, i) has a model over $\overline{\mathbb{Q}}$, so we only need to study the action of automorphisms of $\overline{\mathbb{Q}}$ rather than all of $\mathbb{C}$; for any field K over which (A, i) is defined, $\mathrm{Lie}(A)$ gives a K-vector space with an action of E by $\mathrm{Tr}_K(a|\,\mathrm{Lie}(A)) = \sum_{\varphi\in\Phi} \varphi(a)$ for $a \in E$, and so by condition (c) K must contain E^*.

Theorem 2.2. *Let (A, i) be an abelian variety of CM-type (E, Φ) over $\mathbb{C}$, and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$. For any $s \in \mathbb{A}_{E^*,f}^\times$ whose image under $\mathbb{A}_{E^*,f}^\times \hookrightarrow \mathbb{A}_{E^*}^\times \to E^{*\times}\backslash\mathbb{A}_{E^*}^\times \xrightarrow{\mathrm{Art}} \mathrm{Gal}(E^{*\mathrm{ab}}/E^*)$ is σ, there exists a unique E-linear isogeny $\alpha : A \to \sigma A$ such that $\alpha(N_{\Phi^*}(s) \cdot x) = \sigma x$ for every $x \in V_f A$.*

Proof. Observe that $(\sigma A, \sigma i)$ is of CM type $(E, \sigma\Phi)$. Since σ fixes E^* by definition, by Proposition 2.1 (a) it fixes Φ, i.e. $\sigma\Phi = \Phi$, so $(\sigma A, \sigma i)$ is also of CM type (E, Φ), and therefore by Proposition 1.1 there is an E-isogeny $\alpha : A \to \sigma A$.

On $V_f(A)$, the composition

$$V_f(A) \xrightarrow{V_f(\sigma)} V_f(\sigma A) \xrightarrow{V_f(\alpha)^{-1}} V_f(A)$$

is E-linear and $\mathbb{A}_f$-linear, i.e. linear over $E \otimes_{\mathbb{Q}} \mathbb{A}_f = \mathbb{A}_{E,f}$. The Tate module is one-dimensional over $\mathbb{A}_{E,f}$, so this composition must be given by multiplication by some element a of $\mathbb{A}_{E,f}^\times$. Since α is well-defined up to an element of $E^\times$, a is well-defined, i.e. depends only on σ, as an element of $E^\times\backslash\mathbb{A}_{E,f}^\times$. Thus we get a map $\mathrm{Gal}(E^{*\mathrm{ab}}/E^*) \to E^\times\backslash\mathbb{A}_{E,f}^\times$ sending σ to a, which we can check is a homomorphism. Composing with the reciprocity map $E^{*\times}\backslash\mathbb{A}_{E^*,f}^\times \to \mathrm{Gal}(E^{*\mathrm{ab}}/E^*)$ this gives a map

$$E^{*\times}\backslash\mathbb{A}_{E^*,f}^\times \to E^\times\backslash\mathbb{A}_{E,f}^\times.$$

We might guess that this is the morphism induced from N_{Φ^*}. It suffices to check this on the Frobenius elements $(1, \ldots, 1, \pi_v, 1, \ldots)$ where π_v is a uniformizer for $\mathcal{O}_{E^*,v}$ and is in the vth place for every place v, since these generate $\mathbb{A}_{E^*,f}^\times$.

By Proposition 1.2, the abelian variety (A, i) with CM type (E, Φ) is actually defined over some number field K; by enlarging K suitably, we can assume that it contains all conjugates of E and has good reduction at a prime $\mathfrak{p}$ unramified over its intersection v with $\mathcal{O}_{E^*}$, which is over a prime p unramified in E. (Strictly speaking these conditions fail for some primes, but by restricting to the ray class group we could obtain all primes.)

Recall from the proof of Theorem 1.6 that the ideal generated by the Frobenius π of A at $\mathfrak{p}$ is given by

$$(\pi) = \prod_{\varphi\in\Phi} \varphi^{-1}(\mathrm{Nm}_{K/\varphi(E)}(\mathfrak{p})).$$

For $V = \mathrm{Lie}(A)$, this is just $N_{\Phi *}(\mathrm{Nm}_{K/E^*}(\mathfrak{p}))$, which is $N_{\Phi^*}(\mathcal{O}_E \cap \mathfrak{p})^f$ for some integer f (namely the degree of the extension of residue fields corresponding to $\mathfrak{p}$ over $\mathcal{O}_E \cap \mathfrak{p}$). On the other hand π is given by σ^f, up to some isogenies as above, and so σ is sent under this map to $N_{\Phi^*}(\mathcal{O}_E \cap \mathfrak{p})$. Thus the map is the one induced from N_{Φ^*}, so in particular for any $x \in V_f A$ and σ, s as in the statement of the theorem, $\alpha^{-1}(\sigma x) = ax$ for a the image of s under the map $E^{*\times}\backslash \mathbb{A}^\times_{E^*,f} \to E^\times \backslash \mathbb{A}^\times_{E,f}$ (up to changing α by a constant) which we know is just $N_{\Phi^*}(s)$. Therefore $\alpha^{-1}(\sigma x) = N_{\Phi^*}(s) \cdot x$ and so $\alpha(N_{\Phi^*}(s) \cdot x) = \sigma x$. □

References

[1] James S Milne. Introduction to Shimura varieties. *Harmonic analysis, the trace formula, and Shimura varieties*, 4:265–378, 2005.