Complex Multiplication

J.S. Milne

April 7, 2006

These are preliminary notes[1] for a modern account of the theory of complex multiplication. A shortened (minimal) version will be included in my book on Shimura varieties, and a complete longer version may one day be published separately.

v0.00 April 7, 2006. First version posted on the web; 113 pages.

Please send comments and corrections to me at math@jmilne.org.

Available at `http://www.jmilne.org/math`

[1] This should be taken seriously: there are omissions, repetitions, clumsy statements and proofs, and inconsistencies in notation.

Contents

Preface

> The theory of complex multiplication
> is not only the most beautiful part of
> mathematics but also of all science.
> D. Hilbert[2]

Abelian varieties with complex multiplication[3] are special in that they have the largest possible endomorphism rings. For example, the endomorphism ring of an elliptic curve is usually $\mathbb{Z}$, but when it is not, it is an order in an imaginary quadratic number field, and the elliptic curve is then said to have complex multiplication. Similarly, the endomorphism ring of a simple abelian variety of dimension g is usually $\mathbb{Z}$, but, at the opposite extreme, it may be an order in a number field of degree $2g$, in which case the abelian variety is said to have complex multiplication. Abelian varieties with complex multiplication correspond to special points on the moduli variety of abelian varieties, and their arithmetic is intimately related to that of the values of modular functions and modular forms at those points.

The first important result in the subject, which goes back to Kronecker and Weber, states that the Hilbert class field (maximal abelian unramified extension) of an imaginary quadratic subfield E of $\mathbb{C}$ is generated by the special value $j(\tau)$ of the j-function at any element τ of E in the complex upper half plane generating the ring of integers in E. Here j is the holomorphic function on the complex upper half plane invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$, taking the values 0 and 1728 respectively at $\frac{-1+\sqrt{-3}}{2}$ and $\sqrt{-1}$, and having a simple pole at infinity. The statement is related to elliptic curves through the ideal class group of E, which acts naturally both on the Hilbert class field of E and on the set of isomorphism classes of elliptic curves with endomorphism ring $\mathcal{O}_E$.

Generalizing this, Hilbert asked in the twelfth of his famous problems whether there exist holomorphic functions whose special values generate the abelian extensions (in particular, the class fields) of arbitrary number fields. For quadratic imaginary fields, the theory of elliptic curves with complex multiplication shows that elliptic modular functions have this property (Kronecker, Weber, Takagi, Hasse). Hecke began the study of abelian surfaces

[2] As quoted by Olga Taussky in her obituary for Hilbert in Nature, 152 (1943), 182–183. The following is from a letter she sent to me in October 1990:

> Yes it is true, Hilbert said this and I was in the audience when he said it and I was pleased he said it. It was at the Mathematiker Kongress Zürich 1932. Fueter ... had written an opus in 2 volumes: Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen, Teubner, 1924, 1927. Hilbert presided at Fueter's lecture.

[3] The name is both archaic and imprecise — the term "multiplication" is no longer used to denote an endomorphism, and "complex multiplication" is sometimes used to denote a more general class (Birkenhake and Lange 2004, p262) — but I know of no other.

with complex multiplication in the early 1900s, but the primitive state of algebraic geometry over fields other than $\mathbb{C}$ made this premature. It was not until the 1950s, after Weil had developed the theory of abelian varieties in arbitrary characteristic, that he, Shimura, and Taniyama were able to successfully extend the main statements of the theory of complex multiplication from elliptic curves to abelian varieties. While the resulting theory has provided only a partial answer to Hilbert's problem, it has played an essential role in the theory of modular (and, more generally, Shimura) varieties and in other aspects of number theory.

The complex points of a modular variety parametrize polarized abelian varieties over $\mathbb{C}$ together with a level structure; at a special point, the abelian variety has complex multiplication. To understand the arithmetic nature of the values of modular functions at these special points, it is necessary to understand how abelian varieties with complex multiplication and their torsion points behave under automorphisms of $\mathbb{C}$ (as an abstract field). For automorphisms of $\mathbb{C}$ fixing a certain "reflex" field attached to the abelian variety, this is the main content of the theory of Shimura, Taniyama, and Weil from the 1950s. Their results were extended to all automorphisms of $\mathbb{C}$ by the later work of Deligne, Langlands, and Tate.

NOTATIONS.

By a ***field*** we always mean a commutative field. A ***number field*** is a field of finite degree over $\mathbb{Q}$.[4] An algebraic closure of a field k is denoted k^{al}. We let $\mathbb{C}$ denote an algebraic closure of $\mathbb{R}$ and $\mathbb{Q}^{\mathrm{al}}$ the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. We often use $\overline{\mathbb{Q}}$ to denote an algebraic closure of $\mathbb{Q}$ (not necessarily $\mathbb{Q}^{\mathrm{al}}$). Complex conjugation on $\mathbb{C}$ (or a subfield) is denoted by ι or simply by $a \mapsto \overline{a}$. A ***complex conjugation*** on a field k is an involution induced by complex conjugation on $\mathbb{C}$ and an embedding of k into $\mathbb{C}$.[5] An automorphism σ of a field Ω is said to ***fix*** a subfield k if $\sigma a = a$ for all $a \in k$.

When k is a field, an ***étale algebra*** over k is a finite product of finite separable field extensions of k. Let E be an étale $\mathbb{Q}$-algebra, and let k be a field containing $\mathbb{Q}$. We say that k ***contains all conjugates of*** E if every $\mathbb{Q}$-algebra homomorphism $E \to k^{\mathrm{al}}$ maps into k; equivalently, if there are $[E\colon \mathbb{Q}]$ distinct $\mathbb{Q}$-algebra homomorphisms $E \to k$.

Rings are assumed to have a 1, homomorphisms of rings are required to map 1 to 1, and 1 acts on any module as the identity map. By a k-algebra (k a field) I mean a ring B containing k in its centre.

Following Bourbaki, I require compact topological spaces to be separated (Hausdorff).

Throughout, I use the notations standard in algebraic geometry, which sometimes conflict with those used in other areas. For example, if V and V' are algebraic varieties over a field k, then a morphism $V \to V'$ means a morphism (regular map) defined over k (not some "universal domain"). If K is a field containing k, then V_K is the algebraic variety over K obtained by extension of the base field and $V(K)$ is the set of points of V with coordinates in K.[6] If $\sigma\colon k \hookrightarrow K$ is a homomorphism of fields and V is an algebraic variety (or other algebro-geometric object) over k, then σV has its only possible meaning: apply σ to the coefficients of the equations defining V. The tangent space at a point P of a variety V is denoted $\mathrm{Tgt}_P(V)$.

[4] Following Kronecker (see Vlăduţ 1991, p12), we **do not** assume F to be a subfield of $\mathbb{C}$.

[5] More precisely, it is an automorphism ι' of order 2 of k such that $\rho \circ \iota' = \iota \circ \rho$ for some homomorphism $\rho\colon k \to \mathbb{C}$. Thus, a complex conjugation on k is defined by a homomorphism $\rho\colon k \to \mathbb{C}$ such that $\rho(k)$ is stable under ι but not fixed by it. The complex conjugations on $\mathbb{C}$ are the conjugates of ι by automorphisms of $\mathbb{C}$. According to a theorem of Artin (Collected Papers p257), the complex conjugations on $\overline{\mathbb{Q}}$ are exactly the elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of order 2.

[6] For those who know only schemes, $V(K) = \mathrm{Mor}_k(\mathrm{Spec}\, K, V)$.

Let A and B be sets and let $\sim$ be an equivalence relation on A. If there exists a canonical surjection $A \to B$ whose fibres are the equivalence classes, then I say that B classifies the elements of A modulo $\sim$ or that it classifies the $\sim$-classes of elements of A.

REFERENCES

In addition to those listed at the end, I refer to the following of my course notes (available at www.jmilne.org/math/).
AAG: Algebraic Groups and Arithmetic Groups, v1.0, May 22, 2005.
AG: Algebraic Geometry, v4.0, October 30, 2003.
ANT: Algebraic Number Theory, v2.1, August 31, 1998.
CFT: Class Field Theory, v3.1, May 6, 1997.
FT: Fields and Galois Theory, v3.0, August 31, 2003.
LEC: Lectures on Etale Cohomology, v2.01, August 9, 1998.
MF: Modular Functions and Modular Forms, v1.1, May 22, 1997.

PREREQUISITES

The reader is expected to have a good knowledge of basic algebraic number theory (e.g., ANT and parts of CFT), and basic algebraic geometry (e.g., AG and Hartshorne 1977, II) including abelian varieties (e.g., Milne 1986).

Chapter I

Analytic theory

1 CM-algebras and CM-types

Review of semisimple algebras and their modules

Fix a field k of characteristic zero. In this subsection, all k-algebras B, and all B-modules, will be of finite dimension over k.

A k-algebra is said to be ***semisimple*** if it has no nonzero nilpotent ideals[1], and it is said to be ***simple*** if it has no nonzero two-sided ideals. The Wedderburn theorems say that a semisimple k-algebra is a direct product of its minimal two-sided ideals, each of which is a simple k-algebra; moreover, each simple k-algebra is isomorphic to a matrix algebra over a division k-algebra. For example, a commutative semisimple k-algebra is simply a product of fields.

We now describe the modules over a semisimple k-algebra B. Every such module is semisimple, and hence a direct sum of simple modules. Thus, it suffices to describe the simple modules. Suppose $B \approx M_n(D)$, and choose an isomorphism; then D^n becomes a B-module under left multiplication; it is simple, and every simple B-module is isomorphic to it. Let $B = \prod_{1\le i\le n} B_i$ be the decomposition of B into a product of its simple ideals, and let S_i be a simple B_i-module. When we let B act on S_i through the projection $B \to B_i$, each S_i becomes a simple B-module, and every B-module is isomorphic to a direct sum of copies of the S_i, $S \approx \bigoplus_{i=1}^n r_i S_i$; moreover, $\bigoplus_{i=1}^n r_i S_i \approx \bigoplus_{i=1}^n r_i' S_i$ if and only if $r_i = r_i'$ for all i.

Let k' be a field containing k. If B is semisimple, then so also is $B' \stackrel{\text{def}}{=} B \otimes_k k'$ (here is where we use that k has characteristic zero), but the analogous statement with "simple" is false. Consider, for example, a simple $\mathbb{Q}$-algebra B, and let k be its centre. Then k is a field, and for a field K containing all conjugates of k and splitting B,

$$a \otimes c \leftrightarrow (\dots, \rho(a)c, \dots) \colon k \otimes_{\mathbb{Q}} K \simeq \prod_{\rho: k\to K} K$$
$$B \otimes_{\mathbb{Q}} K \approx \prod_{\rho: k\to K} M_n(K), \quad n^2 = [B\colon k].$$

Let $V_\rho = K^n$ be the simple $B \otimes_{\mathbb{Q}} K$-module corresponding to $\rho\colon k \to K$. Any $B \otimes_{\mathbb{Q}} K$-module isomorphic to $\bigoplus_\rho V_\rho$ is said to be ***reduced***.

[1] An ideal $\mathfrak{a}$ is ***nilpotent*** if $\mathfrak{a}^r = 0$ for some r. In particular, its elements are nilpotent.

PROPOSITION 1.1 *Let B be a simple $\mathbb{Q}$-algebra with centre k. Let K be a field containing all conjugates of k and splitting B, and let V be a $B \otimes_{\mathbb{Q}} K$-module. The characteristic polynomials $\det(T - b|V)$ of all elements b of B acting on the K-vector space V have coefficients in $\mathbb{Q}$ if and only if V is isomorphic to a multiple of the reduced $B \otimes_{\mathbb{Q}} K$-module (equivalently, V is free as a $k \otimes_{\mathbb{Q}} K$-module).*

PROOF. The isomorphism $\alpha\colon B \otimes_{\mathbb{Q}} K \to \prod_{\rho:k\to K} M_n(K)$ is well-determined up to conjugation by an element of $\prod_{\rho:k\to K} M_n(K)^\times$, and hence the characteristic polynomial $P_b(T)$ of $\alpha(b \otimes 1)$ for $b \in B$ is well-defined. It equals $\det(T - b|V)$ where V is the reduced module. For any automorphism σ of K, $\sigma(P_b(T)) = P_b(T)$. Enlarging K to a Galois extension of $\mathbb{Q}$ doesn't change $P_b(T)$, and so this shows that $P_b(T)$ has coefficients in $\mathbb{Q}$.

Any other $B \otimes_{\mathbb{Q}} K$-module M is isomorphic to a direct sum $\bigoplus_\rho m_\rho V_\rho$, $m_\rho \geq 0$. As $a \in k$ acts on V_ρ as multiplication by $\rho(a)$, the characteristic polynomial $P_{M,a}(T)$ of a on $\bigoplus_\rho m_\rho V_\rho$ is $\left(\prod_\rho (T - \rho a)^{m_\rho}\right)^n$. When a generates k, this has coefficients in $\mathbb{Q}$ if and only if the m_ρ are equal.[2] □

Let B be a semisimple k-algebra, and let $B = \prod B_i$ be its decomposition into a product of simple algebras B_i. The centre of each B_i is a field k_i, and each degree $[B_i\colon k_i]$ is a square. The ***reduced degree*** of B over k is defined to be

$$[B\colon k]_{\text{red}} = \sum\nolimits_i [B_i\colon k_i]^{1/2} \cdot [k_i\colon k].$$

For any field k' containing k,

$$\begin{aligned} [B\colon k] &= [B \otimes_k k'\colon k'], \text{ and} \\ [B\colon k]_{\text{red}} &= [B \otimes_k k'\colon k']_{\text{red}}. \end{aligned} \tag{1}$$

PROPOSITION 1.2 *Let B be a semisimple k-algebra. For any faithful B-module M,*

$$\dim_k M \geq [B\colon k]_{\text{red}},$$

and there exists a faithful module for which equality holds if and only if the simple factors of B are matrix algebras over their centres.

PROOF. Let $B = \prod B_i$ where $B_i \approx \prod M_{n_i}(D_i)$ with D_i a central division algebra over k_i, and let $S_i = D_i^{n_i}$ be a simple B_i-module. Then every B-module M is isomorphic to a sum $\bigoplus_i m_i S_i$, and M is faithful if and only if each $m_i > 0$. Therefore, if M is faithful,

$$\dim_k M = \sum\nolimits_i m_i \cdot n_i \cdot [D_i\colon k] \cdot [k_i\colon k] \geq \sum\nolimits_i n_i \cdot [D_i\colon k] \cdot [k_i\colon k].$$

On the other hand,

$$[B\colon k]_{\text{red}} = \sum\nolimits_i n_i \cdot [D_i\colon k]^{\frac{1}{2}} \cdot [k_i\colon k].$$

The proposition is now obvious. □

PROPOSITION 1.3 *Let B be a semisimple k-algebra. Every maximal étale k-subalgebra of B has degree $[B\colon k]_{\text{red}}$ over k.*

PROOF. When B is central simple, the proposition asserts that every maximal subfield of B containing k has degree $[B\colon k]^{\frac{1}{2}}$. This case is proved in CFT, IV 3.5, and the general case follows easily. □

[2] Let $c_a(T) = \prod_\rho (T - \rho a)$ be the characteristic polynomial of a in the field extension $k/\mathbb{Q}$. Because a generates k, $c_a(T)$ is irreducible. Any monic irreducible factor of $P_{M,a}(T)$ in $\mathbb{Q}[T]$ shares a root with $c_a(T)$, and therefore equals it. Hence, if $P_{M,a}(T)$ has coefficients in $\mathbb{Q}$, it is a power of $c_a(T)$.

CM-algebras

A number field E is said to be ***totally real*** if its image under every homomorphism $E \hookrightarrow \mathbb{C}$ is contained in $\mathbb{R}$. When the image is never contained in $\mathbb{R}$, the field is said to be ***totally imaginary***. Equivalently, E is totally real if $E \otimes_{\mathbb{Q}} \mathbb{R} \approx \mathbb{R}^{[E:\mathbb{Q}]}$ and it is totally imaginary if $E \otimes_{\mathbb{Q}} \mathbb{R} \approx \mathbb{C}^{[E:\mathbb{Q}]/2}$. A number field $\mathbb{Q}[\alpha] \simeq \mathbb{Q}[X]/(f(X))$ is totally real if all the roots of $f(X)$ are real and it is totally imaginary if none of the roots are real.

PROPOSITION 1.4 *The following conditions on a number field E are equivalent:*

(a) *E is a totally imaginary quadratic extension of a totally real number field;*
(b) *there exists an automorphism $\iota_E \neq \mathrm{id}$ of E such that $\rho \circ \iota_E = \iota \circ \rho$ for all homomorphisms $\rho\colon E \hookrightarrow \mathbb{C}$;*
(c) *$E = F[\alpha]$ with F totally real, $\alpha^2 \in F$, and $\rho(\alpha^2) < 0$ for all homomorphism $\rho\colon F \hookrightarrow \mathbb{C}$.*

PROOF. Assume (a), and let F be the totally real subfield. The unique nontrivial automorphism of E fixing F has the property required for (b). Let α generate E over F. After completing the square, we may suppose $\alpha^2 \in F$, and then $\rho(\alpha^2) < 0$ for every embedding $\rho\colon F \hookrightarrow \mathbb{C}$ because E is totally imaginary.

Assume (b). Then ι_E has order 2, because $\rho \circ \iota_E^2 = \rho$ for any $\rho\colon E \hookrightarrow \mathbb{C}$. Moreover, its fixed field F is totally real, and E is a totally imaginary quadratic extension of F.

Assume (c). Certainly, the conditions imply that E is a totally imaginary quadratic extension of F. □

Because they occur in the theory of complex multiplication, the fields satisfying these conditions are called ***CM-fields***. Note that a number field E is CM if and only if it has exactly one complex conjugation (by (b)). Clearly, any field isomorphic to a CM-field is CM.

COROLLARY 1.5 *A finite composite of CM-subfields of a field is CM; in particular, the Galois closure of a CM-field in any larger field is CM.*

PROOF. Clearly, each complex embedding of the composite of two CM-fields will induce the same nontrivial complex conjugation on the field. □

REMARK 1.6 Let $K \subset \mathbb{Q}^{\mathrm{al}}$ be a number field. If $\sigma\iota\sigma^{-1}$ acts on K as ι for every $\sigma \in \mathrm{Aut}(\mathbb{Q}^{\mathrm{al}})$, then K is totally real or is a CM-field according as ι fixes E or not. It follows that the union of all CM-subfields of $\mathbb{Q}^{\mathrm{al}}$ is the field fixed by the comutators $[\sigma,\iota] \stackrel{\mathrm{def}}{=} \sigma\iota\sigma^{-1}\iota^{-1}$ of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$, i.e., it is the subfield corresponding to the closure of the group generated by

$$\{[\sigma,\iota] \mid \sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})\}.$$

We denote this field by $\mathbb{Q}^{\mathrm{cm}}$.

REMARK 1.7 Let K be a number field. Since a composite of totally real fields is totally real, K contains a largest totally real subfield F. Moreover, K contains at most one totally imaginary quadratic extension of F, because any such extension is of the form $F[\sqrt{\alpha}]$ with α totally negative; if $F[\sqrt{\beta}]$ is a second such extension, then K contains the totally real field $F[\sqrt{\alpha\beta}]$, which must equal F, and this implies that $F[\sqrt{\alpha}] = F[\sqrt{\beta}]$. If K contains a CM-field E, then $K' \stackrel{\mathrm{def}}{=} E \cdot F$ is the largest CM-subfield of K. It consists of all elements α of K having a conjugate α' in K such that $\rho(\alpha') = \overline{\rho(\alpha)}$ for all embeddings $\rho\colon K \to \mathbb{C}$. For any such embedding, $\rho K' = \rho K \cap \mathbb{Q}^{\mathrm{cm}}$.

A ***CM-algebra*** is a finite product of CM-fields. Equivalently, it is a finite product of number fields admitting an automorphism ι_E that is of order 2 on each factor and such that $\iota \circ \rho = \rho \circ \iota_E$ for all homomorphisms $\rho: E \to \mathbb{C}$. The fixed algebra of ι_E is a product of the largest totally real subfields of the factors. Sometimes we call ι_E complex conjugation and write $\overline{a}$ for $\iota_E a$.

CM-types.

Let E be a CM-algebra. The $\mathbb{Q}$-algebra of homomorphisms $E \to \mathbb{C}$ occur in complex conjugate pairs $\{\varphi, \iota \circ \varphi\}$. A CM-type on E is the choice of one element from each such pair. More formally:

DEFINITION 1.8 A ***CM-type*** on a CM-algebra is a subset $\Phi \subset \mathrm{Hom}(E, \mathbb{C})$ such that

$$\mathrm{Hom}(E, \mathbb{C}) = \Phi \sqcup \iota\Phi \qquad (\text{disjoint union; } \iota\Phi \stackrel{\text{def}}{=} \{\iota \circ \varphi \mid \varphi \in \Phi\}).$$

Alternatively, we may regard a CM-type as a function $\phi: \mathrm{Hom}(E, \mathbb{C}) \to \{0, 1\}$ (the characteristic function of Φ) such that

$$\phi(\rho) + \phi(\iota \circ \rho) = 1 \text{ for all } \rho \in \mathrm{Hom}(E, \mathbb{C}). \tag{2}$$

Let F be the product of the largest totally real subfields of the factors of E. Choosing a CM-type Φ on E amounts to choosing an extension ρ' to E of each embedding $\rho: F \to \mathbb{R}$, and hence an isomorphism of $\mathbb{R}$-algebras

$$E \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\Phi} \prod\nolimits_{\rho: F \to \mathbb{R}} \mathbb{C}, \quad a \otimes r \mapsto (\rho' a \cdot r)_\rho, \quad \Phi = \{\rho' \mid \rho: F \to \mathbb{R}\}. \tag{3}$$

A pair (E, Φ) (or (E, ϕ)) consisting of a CM-algebra E and a CM-type Φ (or ϕ) for E will be called a ***CM-pair***.

Let E_0 be a CM-subalgebra of a CM-algebra E. Every CM-type Φ_0 on E_0, extends to a CM-type on E, namely, to

$$\Phi \stackrel{\text{def}}{=} \{\varphi: E \to \mathbb{C} \mid \varphi | E_0 \in \Phi_0\},$$

and a CM-type Φ on E arises in this way from a CM-type on E_0 if and only if

$$\Phi | E_0 \stackrel{\text{def}}{=} \{\varphi | E_0 \mid \varphi \in \Phi\}$$

is a CM-type on E_0, i.e., no two of the φ in Φ become complex conjugates on E_0 (or, if two elements of Φ have the same restriction to F_0, then they have the same restriction to E_0).

A CM-pair (E, Φ), or just Φ itself, is ***primitive*** if E is a field and there does not exist a proper CM-subfield E_0 of E such that $\Phi | E_0$ is a CM-type on E_0.

PROPOSITION 1.9 *Every CM-pair (E, Φ) with E a field is the extension of a unique primitive CM-pair (E_0, Φ_0) with $E_0 \subset E$. In fact, for any CM-field E_1 containing E and Galois over $\mathbb{Q}$, E_0 is the fixed field of*

$$H = \{\sigma \in \mathrm{Gal}(E_1/\mathbb{Q}) \mid \Phi_1 \sigma = \Phi_1\}.$$

Here Φ_1 is the extension of Φ_0 to E_1 and $\Phi_1 \sigma = \{\varphi \circ \sigma \mid \varphi \in \Phi_1\}$.

PROOF. Assume initially that E is Galois over $\mathbb{Q}$, and define E_0 to be the fixed subfield of $H = \{\sigma \in \mathrm{Gal}(E/\mathbb{Q}) \mid \Phi\sigma = \Phi\}$.

(A) E_0 is a CM-subfield of E and $\Phi|E_0$ is a CM-type on E_0.

As E is a CM-field,

$$\Phi\iota_E = \iota\Phi \neq \Phi,$$

and so ι_E is not in H; it therefore acts nontrivially on E_0. To show that E_0 is a CM-subfield, it remains to show that it is stable under ι_E, i.e., that $\sigma\iota_E a = \iota_E a$ for all $\sigma \in H$ and $a \in E_0$. But, for $\sigma \in H$,

$$\Phi\iota_E\sigma\iota_E = \iota\Phi\sigma\iota_E = \iota\Phi\iota_E = \Phi,$$

and so $\iota_E\sigma\iota_E \in H$. This implies that $\sigma\iota_E a = \iota_E a$ for all $a \in E_0$.

If $\Phi|E_0$ is not a CM-type, then

$$\varphi'|E_0 = \iota \circ \varphi|E_0 \tag{4}$$

for distinct $\varphi, \varphi' \in \Phi$. But (4) implies that $\iota \circ \varphi \in \varphi' H \subset \Phi$, which is a contradiction.

(B) If E' is a CM-subfield of E and $\Phi|E'$ is a CM-type on E', then $E' \supset E_0$.

The conditions imply that Φ is the extension to E of the CM-type $\Phi' \stackrel{\text{def}}{=} \Phi|E'$ on E'. Let σ be an element of G fixing E'. Then $\Phi'\sigma = \Phi'$, which implies that $\Phi\sigma = \Phi$, and so $\sigma \in H$.

(A) and (B) prove the proposition when E is Galois over $\mathbb{Q}$. In the general case, we can embed E in a CM-field E_1 Galois over $\mathbb{Q}$ and extend Φ to a CM-type Φ_1 on E_1. The preceding argument applied to (E_1, Φ_1) gives a smallest CM-field $E_0 \subset E$ such that $\Phi|E_0$ is a CM-type on E_0. □

COROLLARY 1.10 *A CM-pair (E, Φ) is primitive if and only if for some (hence all) CM-fields E_1 containing E and Galois over $\mathbb{Q}$, the subgroup of $\mathrm{Gal}(E_1/\mathbb{Q})$ fixing E is*

$$\{\sigma \in \mathrm{Gal}(E_1/\mathbb{Q}) \mid \Phi_1\sigma = \Phi_1\}$$

where Φ_1 is the extension of Φ to E_1.

PROOF. Immediate from the proposition. □

EXERCISE 1.11 (Shimura and Taniyama 1961, 8.2 = Shimura 1998, 8.2). Let E be a CM-field, and write $E = F[\alpha]$ with $\alpha^2 \in F$ and totally negative. The embeddings $\varphi: E \to \mathbb{C}$ such that $\Im(\varphi(\alpha)) > 0$ form a CM-type Φ on E. Show that (E, Φ) is primitive if and only if

(a) $F[\alpha] = \mathbb{Q}[\alpha]$, and
(b) for any conjugate α' of α over $\mathbb{Q}$ other than α itself, α'/α is not totally positive.

EXERCISE 1.12 (ibid. 8.4). Let $E = \mathbb{Q}[\zeta]$ where ζ is a primitive 13^{th} root of 1 in $\mathbb{C}$. Of the 32 CM-types on E containing the given embedding of E into $\mathbb{C}$, show that only 2 are nonprimitive, and that the remaining 30 CM-types fall into 6 orbits under the action of $\mathrm{Gal}(E/\mathbb{Q})$, each with 5 elements.

DEFINITION 1.13 Let E be an étale $\mathbb{Q}$-algebra, and let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. A ***CM-type*** on E with values in $\overline{\mathbb{Q}}$ is a subset Φ of $\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(E, \overline{\mathbb{Q}})$ such that

$$\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(E, \overline{\mathbb{Q}}) = \Phi \sqcup \sigma\Phi$$

for *all* complex conjugations σ on $\overline{\mathbb{Q}}$.

Note that when E is a CM-algebra and $\overline{\mathbb{Q}} = \mathbb{Q}^{\mathrm{al}}$, this agrees with Definition 1.8.

EXERCISE 1.14 Let Φ be a CM-type on a field E with values in $\overline{\mathbb{Q}}$. Show that there exists a CM-subfield E_0 of E such that no two elements of Φ are complex conjugates on E_0 (and hence there is a CM-type Φ_0 on E_0 such that $\Phi = \{\varphi\colon E \to \overline{\mathbb{Q}} \mid \varphi|E_0 \in \Phi_0\}$).

EXERCISE 1.15 Rewrite this subsection replacing $\mathbb{Q}^{\mathrm{al}}$ and $\mathbb{C}$ with $\overline{\mathbb{Q}}$.

The reflex field of a CM-pair

If σ is an automorphism of $\mathbb{C}$ (or $\mathbb{Q}^{\mathrm{al}}$) and Φ is a CM-type on a CM-algebra E, then

$$\sigma\Phi \stackrel{\text{def}}{=} \{\sigma \circ \varphi \mid \varphi \in \Phi\}$$

is again a CM-type on E.[3]

PROPOSITION 1.16 *Let (E, Φ) be a CM-pair. The following conditions on a subfield E^* of $\mathbb{Q}^{\mathrm{al}}$ are equivalent:*

(a) *$\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ fixes E^* if and only if $\sigma\Phi = \Phi$;*
(b) *E^* is the subfield of $\overline{\mathbb{Q}}$ generated by the elements $\sum_{\varphi\in\Phi}\varphi(a)$, $a \in E$.*

PROOF. If $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ permutes the φ's in Φ, then clearly it fixes all elements of the form $\sum_{\varphi\in\Phi}\varphi(a)$. Conversely, if

$$\textstyle\sum_{\varphi\in\Phi}\varphi(a) = \sum_{\varphi\in\Phi}(\sigma\circ\varphi)(a) \text{ for all } a \in E^\times,$$

then $\{\sigma \circ \varphi \mid \varphi \in \Phi\} = \Phi$ by Dedekind's theorem on the independence of characters (FT 5.14).[4] This shows that conditions (a) and (b) define the same field. □

DEFINITION 1.17 The field satisfying the equivalent conditions in the proposition is called the ***reflex field*** E^* of (E, Φ).

Note that, in contrast to E, which need not even be a field, E^* is a *sub*field of $\mathbb{Q}^{\mathrm{al}}$.

PROPOSITION 1.18 *Let (E, Φ) be a CM-pair.*

(a) *The reflex field E^* of (E, Φ) is a CM-field.*
(b) *If $(E, \Phi) = \prod_{1\le i\le m}(E_i, \Phi_i)$, then $E^* = E_1^* \cdots E_m^*$.*
(c) *The reflex field of any extension (E_1, Φ_1) of (E, Φ) equals that of (E, Φ).*

[3] Note that, because E is CM,

$$\iota\circ(\sigma\circ\varphi) = (\sigma\circ\varphi)\circ\iota_E = \sigma\circ(\iota\circ\varphi);$$

therefore, if $\iota\circ(\sigma\circ\varphi) = \sigma\circ\varphi'$, then $\sigma\circ(\iota\circ\varphi) = \sigma\circ\varphi'$ and $\iota\circ\varphi = \varphi'$. Hence $\sigma\Phi \cap \iota\sigma\Phi = \emptyset$, and it follows (by counting) that $\mathrm{Hom}(E, \mathbb{C}) = \sigma\Phi \sqcup \iota\sigma\Phi$.

[4] In more detail, the equation says that

$$\textstyle\sum_{\varphi\in\sigma\Phi}\varphi - \sum_{\varphi\in\Phi}\varphi = 0,$$

and Dedekind's theorem says that this is possible only if each φ in Φ occurs exactly once in $\sigma\Phi$.

PROOF. (a) Let $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ and $a \in E$. Because E is a CM-algebra,

$$\begin{aligned}\sigma\iota\left(\sum_{\varphi\in\Phi}\varphi(a)\right) &= \sigma\left(\sum_{\varphi\in\Phi}\varphi(\iota_E a)\right)\\ &= \sum_{\varphi\in\Phi}(\sigma\circ\varphi)(\iota_E a)\\ &= \iota\left(\sum_{\varphi\in\Phi}(\sigma\circ\varphi)(a)\right)\\ &= \iota\sigma\left(\sum_{\varphi\in\Phi}\varphi(a)\right),\end{aligned}$$

and so E^* is either CM or totally real (cf. 1.6). As $\iota\Phi \neq \Phi$, it must be CM.

(b) Because $\Phi = \Phi_1 \sqcup \ldots \sqcup \Phi_n$ as $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$-sets,

$$\{\sigma \mid \sigma\Phi = \Phi\} = \bigcap\nolimits_i \{\sigma \mid \sigma\Phi_i = \Phi_i\}.$$

(c) Clearly $\sigma\Phi_1 = (\sigma\Phi)_1$, and so $\sigma\Phi_1 = \Phi_1 \iff \sigma\Phi = \Phi$. □

EXAMPLE 1.19 Consider a CM-pair (E, Φ) with E a subfield of $\mathbb{Q}^{\mathrm{al}}$. Let E_1 be the Galois closure of E in $\mathbb{Q}^{\mathrm{al}}$, and let Φ_1 be the extension of Φ to E_1. Regard the elements of Φ_1 as automorphisms of E_1, and let $\Phi_1^{-1} = \{\varphi^{-1} \mid \varphi \in \Phi_1\}$. Then Φ_1^{-1} is a CM-type on E_1, and the primitive subpair (E_0, Φ_0) of (E_1, Φ_1^{-1}) (see 1.9) has $E_0 = E^*$, the reflex field of (E, Φ).[5] The pair (E_0, Φ_0) is denoted (E^*, Φ^*) and called the ***reflex CM-pair***of $(E \subset \mathbb{C}, \Phi)$ (and Φ^* is called the ***reflex CM-type*** of Φ).

EXERCISE 1.20 Rewrite this subsection replacing $\mathbb{Q}^{\mathrm{al}}$ and $\mathbb{C}$ with $\overline{\mathbb{Q}}$. Is it necessary to assume that E is a CM-algebra?

The reflex norm.

In this subsection, $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$ (not necessarily *the* algebraic closure in $\mathbb{C}$). By a CM-pair we mean a CM-algebra E together with a subset $\Phi \subset \mathrm{Hom}(E, \overline{\mathbb{Q}})$ such that

$$\mathrm{Hom}(E, \overline{\mathbb{Q}}) = \Phi \sqcup \iota'\Phi$$

for one (hence every) complex conjugation ι' on $\overline{\mathbb{Q}}$. The reflex field E^* of (E, Φ) is the subfield of $\overline{\mathbb{Q}}$ generated by the elements $\sum_{\varphi\in\Phi}\varphi(a)$ with $a \in E$, and

$$\mathrm{Gal}(\overline{\mathbb{Q}}/E^*) = \{\sigma \mid \sigma\Phi = \Phi\}.$$

Let k be a number field. To give a finitely generated $E \otimes_{\mathbb{Q}} k$-module amounts to giving a finite dimensional $\mathbb{Q}$-vector space together with commuting $\mathbb{Q}$-linear actions of E and k (i.e., an (E, k)-bimodule over $\mathbb{Q}$), or a finite dimensional k-vector space V together with a k-linear action of E (i.e., an action of E on V such that each $a \in E$ acts by k-linear endomorphisms).

[5] Recall (1.9) that E_0 is the fixed field of the group

$$\{\sigma \mid \Phi_1^{-1}\sigma = \Phi_1^{-1}\},$$

and (1.16) that E^* is the fixed field of the group

$$\{\sigma \mid \sigma\Phi = \Phi\} = \{\sigma \mid \sigma\Phi_1 = \Phi_1\}.$$

Obviously, these groups are equal.

PROPOSITION 1.21 *Let (E,Φ) be a CM-pair, and let k be a subfield of $\overline{\mathbb{Q}}$. There exists a finitely generated $E\otimes_{\mathbb{Q}}k$-module V such that*

$$\mathrm{Tr}_k(a|V)=\textstyle\sum_{\varphi\in\Phi}\varphi(a),\quad \text{all } a\in E, \tag{5}$$

if and only if $k\supset E^*$, in which case V is uniquely determined up to an $E\otimes_{\mathbb{Q}}k$-isomorphism.

PROOF. If a acts k-linearly on V, then $\mathrm{Tr}_k(a|V)\in k$, and so, if there exists a k-linear action of E satisfying (5) on a k-vector space V, then certainly $k\supset E^*$.

For the converse, we initially assume that k contains all the conjugates of E. There is then a canonical isomorphism

$$e\otimes a\mapsto(\rho e\cdot a)_\rho\colon E\otimes_{\mathbb{Q}}k\to\textstyle\prod_{\rho:E\to k}k,$$

and so any $E\otimes_{\mathbb{Q}}k$-module V is of the form $\bigoplus m_\rho k_\rho$ for unique nonnegative integers m_ρ, where k_ρ denotes a one-dimensional k-vector space on which $e\in E$ acts as $\rho(e)$. Thus, up to isomorphism, there exists exactly one $E\otimes_{\mathbb{Q}}k$-module satisfying (5), namely, $\bigoplus_{\varphi\in\Phi}k_\varphi$.

For a general k containing E^*, we use the following statement:

> Let Ω be a finite Galois extension of k with Galois group Γ; the functor $V\mapsto\Omega\otimes_k V$ is an equivalence from the category of k-vector spaces to the category of Ω-vector spaces endowed with a semilinear action of Γ (see AG 16.14; an action is semilinear if $\gamma(av)=\gamma a\cdot\gamma v$ for $\gamma\in\Gamma$, $a\in\Omega$, $v\in V$).

Let Ω be any finite Galois extension Ω of k containing all conjugates of E. Consider the $E\otimes_{\mathbb{Q}}\Omega$-module $\bigoplus_{\varphi\in\Phi}\Omega_\varphi$, where Ω_φ is a one-dimensional Ω-vector space on which $e\in E$ acts as $\varphi(e)$. Because Φ is stable under Γ, we can define a semilinear action of Γ on $\bigoplus_{\varphi\in\Phi}\Omega_\varphi$ by the rule

$$\gamma(\dots,\overset{\varphi}{v},\dots)=(\dots,\overset{\gamma\circ\varphi}{\gamma v},\dots),\quad \gamma\in\Gamma,$$

and one checks that this is the *only* such action commuting with the action of E.[6] Any $E\otimes_{\mathbb{Q}}k$-module satisfying (5) becomes isomorphic to $\prod_{\varphi\in\Phi}\Omega_\varphi$ over Ω, and so this shows that, up to isomorphism, there exists exactly one such $E\otimes_{\mathbb{Q}}k$-module. □

COROLLARY 1.22 *The reflex field E^* is the smallest subfield of $\overline{\mathbb{Q}}$ such that there exists an $E\otimes_{\mathbb{Q}}E^*$-module V with*

$$V\otimes_{E^*}\overline{\mathbb{Q}}\simeq\bigoplus\nolimits_{\varphi\in\Phi}\overline{\mathbb{Q}}_\varphi\qquad\text{(as an } E\otimes_{\mathbb{Q}}\overline{\mathbb{Q}}\text{-module)} \tag{6}$$

where $\overline{\mathbb{Q}}_\varphi$ is a one-dimensional $\overline{\mathbb{Q}}$-vector space on which E acts through φ.

PROOF. Restatement of the proposition. □

[6] Use that

$$\Omega_\varphi=\{x\in V\mid a\cdot x=\varphi(a)x \text{ all } a\in E\}.$$

Let V_Φ be an $E \otimes_{\mathbb{Q}} k$-module satisfying (5). An element a of k defines an endomorphism of V_Φ regarded as an E-vector space, whose determinant we denote by $\det_E(a|V_\Phi)$. If $a \in k^\times$, then $\det_E(a|V_\Phi) \in E^\times$, and so in this way we get a homomorphism

$$N_{k,\Phi}\colon k^\times \to E^\times.$$

More generally, for any $\mathbb{Q}$-algebra R and invertible element of a of $k \otimes_{\mathbb{Q}} R$, we get an invertible element

$$N_{k,\Phi}(a) = \det_{E\otimes_{\mathbb{Q}}R}(a|V_\Phi \otimes_{\mathbb{Q}} R)$$

of $E \otimes_{\mathbb{Q}} R$. In this way, we get a homomorphism

$$N_{k,\Phi}(R)\colon (k \otimes_{\mathbb{Q}} R)^\times \to (E \otimes_{\mathbb{Q}} R)^\times$$

which is functorial in R and independent of the choice of V_Φ. It is called the ***reflex norm*** from k to E (relative to Φ). When $k = E^*$, we drop it from the notation.

PROPOSITION 1.23 *For any number field k with $E^* \subset k \subset \overline{\mathbb{Q}}$,*

$$N_{k,\Phi} = N_\Phi \circ \mathrm{Nm}_{k/E^*}. \tag{7}$$

PROOF. Choose an $E \otimes_{\mathbb{Q}} E^*$-module V_Φ satisfying (6), and let $V' = k \otimes_{E^*} V_\Phi$. When we use V' to compute $N_{k,\Phi}$, and V_Φ to compute N_Φ, we obtain (7). □

REMARK 1.24 (a) For any isomorphism $\sigma\colon E \to E'$,

$$N_{\Phi\sigma}(a) = \sigma N_\Phi(a), \text{ all } a \in E^*,$$

where $\Phi\sigma = \{\varphi \circ \sigma \mid \varphi \in \Phi\}$.

(b) Let V_Φ be an $E \otimes_{\mathbb{Q}} k$-module satisfying (5). Then $V_\Phi \oplus V_{\iota\Phi}$ satisfies

$$\mathrm{Tr}_k(a|V) = \sum\nolimits_{\rho\colon E\to\overline{\mathbb{Q}}} \rho(a), \text{ all } a \in E.$$

Therefore $V_\Phi \oplus V_{\iota\Phi}$ is a free $E \otimes_{\mathbb{Q}} k$-module of rank 1, and so

$$N_\Phi(a) \cdot N_{\iota\Phi}(a)$$

Therefore $V_\Phi \oplus V_{\iota\Phi}$ is free of rank 1, and so

$$N_\Phi(a) \cdot N_{\iota\Phi}(a) = \mathrm{Nm}_{k/\mathbb{Q}}(a), \text{ all } a \in k^\times. \tag{8}$$

Since $N_{\iota\Phi}(a) = N_{\Phi\iota_E}(a) = \iota_E N_\Phi(a)$, this can be rewritten as

$$N_\Phi(a) \cdot \iota_E N_\Phi(a) = \mathrm{Nm}_{k/\mathbb{Q}}(a), \text{ all } a \in k^\times. \tag{9}$$

More generally, for any $\mathbb{Q}$-algebra R,

$$N_\Phi(a) \cdot \iota_E N_\Phi(a) = \mathrm{Nm}_{k\otimes_{\mathbb{Q}}R/R}(a), \text{ all } a \in (k \otimes_{\mathbb{Q}} R)^\times. \tag{10}$$

REMARK 1.25 In terms of algebraic tori (see §4), $N_{k,\Phi}$ is a homomorphism $T^k \to T^E$, where T^k and T^E are the algebraic tori over $\mathbb{Q}$ with $\mathbb{Q}$-points $k^\times$ and $E^\times$ respectively (i.e., $T^k = (\mathbb{G}_m)_{k/\mathbb{Q}}$ and $T^E = (\mathbb{G}_m)_{E/\mathbb{Q}}$).

Let F be the largest totally real subalgebra of E. The norm $a \mapsto a \cdot \iota_E a\colon E^\times \to F^\times$ defines a homomorphism $T^E \to T^F$, and we let T equal the fibre product $T = \mathbb{G}_m \times_{T^F} T^E$:

$$\begin{array}{ccc} T & \longrightarrow & T^E \\ \downarrow & & \downarrow \\ \mathbb{G}_m & \longrightarrow & T^F. \end{array}$$

Thus T is the subtorus of T^E with

$$T(\mathbb{Q}) = \{a \in E^\times \mid a \cdot i_E a \in F^\times\}.$$

Equation (10) shows that the homomorphism $N_{k,\Phi}\colon T^k \to T^E$ factors through $T \subset T^E$.

From $N_{k,\Phi}$ we obtain homomorphisms (by taking $R = \mathbb{Q}, \mathbb{Q}_l, \mathbb{R}$):

$$\begin{aligned} N_0&\colon k^\times \to E^\times, \\ N_l&\colon k_l^\times \to E_l^\times, \quad k_l = k \otimes_{\mathbb{Q}} \mathbb{Q}_l, \quad E_l = E \otimes_{\mathbb{Q}} \mathbb{Q}_l, \\ N_\infty&\colon k_\infty^\times \to E_\infty^\times, \quad k_\infty = k \otimes_{\mathbb{Q}} \mathbb{R}, \quad E_\infty = E \otimes \mathbb{R}. \end{aligned}$$

From these maps, we get a continuous homomorphism on the groups of idèles $\mathbb{A}_k^\times \to \mathbb{A}_E^\times$ which is compatible with N_0, and hence induces a homomorphism on the idèle classes. Moreover, the homomorphism on the finite idèles passes to the quotient and defines a homomorphism $N_{k,\Phi}$ on the groups of fractional ideals, which is compatible with N_0, and so induces a homomorphism on the ideal classes.

PROPOSITION 1.26 *Let $k \subset \overline{\mathbb{Q}}$ be a finite extension of E^* containing all conjugates of E. For any nonzero element or fractional ideal a of k,*

$$N_{k,\Phi}(a) = \prod\nolimits_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\, a). \tag{11}$$

PROOF. For $a \in k^\times$,

$$\det{}_E(a\colon k_\varphi \to k_\varphi) = \varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\, a),$$

which implies (11) in this case.

Each side of (11) defines a homomorphism on the groups of fractional ideals, which are torsion-free, and so it suffices to prove that the two homomorphisms agree on principal ideals. This we have just done. □

COROLLARY 1.27 *For any finite extension $k \subset \overline{\mathbb{Q}}$ of E^* containing all conjugates of E and fractional ideal $\mathfrak{a}$ of E^*,*

$$N_\Phi(\mathfrak{a})^{[k:E^*]} = \prod\nolimits_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\, \mathfrak{a}') \tag{12}$$

where $\mathfrak{a}'$ is the extension of $\mathfrak{a}$ to a fractional ideal of k (so $\mathfrak{a}' = \mathfrak{a}\mathcal{O}_k$ if $\mathfrak{a}$ is integral).

PROOF. We have

$$N_{k,\Phi}(\mathfrak{a}') \overset{(7)}{=} N_\Phi(\mathrm{Nm}_{k/E^*}\mathfrak{a}) = N_\Phi(\mathfrak{a}^{[k:E^*]})$$

and so (12) follows from (11). □

Note that (12) determines N_Φ as a homomorphism from the fractional ideals of E^* to the fractional ideals of E.

EXAMPLE 1.28 Consider a CM-pair (E,Φ) with E a subfield of $\overline{\mathbb{Q}}$. The reflex CM-pair (E^*,Φ^*) can be described as follows: choose a subfield L of $\overline{\mathbb{Q}}$ containing E and Galois over $\mathbb{Q}$ (for example, $L=\overline{\mathbb{Q}}$) and let $\Phi_L = \{\tau\in\mathrm{Gal}(L/\mathbb{Q}) \mid \tau|E\in\Phi\}$; then

$$\mathrm{Gal}(L/E^*) = \{\sigma\in\mathrm{Gal}(L/\mathbb{Q}) \mid \sigma\Phi=\Phi\};$$

the set Φ_L is stable under the left action of $\mathrm{Gal}(L/E^*)$, and when we write

$$\Phi_L^{-1} = \bigsqcup_{\psi\in\Phi_L^*} \psi\,\mathrm{Gal}(L/E^*) \quad \text{(disjoint union)},$$

$\Phi^* = \{\psi|E^* \mid \psi\in\Phi_L^*\}$ is the reflex CM-type on E^*. The map

$$a\mapsto \prod_{\psi\in\Phi^*}\psi(a)\colon E^{*\times}\to L^\times$$

factors through $E^\times\subset L^\times$, and the resulting map $E^{*\times}\to E^\times$ is N_Φ — this is a restatement of (1.26). Because it has this description, other authors write N_{Φ^*} where we write N_Φ.[7]

Classification of the primitive CM-pairs

An ***isomorphism of CM-pairs*** $(E,\Phi)\to(E',\Phi')$ is an isomorphism $\alpha\colon E\to E'$ of $\mathbb{Q}$-algebras such that $\varphi\circ\alpha\in\Phi$ whenever $\varphi\in\Phi'$.

Let (E,Φ) be a CM-pair, and let k be a CM subfield of $\overline{\mathbb{Q}}$ Galois over $\mathbb{Q}$ and containing E^*. For $\rho\colon E\to\overline{\mathbb{Q}}$ and $\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, define

$$\psi_\rho(\sigma) = \begin{cases} 1 & \text{if } \rho\in\sigma\Phi \\ 0 & \text{otherwise.}\end{cases}$$

In other words, $\psi_\rho(\sigma)=\phi(\sigma^{-1}\circ\rho)$ where ϕ is the characteristic function of Φ.

LEMMA 1.29 *For each ρ, the number $\psi_\rho(\sigma)$ depends only on the restriction of σ to E^* and the map*

$$\sigma\mapsto\psi_\rho(\sigma)\colon \mathrm{Hom}(k,\overline{\mathbb{Q}})\to\{0,1\}$$

is a CM-type on k.

PROOF. If $\sigma'|E^*=\sigma|E^*$, then $\sigma'=\sigma\circ\tau$ for some τ fixing E^*,[8] and so

$$\sigma'\Phi = \sigma\tau\Phi = \sigma\Phi;$$

hence $\psi_\rho(\sigma')=\psi_\rho(\sigma)$. As $\sigma\Phi$ is a CM-type on E, ρ lies in exactly one of $\sigma\Phi$ or $\iota\sigma\Phi$, and so

$$\psi_\rho(\sigma)+\psi_\rho(\iota\circ\sigma)=1.$$

□

[7] For us, the reflex CM-type plays almost no role.

[8] Think of σ and σ' as automorphisms of k, and take $\tau=\sigma^{-1}\circ\sigma'$.

For any $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$,

$$\psi_{\tau\circ\rho}(\sigma) = \phi(\sigma^{-1}\circ\tau\circ\rho) = \psi_\rho(\tau^{-1}\circ\sigma) = (\tau\psi_\rho)(\sigma),$$

and so, as ρ runs over the embeddings $E \hookrightarrow \overline{\mathbb{Q}}$, ψ_ρ runs over a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbit of CM-types on k.

PROPOSITION 1.30 *The map $(E,\Phi) \mapsto \{\psi_\rho\}$ defines a bijection from the set of isomorphism classes of primitive CM-pairs (E,Φ) whose reflex field is contained in k to the set of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of CM-types on k.*

PROOF. We construct an inverse. For a CM-type Ψ on k, let (E_Ψ,Φ_Ψ) be the reflex CM-pair of (k,Ψ) (see 1.19). By definition, (E_Ψ,Φ_Ψ) is the primitive subpair of (k,Ψ^{-1}). Its isomorphism class depends only on the $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$-orbit of Ψ,[9] and the map $\Psi \mapsto (E_\Psi,\Phi_\Psi)$ provides the required inverse.[10] □

Let k be a composite of CM-subfields of $\overline{\mathbb{Q}}$ (e.g., k could be the composite $\mathbb{Q}^{\mathrm{cm}}$ of all CM-subfields of $\overline{\mathbb{Q}}$). We define a ***CM-type*** on k to be a locally constant map $\phi\colon \mathrm{Hom}(k,\overline{\mathbb{Q}}) \to \{0,1\}$ such that $\phi(\rho)+\phi(\iota\circ\rho) = 1$ for all ρ. For example, the CM-types on $\mathbb{Q}^{\mathrm{cm}}$ are the extensions to $\mathbb{Q}^{\mathrm{cm}}$ of a CM-type on some CM-subfield of $\overline{\mathbb{Q}}$.

COROLLARY 1.31 *The map $(E,\Phi) \mapsto \{\psi_\rho\}$ defines a bijection from the set of isomorphism classes of primitive CM-pairs (E,Φ) to the set of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of CM-types on $\mathbb{Q}^{\mathrm{cm}}$.*

PROOF. Pass to the limit over all CM-subfields of $\overline{\mathbb{Q}}$ in the proposition. □

EXAMPLE 1.32 From (1.12) we can read off the list of isomorphism classes of primitive CM-pairs whose reflex field is contained in $\mathbb{Q}[e^{2\pi i/13}]$.

REMARK 1.33 Let (E,Φ) be a CM-pair with reflex field contained in k, and let ψ_ρ be the CM-type on k defined by an embedding $\rho\colon E \hookrightarrow \overline{\mathbb{Q}}$. For any $\mathbb{Q}$-algebra R and $a\otimes r \in (k\otimes_{\mathbb{Q}} R)^\times$,

$$N_\rho(a\otimes r) \stackrel{\mathrm{def}}{=} \prod\nolimits_{\sigma:k\to\mathbb{Q}^{\mathrm{al}}} (\sigma a\otimes r)^{\psi_\rho(\sigma)}$$

is independent of ρ, and equals $N_\Phi(a\otimes r)$.

REMARK 1.34 As the above discussion makes clear, attached to a CM-pair (E,Φ) there is only an orbit of CM-types on the reflex field E^*. However, when E is a *subfield* of $\mathbb{Q}^{\mathrm{al}}$, there is a well-defined CM-type Φ^* on E^* corresponding to the given embedding of E, called the reflex of Φ (see 1.19).

EXERCISE 1.35 Rewrite this section for a k that is not necessarily Galois over $\mathbb{Q}$.

[9] For $\tau \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$, $E_{\tau\Psi} = \tau E_\Psi$ and $\tau\colon E_\Psi \to E_{\tau\Psi}$ is an isomorphism (E_Ψ,Φ_Ψ).

[10] Consider, for example, a CM-pair (E,Φ) and a fixed embedding of E into $\mathbb{Q}^{\mathrm{al}}$. The composite

$$(E,\Phi) \mapsto \Psi \mapsto (E_\Psi,\Phi_\Psi)$$

sends (E,Φ) to the reflex (E^{**},Φ^{**}) of its reflex (E^*,Φ^*). It is obvious from the definition of the reflex CM-pair, that (E^{**},Φ^{**}) is a primitive CM-subpair of (E,Φ), and therefore equals it if (E,Φ) is primitive.

Positive involutions and CM-algebras

Let B be an algebra (not necessarily commutative) over a field k. An ***involution*** of B is a k-linear map $b \mapsto b' : B \to B$ such that $(ab)' = b'a'$ and $(b')' = b$ for $a, b \in B$. Because of our convention on ring homomorphisms, $1' = 1$ and so $c' = c$ for $c \in k$.

Throughout this subsection, Q is a subfield of $\mathbb{R}$. An involution $'$ on a finite-dimensional Q-algebra B is said to be ***positive*** if

$$\mathrm{Tr}_{B/Q}(b' \cdot b) > 0 \tag{13}$$

for every nonzero $b \in B$. Note that

$$(b_1, b_2) \mapsto \mathrm{Tr}_{B/Q}(b_1' \cdot b_2) : B \times B \to Q$$

is Q-bilinear, and so it suffices to check (13) for the elements of a Q-basis for B. Therefore, an involution on B is positive if and only if its linear extension to $B \otimes_Q \mathbb{R}$ is positive.

PROPOSITION 1.36 *Every finite-dimensional Q-algebra admitting a positive involution is semisimple.*

PROOF. Let B admit a positive involution $'$, and let $\mathfrak{a}$ be a nilpotent two-sided ideal in B. We have to show that $\mathfrak{a} = 0$. If not, there exists a nonzero $a \in \mathfrak{a}$. Then $b \overset{\text{def}}{=} a'a \in \mathfrak{a}$ and is nonzero because $\mathrm{Tr}_{B/Q}(b) > 0$. As $b = b'$, $\mathrm{Tr}_{B/Q}(b^2) > 0$ and so $b^2 \neq 0$; similarly $\mathrm{Tr}_{B/Q}(b^4) > 0$ and so $b^4 \neq 0$, etc., contradicting the nilpotence of $\mathfrak{a}$. □

PROPOSITION 1.37 *Let B be a finite-dimensional Q-algebra. The following conditions on an involution $'$ of B are equivalent:*

(a) *B is semisimple and some faithful B-module V admits a positive definite symmetric Q-bilinear form $(\ |\ ) : V \times V \to Q$ such that*

$$(bu|v) = (u|b'v), \text{ all } b \in B,\ u, v \in V; \tag{14}$$

(b) *every B-module admits a positive definite symmetric Q-bilinear form satisfying (14);*

(c) *$'$ is positive.*

PROOF. (a) $\Longrightarrow$ (b). Every B-module is a direct summand of a direct sum of copies of V (see p9), and the restriction of a bilinear form as in (a) to a B-submodule is of the same type.

(b) $\Longrightarrow$ (c). We may suppose $Q = \mathbb{R}$. Let W be a B-module. According to (b), there exists a positive definite symmetric $\mathbb{R}$-bilinear form $(\ |\ ) : W \times W \to \mathbb{R}$ satisfying (14). Because $Q = \mathbb{R}$, there exists an orthonormal basis $e_1, \dots, e_n$ for W relative to $(\ |\ )$, and, for any $b \in B$, the trace of $b'b$ on W is

$$\sum\nolimits_i (e_i|b'be_i) \overset{(14)}{=} \sum\nolimits_i (be_i|be_i),$$

which is > 0 unless b acts as zero on W. When we apply this remark with $W = B$, we find that $\mathrm{Tr}_{B/\mathbb{R}}(b'b) > 0$ unless $b = 0$.

(c) $\Longrightarrow$ (a). Proposition 1.36 shows that B is semisimple, and for V we can take B with $(u|v) = \mathrm{Tr}_{B/Q}(uv')$. □

EXAMPLE 1.38 (a) For a totally real number field F, the identity involution is positive.

(b) For a CM-field E, the involution ι_E is positive.

PROPOSITION 1.39 *Every finite-dimensional commutative $\mathbb{Q}$-algebra with positive involution is a product of pairs as in (1.38).*

PROOF. First consider an arbitrary finite-dimensional semisimple algebra B with involution $'$ over a field k. The involution $'$ permutes the set of simple two-sided ideals in B, from which it follows easily that B decomposes (as a $\mathbb{Q}$-algebra with involution) into a product each of whose factors is either (a) a simple algebra with an involution or (b) the product of two simple algebras interchanged by $'$.

Next assume that B is commutative, that $k = \mathbb{R}$, and that $'$ is positive. Case (b) is excluded[11], from which it follows that the only possibilities for the factors are $(\mathbb{R}, \mathrm{id})$ or $(\mathbb{C}, \iota)$.

Finally assume that B is commutative, that $k = \mathbb{Q}$, and that $'$ is positive. Case (b) is again excluded, and so we need consider only the case that B is a field. Then $\mathrm{Aut}(\mathbb{C})$ acts transitively on the set of homomorphisms $B \to \mathbb{C}$, and it follows that all factors of $(B,') \otimes_{\mathbb{Q}} \mathbb{R}$ are of the same type. If they are $(\mathbb{R}, \mathrm{id})$, B is totally real and $' = \mathrm{id}$; if they are $(\mathbb{C}, \iota)$, B is a CM-field and $' = \iota$. □

COROLLARY 1.40 *The CM-algebras are exactly the finite-dimensional commutative $\mathbb{Q}$-algebras admitting a (unique) positive involution that acts nontrivially on each factor.*

2 Complex abelian varieties

Complex tori

A ***lattice*** Λ in a $\mathbb{C}$-vector space V is the $\mathbb{Z}$-submodule generated by an $\mathbb{R}$-basis for V, i.e., such that $\mathbb{R} \otimes_{\mathbb{Z}} \Lambda \simeq V$. Equivalently, it is a discrete subgroup Λ of V such that V/Λ is compact (ANT 4.14). The quotient V/Λ is a complex manifold with a distinguished point, namely, $0 + \Lambda$, and any pointed complex manifold isomorphic to such a quotient is called a ***complex torus***. Equivalently, a complex manifold M with a distinguished point 0 is a complex torus if the exponential map

$$\exp: \mathrm{Tgt}_0(M) \to M$$

realizes M as the quotient of the complex vector space $\mathrm{Tgt}_0(M)$ by a lattice. In particular, we see that a complex torus has a canonical uniformization $\theta: V/\Lambda \xrightarrow{\simeq} M$.

PROPOSITION 2.1 *Every complex torus is a compact connected complex Lie group. Conversely, if M is a compact connected complex Lie group, then the exponential map realizes M as a complex torus.*

PROOF. The first assertion is obvious; for the second, see, for example, Mumford 1970, I 1. □

PROPOSITION 2.2 *Let $M \simeq V/\Lambda$ and $M' \simeq V'/\Lambda'$ be complex tori. A $\mathbb{C}$-linear map $\alpha: V \to V'$ such that $\alpha(\Lambda) \subset \Lambda'$ defines a holomorphic map $M \to M'$ sending 0 to 0, and every holomorphic map $M \to M'$ sending 0 to 0 is of this form (for a unique α).*

[11] For if $B = B_1 \times B_2$, then $(a,0)(a,0)' = (0,0)$.

PROOF. We choose bases, and identify V and V' with $\mathbb{C}^n$ and $\mathbb{C}^{n'}$ respectively. The map $\mathbb{C}^n \xrightarrow{\alpha} \mathbb{C}^{n'} \to \mathbb{C}^{n'}/\Lambda'$ is holomorphic, and it factors through $\mathbb{C}^n/\Lambda$. Because $\mathbb{C}^n/\Lambda$ has the quotient complex structure, the resulting map $\mathbb{C}^n/\Lambda \to \mathbb{C}^{n'}/\Lambda'$ is holomorphic. Conversely, let $\varphi\colon \mathbb{C}^n/\Lambda \to \mathbb{C}^{n'}/\Lambda'$ be a holomorphic map such that $\varphi(0) = 0$. Then $\mathbb{C}^n$ and $\mathbb{C}^{n'}$ are universal covering spaces of $\mathbb{C}^n/\Lambda$ and $\mathbb{C}^{n'}/\Lambda'$, and a standard result in topology (Hatcher 2002, 1.33, 1.34) shows that φ lifts uniquely to a continuous map $\alpha\colon \mathbb{C}^n \to \mathbb{C}^{n'}$ such that $\alpha(0) = 0$:

$$\begin{array}{ccc} \mathbb{C}^n & \xrightarrow{\alpha} & \mathbb{C}^{n'} \\ \downarrow & & \downarrow \\ \mathbb{C}^n/\Lambda & \xrightarrow{\varphi} & \mathbb{C}^{n'}/\Lambda'. \end{array}$$

We have to show that α is linear. Because the vertical arrows are local isomorphisms, α is holomorphic. For any $\omega \in \Lambda$, the map $z \mapsto \alpha(z+\omega) - \alpha(z)$ is continuous and takes values in $\Lambda' \subset \mathbb{C}$; as $\mathbb{C}^n$ is connected and Λ' is discrete, it must be constant. Therefore,

$$\frac{\partial \alpha}{\partial z_j}(z+\omega) - \frac{\partial \alpha}{\partial z_j}(z) = 0,$$

and so, for each j, $\frac{\partial \alpha}{\partial z_j}$ defines a holomorphic function $\mathbb{C}^n/\Lambda \to \mathbb{C}^{n'}$, which must be constant (because $\mathbb{C}^n/\Lambda$ is compact). Write α as an n'-tuple $(\alpha_1, \dots, \alpha_{n'})$ of holomorphic functions α_i in n variables. Because $\alpha_i(0) = 0$ and $\frac{\partial \alpha_i}{\partial z_j}$ is constant for each j, the power series expansion of α_i at 0 is of the form $\sum_j a_{ij} z_j$. Now α_i and $\sum_j a_{ij} z_j$ are holomorphic functions on $\mathbb{C}^n$ that coincide on a neighbourhood of 0, and so are equal on the whole of $\mathbb{C}^n$. □

COROLLARY 2.3 *Every holomorphic map $M \to N$ of complex tori sending 0_M to 0_N is a homomorphism. In particular, the group structure on M is uniquely determined by the zero element.*

A ***Riemann pair*** (Λ, J) is a free $\mathbb{Z}$-module of finite rank Λ together with a complex structure J on $\mathbb{R} \otimes \Lambda$ (i.e., J is an $\mathbb{R}$-linear endomorphism of Λ with square -1). A ***homomorphism*** $(\Lambda, J) \to (\Lambda', J')$ ***of Riemann pairs*** is a homomorphism $\alpha\colon \Lambda \to \Lambda'$ of $\mathbb{Z}$-modules such that $\mathrm{id} \otimes \alpha\colon \mathbb{R} \otimes \Lambda \to \mathbb{R} \otimes \Lambda'$ is $\mathbb{C}$-linear.

PROPOSITION 2.4 *The functor $(\Lambda, J) \mapsto M(\Lambda, J) \stackrel{def}{=} (\mathbb{R} \otimes \Lambda, J)/\Lambda$ is an equivalence from the category of Riemann pairs to the category of complex tori.*

PROOF. Proposition 2.2 says that the functor is fully faithful, and it is essentially surjective by definition. □

EXAMPLE 2.5 Let (E, Φ) be a CM-pair, and let Λ be a lattice in E, so that $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q} \simeq E$. Recall that Φ defines an isomorphism $E \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{(3)} \mathbb{C}^{\Phi}$,[12] and so

$$\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{R} \simeq E \otimes_{\mathbb{Q}} \mathbb{R} \overset{\Phi}{\simeq} \mathbb{C}^{\Phi},$$

[12]Here $\mathbb{C}^{\Phi}$ is the set of maps $\Phi \to \mathbb{C}$. In other words, it is a product of copies of $\mathbb{C}$ indexed by the elements of Φ.

from which $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ acquires a complex structure. Thus, from a CM-pair (E, Φ) and a lattice Λ in E, we get a Riemann pair (Λ, J_Φ), and hence an abelian variety A_Φ together with a homomorphism $i_\Phi\colon E \to \mathrm{End}^0(A_\Phi)$ such that

$$\begin{array}{ccc} \mathbb{C}^\Phi & \longrightarrow & A_\Phi \\ \downarrow{\scriptstyle z\mapsto\Phi(a)z} & & \downarrow{\scriptstyle i_\Phi(a)} \\ \mathbb{C}^\Phi & \longrightarrow & A_\Phi \end{array}$$

commutes for all a in

$$\{a \in E \mid a\Lambda \subset \Lambda\} \simeq \mathrm{End}(A_\Phi).$$

We also write Φ for the map $a \mapsto (\varphi(a))_\varphi\colon \Lambda \to \mathbb{C}^\Phi$ realizing Λ as a lattice in $\mathbb{C}^\Phi$.

An ***isogeny*** of complex tori is a surjective homomorphism with finite kernel. By an ***"isogeny"*** we mean an invertible element of

$$\mathrm{Hom}^0(M, N) \stackrel{\text{def}}{=} \mathrm{Hom}(M, N) \otimes \mathbb{Q}.$$

Thus an "isogeny" $M \to N$ need not be a map from $M \to N$, but some integer multiple will be (in fact, an isogeny). More generally, by a ***"homomorphism"*** $M \to N$ we mean an element of $\mathrm{Hom}^0(M, N)$.[13]

The cohomology of complex tori

By a real torus, we mean a quotient $M = V/\Lambda$ of a real vector space V by a lattice Λ. For example, the circle $S^1 \simeq \mathbb{R}/\mathbb{Z}$ is a real torus. Then V is a universal covering space of M with Λ as its group of covering transformations, and so $\pi_1(M, 0) \simeq \Lambda$ (Hatcher 2002, 1.40). Therefore, (ib. 2A.1)

$$H_1(M, \mathbb{Z}) \simeq \Lambda \tag{15}$$

and (Greenberg 1967, 23.14)

$$H^1(M, \mathbb{Z}) \simeq \mathrm{Hom}(\Lambda, \mathbb{Z}). \tag{16}$$

PROPOSITION 2.6 *For a real torus $M \simeq V/\Lambda$, there is a canonical isomorphism*

$$H^n(M, \mathbb{Z}) \simeq \mathrm{Hom}(\textstyle\bigwedge^n \Lambda, \mathbb{Z}),$$

i.e., $H^n(M, \mathbb{Z})$ is canonically isomorphic to the set of n-alternating forms $\Lambda \times \cdots \times \Lambda \to \mathbb{Z}$.

PROOF. From (16), we see that

$$\textstyle\bigwedge^n H^1(M, \mathbb{Z}) \simeq \bigwedge^n \mathrm{Hom}(\Lambda, \mathbb{Z}).$$

[13] Equivalently, we could define a "homomorphism" $M \to N$ to be a pair (a, m) with a a homomorphism $M \to N$ and m an integer > 0, modulo the equivalence relation

$$(a, m) \sim (b, n) \iff na = bm.$$

Since[14]

$$\bigwedge^n \mathrm{Hom}(\Lambda, \mathbb{Z}) \simeq \mathrm{Hom}(\bigwedge^n \Lambda, \mathbb{Z}),$$

we see that it suffices to show that cup-product defines an isomorphism

$$\bigwedge^n H^1(M, \mathbb{Z}) \to H^n(M, Z). \tag{17}$$

Let $\mathcal{T}$ be the class of topological manifolds M whose cohomology groups are free $\mathbb{Z}$-modules of finite rank and for which the maps (17) are isomorphisms for all n. Certainly, the circle S^1 is in $\mathcal{T}$ (its cohomology groups are $\mathbb{Z}$, $\mathbb{Z}$, $0, \ldots$), and the Künneth formula (Hatcher 2002, 3.16 et seq.) shows that if M_1 and M_2 are in $\mathcal{T}$, then so also is $M_1 \times M_2$. As a topological manifold, $\mathbb{R}^{2n}/\Lambda \approx (S^1)^{2n}$, and so M is in $\mathcal{T}$. □

REMARK 2.7 Therefore,

$$\bigwedge^n \mathrm{Hom}_{\mathbb{R}\text{-linear}}(V, \mathbb{C}) \simeq H^n(M, \mathbb{C}) \simeq H^n_{\mathrm{dR}}(M).$$

The composite isomorphism can be described as follows [to be added, cf. Debarre 1999].

Every $\mathbb{R}$-linear map $V \to \mathbb{C}$ can be written uniquely as the sum of a $\mathbb{C}$-linear map and a $\mathbb{C}$-semilinear map (i.e., an additive homomorphism $\alpha\colon V \to \mathbb{C}$ such that $\alpha(av) = \overline{a}v$ for $a \in \mathbb{C}$, $v \in V$). Thus,

$$\mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C}) = T \oplus \overline{T}$$

where

$$T = \mathrm{Hom}_{\mathbb{C}\text{-linear}}(V, \mathbb{C})$$
$$\overline{T} = \mathrm{Hom}_{\mathbb{C}\text{-semilinear}}(V, \mathbb{C}).$$

Therefore,

$$\bigwedge^n \mathrm{Hom}_{\mathbb{R}}(V, \mathbb{C}) \simeq \bigoplus\nolimits_{p+q=n} \bigwedge^p T \otimes \bigwedge^q \overline{T}.$$

On the other hand, there is the Hodge decomposition

$$H^n_{\mathrm{dR}}(M) \simeq \bigoplus\nolimits_{p+q=n} H^{p,q}(M), \quad H^{p,q}(M) = H^q(M, \Omega^p).$$

PROPOSITION 2.8 *The two decompositions correspond under the isomorphism in (2.7); in particular,*

$$\bigwedge^p T \otimes \bigwedge^q \overline{T} \simeq H^q(M, \Omega^p).$$

[14]For a free $\mathbb{Z}$-module Λ of finite rank, the pairing

$$\bigwedge^n \Lambda^\vee \times \bigwedge^n \Lambda \to \mathbb{Z}$$

determined by

$$(f_1 \wedge \cdots \wedge f_n, v_1 \otimes \cdots \otimes v_n) = \det(f_i(v_j))$$

is perfect, because it is modulo p for every p — see Bourbaki 1958, §8. Here $\Lambda^\vee = \mathrm{Hom}(\Lambda, \mathbb{Z})$ and "perfect" means the discriminant is a unit in $\mathbb{Z}$, so that the pairing defines an isomorphism

$$\bigwedge^n \Lambda^\vee \to \mathrm{Hom}(\bigwedge^n \Lambda, \mathbb{Z}).$$

We shall describe the Hodge structure later. Here we only need that

$$H^1(M,\mathbb{R}) \simeq \Gamma(M,\Omega^1_{\text{hol}}),$$

so that

$$H^1(M,\mathbb{C}) \simeq \Gamma(M,\Omega^1_{\text{hol}}) \oplus \overline{\Gamma(M,\Omega^1_{\text{hol}})},$$

and, dually,

$$H_1(M,\mathbb{C}) \simeq \text{Tgt}_0(A) \oplus \overline{\text{Tgt}_0(A)}. \tag{18}$$

Hermitian forms and alternating forms

To give a complex vector space amounts to giving a real vector space V together with an endomorphism $J: V \to V$ such that $J^2 = -1$. A ***hermitian form*** on (V, J) is an $\mathbb{R}$-bilinear mapping $(\,|\,): V \times V \to \mathbb{C}$ such that $(Ju|v) = \sqrt{-1}(u|v)$ and $(v|u) = \overline{(u|v)}$. When we write[15]

$$(u|v) = \varphi(u,v) - \sqrt{-1}\psi(u,v), \quad \varphi(u,v), \psi(u,v) \in \mathbb{R}, \tag{19}$$

the pairings $u, v \mapsto \varphi(u,v)$ and $u, v \mapsto \psi(u,v)$ are $\mathbb{R}$-bilinear, and

$$\varphi \text{ is symmetric} \qquad \varphi(Ju, Jv) = \varphi(u,v), \tag{20}$$

$$\psi \text{ is alternating} \qquad \psi(Ju, Jv) = \psi(u,v), \tag{21}$$

$$\psi(u,v) = -\varphi(u, Jv), \qquad \varphi(u,v) = \psi(u, Jv). \tag{22}$$

[16]As $(u|u) = \varphi(u,u)$, $(\,|\,)$ is positive definite if and only if φ is positive definite. Conversely, if φ satisfies (20) (resp. ψ satisfies (21)), then the formulas (22) and (19) define a hermitian form:

$$(u|v) = \varphi(u,v) + \sqrt{-1}\varphi(u, Jv) \quad (\text{resp. } (u|v) = \psi(u, Jv) - \sqrt{-1}\psi(u,v)). \tag{23}$$

Riemann forms

Let (Λ, J) be a Riemann pair. An ***integral Riemann form*** (or just ***Riemann form***) for (Λ, J) is an alternating $\mathbb{Z}$-bilinear form $\psi: \Lambda \times \Lambda \to \mathbb{Z}$ such that

$$(x,y) \mapsto \psi_{\mathbb{R}}(x, Jy): \Lambda_{\mathbb{R}} \times \Lambda_{\mathbb{R}} \to \mathbb{R}$$

is symmetric and positive definite. Equivalently (see above), it is the imaginary part of a positive definite hermitian form that takes integer values on Λ.

Let ψ be an alternating $\mathbb{Z}$-bilinear form on Λ, and let $\psi_J(x,y) = \psi_{\mathbb{R}}(x, Jy)$. Then ψ_J is symmetric and positive definite if and only if

- $\diamond$ $\psi_{\mathbb{R}}(Jx, Jy) = \psi_{\mathbb{R}}(x,y)$ for all $x, y \in \Lambda_{\mathbb{R}}$, and

[15]For example, let $V = \mathbb{C}$, so $(z|z') = az\overline{z}'$ for some $a > 0$. Then the decomposition (19) is ($i = \sqrt{-1}$)

$$\underbrace{a(x+iy)(x'-iy')}_{} = \underbrace{a(xx'+yy')}_{} - i\,\underbrace{a(xy'-yx')}_{}.$$

[16]Should re-think these signs. Perhaps remove the $-$ from (19) and define ψ_J to be $\psi(Jx,y) = -\psi(x,Jy)$. Then need to choose α in (2.9) so that $\Im(\varphi\alpha) < 0$, and need to change (Deligne's) definition of the polarization of a Hodge structure (so that $(2\pi i)^n\psi(h(i)x,y) > 0$ rather than $(2\pi i)^n\psi(x,h(i)y) > 0$; Deligne 1979).

◇ $\psi_{\mathbb{R}}(x, Jx) > 0$ for all nonzero $x \in \Lambda_{\mathbb{R}}$.

A Riemann form ψ is nondegenerate, and so, for any $\alpha \in \mathrm{End}^0(\Lambda, J)$, there exists a unique $\alpha' \in \mathrm{End}^0(\Lambda, J)$ such that

$$\psi(\alpha x, y) = \psi(x, \alpha' y), \quad \text{all } x, y \in \Lambda_{\mathbb{Q}}.$$

The map $\alpha \mapsto \alpha'$ is an involution on $\mathrm{End}^0(\Lambda, J)$, called the ***Rosati involution*** (relative to ψ). For $x, y \in \Lambda_{\mathbb{R}}$ and $\alpha \in \mathrm{End}^0(\Lambda, J)$,

$$\psi_J(\alpha x, y) = \psi(J\alpha x, y) = \psi(\alpha J x, y) = \psi(Jx, \alpha' y) = \psi_J(x, \alpha' y),$$

and so the Rosati involution is positive (1.37).

By a ***rational Riemann form***, we mean an alternating $\mathbb{Q}$-bilinear form $\psi\colon \Lambda_{\mathbb{Q}} \times \Lambda_{\mathbb{Q}} \to \mathbb{Q}$ such that $(x, y) \mapsto \psi(x, Jy)\colon \Lambda_{\mathbb{R}} \times \Lambda_{\mathbb{R}} \to \mathbb{R}$ is symmetric and positive definite. Then $\psi(\Lambda, \Lambda) \subset \frac{1}{m}\mathbb{Z}$ for some positive integer m, and $m\psi$ is an (integral) Riemann form.

EXAMPLE 2.9 Let (E, Φ) be a CM-pair, and write $\overline{a}$ for $\iota_E a$. Let Λ be a lattice in E, and let (Λ, J_Φ) be the corresponding Riemann pair (2.5). Then

$$R \stackrel{\text{def}}{=} \{a \in E \mid a\Lambda \subset \Lambda\}$$

is an order in $\mathcal{O}_E$, and $R \subset \mathrm{End}(\Lambda, J_\Phi)$. Therefore, $E \subset \mathrm{End}^0(\Lambda, J_\Phi)$. We wish to determine the rational Riemann forms on (Λ, J_Φ) for which the Rosati involution stabilizes E (and therefore acts on it as ι_E — recall (1.40) that ι_E is the only positive involution on E). To give such a form amounts to giving a nondegenerate $\mathbb{Q}$-bilinear form $\psi\colon E \times E \to \mathbb{Q}$ such that

(a) $\psi(ax, y) = \psi(x, \overline{a}y)$, all $a, x, y \in E$,
(b) $\psi(x, y) = -\psi(y, x)$, all $x, y \in E$,
(c) $\psi(J_\Phi x, J_\Phi y) = \psi(x, y)$, all $x, y \in E \otimes \mathbb{R}$,
(d) $\psi(x, J_\Phi x) > 0$ for all nonzero $x \in E \otimes \mathbb{R}$.

The following statements are left as an easy exercise for the reader (see the appendix).

◇ For any $\alpha \in E^\times$,

$$(x, y) \mapsto \mathrm{Tr}_{E/\mathbb{Q}}(\alpha x \overline{y})\colon E \times E \to \mathbb{Q} \tag{24}$$

is a nondegenerate $\mathbb{Q}$-bilinear form satisfying (a), and every such form arises in this way from a unique α.

◇ Condition (b) holds for the form (24) if and only if $\overline{\alpha} = -\alpha$.

◇ Condition (c) holds automatically for the form (24).

◇ Condition (d) holds for the form (24) if and only if $\Im(\varphi(\alpha)) > 0$ for all $\varphi \in \Phi$.

We conclude that the rational Riemann forms for (Λ, J_Φ) are in one-to-one correspondence with the $\alpha \in E^\times$ such that $\overline{\alpha} = -\alpha$ and $\Im(\varphi(\alpha)) > 0$ for all $\varphi \in \Phi$.

Let F be the product of the largest totally real subfields of the factors of E. Then (cf. 1.4) $E = F[\alpha]$ with $\alpha^2 \in F$, which implies that $\overline{\alpha} = -\alpha$. The weak approximation theorem (CFT 6.3) shows that α can chosen so that $\Im(\varphi(\alpha)) > 0$ for all $\varphi \in \Phi$. Thus, αs with the required properties certainly exist, and so (Λ, J_Φ) is polarizable.

Let α be one element of $E^\times$ such that $\overline{\alpha} = -\alpha$ and $\Im(\varphi(\alpha)) > 0$ for all $\varphi \in \Phi$. Then the other such elements are exactly those of the form αa with a a totally positive element of F (i.e., $\overline{a} = a$ and $\varphi(a) > 0$ for all $\varphi\colon F \to \mathbb{R}$).

Abelian varieties

DEFINITION 2.10 An ***abelian variety*** is a complex torus that admits a Riemann form.

EXAMPLE 2.11 For any CM-pair (E,Φ) and lattice Λ in E, the complex torus $\mathbb{C}^\Phi/\Phi(\Lambda)$ admits a polarization (2.9), and so is an abelian variety.

If $A \simeq V/\Lambda$ is an abelian variety, then so also is $A^\vee \stackrel{\text{def}}{=} V'/\Lambda'$, where V' is the space of semilinear maps $V \to \mathbb{C}$ and $\Lambda' = \{f \in V^\vee \mid f(\Lambda) \subset \mathbb{Z}\}$. Moreover, an integral Riemann form ψ on A defines an isogeny

$$[a] \mapsto ([x] \mapsto [\psi(a,x)]) \colon A \to A^\vee.$$

Here $[a] = a + \Lambda \in A$.

THEOREM 2.12 (POINCARÉ REDUCIBILITY THEOREM) *For any abelian subvariety B of an abelian variety A, there exists an abelian variety $B' \subset A$ such that $B \cap B'$ is finite and $B + B' = A$, i.e., such that $(b,b') \mapsto b + b' \colon B \times B' \to A$ is an isogeny.*

PROOF. Let $A \simeq V/\Lambda$ be the canonical uniformization of A, and let $W \subset V$ be the tangent space at 0 of $B \subset A$; then

$$B = W/(\Lambda \cap W) \subset V/\Lambda = A.$$

Choose an integral Riemann form ψ for A, and let $W^\perp$ be the orthogonal complement to W under $\psi_{\mathbb{R}}$. Then $W^\perp$ is stable under J, and $\Lambda \cap W^\perp$ is a lattice in $W^\perp$ because it has rank

$$\operatorname{rank}\Lambda - \operatorname{rank}\Lambda \cap W = 2\dim_{\mathbb{C}} W^\perp.$$

As $\psi|\Lambda\cap W^\perp$ is a Riemann form for $(\Lambda\cap W^\perp, J|W^\perp)$, $B' \stackrel{\text{def}}{=} W^\perp/W^\perp\cap\Lambda$ is an abelian subvariety of A. Moreover, $B \cap B'$ is finite. □

An abelian variety A is said to be ***simple*** if it has no proper nonzero abelian subvarieties. It follows easily from the theorem that each abelian variety A is isogenous to a product $\prod A_i^{r_i}$ of powers of nonisogenous simple abelian varieties A_i; the r_i are uniquely determined and the A_i are uniquely determined up to isogeny. Moreover, each $\operatorname{End}^0(A_i)$ is a division algebra, $\operatorname{End}^0(A_i^{r_i})$ is equal to the matrix algebra $M_{r_i}(A_i)$, and $\operatorname{End}^0(A) = \prod \operatorname{End}^0(A_i^{r_i})$. In particular, $\operatorname{End}^0(A)$ is semisimple.[17]

EXERCISE 2.13 Let A be the quotient of $\mathbb{C}^2$ by the lattice generated by $(i,0)$, $(\sqrt{2},i)$, $(1,0)$, $(0,1)$, and let B be the quotient of $\mathbb{C}$ by the lattice generated by i and 1. Show that the image $\overline{B}$ of the map

$$z \mapsto (z,0) \colon B \to A$$

is a complex subtorus of the complex torus A for which there does not exist a complex subtorus $B' \subset A$ such that $\overline{B} \cap B'$ is finite and $\overline{B} + B' = A$. (Hence, no Riemann form exists for A. In fact, most complex tori are not abelian varieties.)

[17] This also follows from the fact that the Rosati involution on $\operatorname{End}^0(A)$ defined by any Riemann form is positive.

3 Abelian varieties with complex multiplication

Definition of CM abelian varieties

PROPOSITION 3.1 *For any abelian variety A,*

$$2\dim A \geq [\mathrm{End}^0(A)\colon \mathbb{Q}]_{\mathrm{red}}.$$

When equality holds, $\mathrm{End}^0(A)$ is a product of matrix algebras over fields.[18]

PROOF. As $\mathrm{End}^0(A)$ is a semisimple $\mathbb{Q}$-algebra acting faithfully on the $2\dim A$-dimensional $\mathbb{Q}$-vector space $H_1(A,\mathbb{Q})$, this follows from (1.2). □

DEFINITION 3.2 A complex abelian variety A is said to have ***complex multiplication*** (or be of ***CM-type***, or be a ***CM abelian variety***) if

$$2\dim A = [\mathrm{End}^0(A)\colon \mathbb{Q}]_{\mathrm{red}}.$$

PROPOSITION 3.3 *The following conditions on an abelian variety A are equivalent:*

(a) *A has complex multiplication;*
(b) *$\mathrm{End}^0(A)$ contains an étale subalgebra of degree $2\dim A$ over $\mathbb{Q}$;*
(c) *for any Weil cohomology $X \mapsto H^*(X)$ with coefficient field Ω, the centralizer of $\mathrm{End}^0(A)$ in $\mathrm{End}_\Omega(H^1(A))$ is commutative (and equals $C(A)\otimes_{\mathbb{Q}}\Omega$ where $C(A)$ is the centre of $\mathrm{End}^0(A)$).*

PROOF. (a) $\iff$ (b). According to (1.3), the degree of a maximal étale subalgebra is $[\mathrm{End}^0(A)\colon\mathbb{Q}]_{\mathrm{red}}$.

(a) $\iff$ (c). From the definition of a Weil cohomology, one deduces that $H^1(A)$ has dimension $2\dim A$ over Ω, and that $\mathrm{End}^0(A)\otimes_{\mathbb{Q}}\Omega$ acts faithfully on it. Thus, if (a) holds, then $\mathrm{End}^0(A)\otimes_{\mathbb{Q}}\Omega$ is a product of matrix algebras over fields and $H^1(A)$ is reduced (1.2). From this, (c) follows. The converse is equally easy. □

EXAMPLE 3.4 For any CM-pair (E,Φ) and lattice Λ in E, the abelian variety $A_\Phi = \mathbb{C}^\Phi/\Phi(\Lambda)$ (see 2.11) has complex multiplication because $\mathrm{End}^0(A)$ contains the étale subalgebra E, which has degree $2\dim A_\Phi$ over $\mathbb{Q}$.

REMARK 3.5 Let $A \sim \prod_i A_i^{n_i}$ be the decomposition of A (up to isogeny) into a product of isotypic abelian varieties. Then $D_i = \mathrm{End}^0(A_i)$ is a division algebra, and $\mathrm{End}^0(A) \simeq \prod_i M_{n_i}(D_i)$ is the decomposition $\mathrm{End}^0(A)$ into a product of simple $\mathbb{Q}$-algebras. From (3.3), we see that A has complex multiplication if and only if D_i is a commutative field of degree $2\dim A_i$ for all i. In particular, a simple abelian variety A has complex multiplication if and only if $\mathrm{End}^0(A)$ is a field of degree $2\dim A$ over $\mathbb{Q}$, and an arbitrary abelian variety has complex multiplication if and only if each simple isogeny factor does.

PROPOSITION 3.6 *(a) A simple abelian variety A has complex multiplication if and only if $\mathrm{End}^0(A)$ is a CM-field of degree $2\dim A$ over $\mathbb{Q}$.*

(b) An isotypic abelian variety A has complex multiplication if and only if $\mathrm{End}^0(A)$ contains a field of degree $2\dim A$ over $\mathbb{Q}$ (which can be chosen to be a CM-field invariant under some Rosati involution).

(c) An abelian variety A has complex multiplication if and only if $\mathrm{End}^0(A)$ contains an étale $\mathbb{Q}$-algebra (which can be chosen to be a CM-algebra invariant under some Rosati involution) of degree $2\dim A$ over $\mathbb{Q}$ (in which case $H_1(A,\mathbb{Q})$ is free of rank 1).

[18] *Recall (see Notations) that fields are commutative.*

PROOF. (a) After the remark, it remains to show that if $\mathrm{End}^0(A)$ is a field of degree $2\dim A$ then it is CM. We know that it is either totally real or CM because it is stable under the Rosati involutions (1.39), and Lemma 3.7 below shows that it must be the former.

(b) Write $A \sim A_0^m$ with A_0 simple. Then $E_0 = \mathrm{End}^0(A_0)$ is a CM-field. Let F be a totally real field of degree m over $\mathbb{Q}$ that it linearly disjoint from E_0. Then $E \stackrel{\text{def}}{=} E_0 \cdot F$ is a CM-field of degree $2\dim A$, and the choice of an E_0-basis for it defines an embedding of it into $M_m(E_0) \simeq \mathrm{End}^0(A)$. Moreover, (2.9) provides A with a polarization under which E is stable.

(c) Follows from (b) ($H_1(A,\mathbb{Q})$ is free of rank 1 because E acts faithfully on it). □

LEMMA 3.7 *Let F be a subfield of* $\mathrm{End}^0(A)$, *some abelian variety A. If F has a real prime, then* $[F\colon\mathbb{Q}]$ *divides* $\dim A$.

PROOF. For any endomorphism α of A, there is a (unique) polynomial $P_\alpha(T) \in \mathbb{Q}[T]$ of degree $2\dim A$ such that, for all rational numbers r, $P_\alpha(r) = \deg(\alpha - r_A)$; moreover, $P_\alpha(T)$ is the characteristic polynomial of α on $H_1(A,\mathbb{Q})$ (see Milne 1986, Section 12, for a proof in a more abstract setting).

Note that $H_1(A,\mathbb{Q})$ is a vector space of dimension $m \stackrel{\text{def}}{=} 2\dim A/[F\colon\mathbb{Q}]$ over F, and so, for any $\alpha \in \mathrm{End}(A) \cap F$, $P_\alpha(T)$ is the m^{th}-power of the characteristic polynomial of α in $F/\mathbb{Q}$. In particular,

$$\mathrm{Nm}_{F/\mathbb{Q}}(\alpha)^m = \deg(\alpha) \geq 0.$$

However, if F has a real prime, then α can be chosen to be large and negative at that prime and close to 1 at the remaining primes (weak approximation theorem, CFT 6.3), so that $\mathrm{Nm}_{F/\mathbb{Q}}(\alpha) < 0$. This gives a contradiction unless m is even. □

REMARK 3.8 A subalgebra E of $\mathrm{End}^0(A)$ for which $H_1(A,\mathbb{Q})$ has rank 1 need not be CM, even when it is a field. Consider, for example, an elliptic curve A_0 with complex multiplication by a quadratic imaginary field E_0, and let $A = A_0^m$. Let F be any field of degree m over $\mathbb{Q}$ and linearly disjoint from E_0, and embed F into $\mathrm{GL}_m(\mathbb{Q})$, hence into $\mathrm{GL}_m(E_0)$. Then $H_1(A,\mathbb{Q})$ is of dimension 1 over the field $E = E_0F \subset \mathrm{End}^0(A)$, but E is CM if and only if F is totally real or CM (note that a field with Galois group A_5 and can not be CM).

REMARK 3.9 An abelian variety A with complex multiplication by E is isogenous to a principal abelian variety, i.e., an abelian variety on which the full ring of integers of E acts. To see this, write $A = \mathbb{C}^\Phi/\Phi(\mathfrak{a})$ with $\mathfrak{a}$ a lattice in E, and consider $\mathbb{C}^\Phi/\Phi(\mathfrak{b})$ where $\mathfrak{b}$ is an ideal contained in $\mathfrak{a}$.

EXERCISE 3.10 Let L be a simple $\mathbb{Q}$-algebra of finite degree d^2 over its centre F, and let A be an abelian variety containing L in its endomorphism algebra.

(a) Show that for any semisimple commutative $\mathbb{Q}$-subalgebra R of $\mathrm{End}^0_L(A)$, $\dim_{\mathbb{Q}} R \leq (2\dim A)/d$, and that equality holds for some R if and only A has complex multiplication.

(b) Let $'$ be a Rosati involution on $\mathrm{End}^0(A)$ stabilizing L; show that, if A has complex multiplication, then there is an R as in (a) that is stabilized by $'$.

The reflex field of an abelian variety with complex multiplication

Let E_0 be the centre of $\mathrm{End}^0(A)$. There exists a CM-type Φ_0 on E_0 with the following property: suppose A is of CM-type (E,Φ) (relative to $E \hookrightarrow \mathrm{End}^0(A)$); then (E,Φ) extends (E_0,Φ_0). Therefore, the reflex field of (E_0,Φ_0) equals the reflex field of any such (E,Φ) (1.18c). We call it the ***reflex field*** of A.

Classification up to isogeny

3.11 Let A be an abelian variety with complex multiplication, so that $\mathrm{End}^0(A)$ contains a CM-algebra E for which $H_1(A,\mathbb{Q})$ is free E-module of rank 1, and let Φ be the set of homomorphisms $E \to \mathbb{C}$ occurring in the representation of E on $\mathrm{Tgt}_0(A)$, i.e., $\mathrm{Tgt}_0(A) \simeq \bigoplus_{\varphi\in\Phi} \mathbb{C}_\varphi$ where $\mathbb{C}_\varphi$ is a one-dimensional $\mathbb{C}$-vector space on which $a \in E$ acts as $\varphi(a)$. Then, because

$$H_1(A,\mathbb{R}) \simeq \mathrm{Tgt}_0(A) \oplus \overline{\mathrm{Tgt}_0(A)} \tag{25}$$

(see (25)) Φ_A is a CM-type on E, and we say that, A together with the injective homomorphism $i\colon E \to \mathrm{End}^0(A)$, is of ***CM-type*** (E,Φ).

Let e be a basis vector for $H_1(A,\mathbb{Q})$ as an E-module, and let $\mathfrak{a}$ be the lattice in E such that $\mathfrak{a}e = H_1(A,\mathbb{Z})$. Under the isomorphism (cf. (25))

$$H_1(A,\mathbb{R}) \simeq \bigoplus\nolimits_{\varphi\in\Phi} \mathbb{C}_\varphi \oplus \bigoplus\nolimits_{\varphi\in\iota\Phi} \mathbb{C}_\varphi,$$

$$e\otimes 1 \longleftrightarrow (\ldots, e_\varphi, \ldots; \ldots, e_{\iota\circ\varphi}, \ldots)$$

where each e_φ is a $\mathbb{C}$-basis for $\mathbb{C}_\varphi$. The e_φ determine an isomorphism

$$\mathrm{Tgt}_0(A) \simeq \bigoplus\nolimits_{\varphi\in\Phi} \mathbb{C}_\varphi \simeq \mathbb{C}^\Phi,$$

and hence a commutative square of isomorphisms in which the top arrow is the canonical parametrization:

$$\begin{array}{ccc} \mathrm{Tgt}_0(A)/\Lambda & \longrightarrow & A \\ \downarrow & & \downarrow \\ \mathbb{C}^\Phi/\Phi(\mathfrak{a}) & = & A_\Phi. \end{array} \tag{26}$$

PROPOSITION 3.12 *The map $(A,i) \mapsto (E,\Phi)$ gives a bijection from the set of isogeny classes of pairs (A,i) to the set of isomorphism classes of CM-pairs, with inverse $(E,\Phi) \mapsto (A_\Phi, i_\Phi)$.*

PROOF. We have well-defined maps between the two sets, whose composites we shall show to identity maps. Let (E,Φ) be the CM-type of (A,i); then (26) shows that $(A,i) \approx (A_\Phi, i_\Phi)$. In the other direction, it is obvious that (A_Φ, i_Φ) is of CM-type (E,Φ). □

We make this classification more precise in the case of simple abelian varieties with complex multiplication....

PROPOSITION 3.13 *Let A be a simple abelian variety with complex multiplication, and let $E = \mathrm{End}^0(A)$. Then (E,Φ_A) is a primitive CM-type, and the map $A \mapsto (E,\Phi_A)$ defines a bijection from the set of isogeny classes of simple abelian varieties with complex multiplication to the set of isomorphism classes of primitive CM-pairs.*

PROOF. Because A is simple, E is a field. If (E, Φ_A) is not primitive, and so is the extension of a CM-type (E_0, Φ_0) with E_0 a proper subfield of E, then A will be isogenous to $A_{\Phi_0}^{[E:E_0]}$, and so is not simple. □

COROLLARY 3.14 *The simple abelian varieties with complex multiplication are classified up to isogeny*[19] *by the Γ-orbits of CM-types on $\mathbb{Q}^{\mathrm{cm}}$ where $\Gamma = \mathrm{Gal}(\mathbb{Q}^{\mathrm{cm}}/\mathbb{Q})$ (or $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$).*

PROOF. Combine Proposition 3.13 with Proposition 1.30. □

COROLLARY 3.15 *The pairs (A, ρ) consisting of a simple CM abelian variety and an embedding $\mathrm{End}^0(A) \hookrightarrow \mathbb{Q}^{\mathrm{al}}$ are classified up to isogeny by the CM-types on $\mathbb{Q}^{\mathrm{cm}}$.*

REMARK 3.16 Let A be a simple abelian variety corresponding, as in the Corollary, to the Γ-orbit Ψ, and let $E = \mathrm{End}^0(A)$. For each $\psi \in \Psi$, let E_ψ be the fixed field of $\{\sigma \in \Gamma \mid \sigma\psi = \psi\}$. Then, as ψ runs through Ψ, E_ψ runs through the conjugates of E in $\mathbb{Q}^{\mathrm{al}}$.

Classification up to isomorphism

Let (A, i) be of CM-type (E, Φ). Let e be an E-basis element of $H_1(A, \mathbb{Q})$, and set $H_1(A, \mathbb{Z}) = \mathfrak{a}e$ with $\mathfrak{a}$ a lattice in E. We saw in (3.11) that e determines an isomorphism

$$\theta\colon (A_\Phi, i_\Phi) \to (A, i), \quad A_\Phi \stackrel{\mathrm{def}}{=} \mathbb{C}^\Phi/\Phi(\mathfrak{a}).$$

Conversely, every isomorphism $\mathbb{C}^\Phi/\Phi(\mathfrak{a}) \to A$ commuting with the actions of E arises in this way from an E-basis element of $H_1(A, \mathbb{Q})$, because

$$E \simeq H_1(A_\Phi, \mathbb{Q}) \stackrel{\theta}{\simeq} H_1(A, \mathbb{Q}).$$

If e is replaced by ae, $a \in E^\times$, then θ is replaced by $\theta \circ a^{-1}$.

We use this observation to classify triples (A, i, ψ) where A is an abelian variety, $i\colon E \to \mathrm{End}^0(A)$ is a homomorphism making $H_1(A, \mathbb{Q})$ into a free module of rank 1 over the CM-algebra E, and ψ is a rational Riemann form whose Rosati involution stabilizes $i(E)$ and induces ι_E on it.

Let $\theta\colon \mathbb{C}^\Phi/\Phi(\mathfrak{a}) \to A$ be the isomorphism defined by some basis element e of $H_1(A, \mathbb{Q})$. According to (2.9), there exists a unique element $t \in E^\times$ such that $\psi(xe, ye) = \mathrm{Tr}_{E/\mathbb{Q}}(tx\overline{y})$. The triple (A, i, ψ) is said to be of ***type*** $(E, \Phi; \mathfrak{a}, t)$ relative to θ (cf. Shimura 1971, Section 5.5 B).

PROPOSITION 3.17 *The type $(E, \Phi; \mathfrak{a}, t)$ determines (A, i, ψ) up to isomorphism. Conversely, (A, i, ψ) determines the type up to a change of the following form: if θ is replaced by $\theta \circ a^{-1}$, $a \in E^\times$, then the type becomes $(E, \Phi; a\mathfrak{a}, t/a\overline{a})$. The quadruples $(E, \Phi; \mathfrak{a}, t)$ that arise as the type of some triple are exactly those in which (E, Φ) is a CM-pair, $\mathfrak{a}$ is a lattice in E, and t is an element of $E^\times$ such that $\iota_E t = -t$ and $\Im(\varphi(t)) > 0$ for all $\varphi \in \Phi$.*

PROOF. Routine verification. □

[19] *We mean by this that there is a canonical map sending a simple abelian variety with complex multiplication to an orbit of CM-types whose fibres are exactly the isogeny classes.*

4 Mumford-Tate groups

Review of algebraic groups of multiplicative type

Let k be a field of characteristic zero. We use the terminology from AAG. In particular, by an affine algebraic group over a field k, we mean a functor G from k-algebras to groups that is represented by a finitely generated k-algebra $k[G]$ (which is automatically geometrically reduced; ibid. 2.31). The algebra $k[G]$ has maps Δ, ϵ, S which make it into a k-bialgebra,[20] and every k-bialgebra arises from a (unique) affine algebraic group.

For any finitely generated abelian group M (written multiplicatively), the functor $D(M)$ of k-algebras

$$R \mapsto \mathrm{Hom}(M, R^\times) \qquad \text{(homomorphisms of abelian groups)}$$

is an affine algebraic group with bialgebra $k[M]$, the k-vector space with basis the elements of M and the k-bialgebra structure

$$(\textstyle\sum_i a_i m_i)(\sum_j b_j m_j) = \sum_{i,j} a_i b_j m_i m_j, \quad a_i, b_j \in k, \quad m_i, m_j \in M,$$
$$\Delta(m) = m \otimes m, \quad \epsilon(m) = 1, \quad S(m) = m^{-1}.$$

The affine algebraic groups G arising in this way are called ***diagonalizable groups***. They are exactly those whose bialgebra is generated by "group-like" elements, i.e., elements m such that $\Delta(m) = m \otimes m$. The group-like elements in $k[M]$ are exactly the elements of M.

The diagonalizable group associated with the abelian group $\mathbb{Z}$ is $\mathbb{G}_m$, which represents the functor

$$R \mapsto R^\times.$$

Its bialgebra is $k[T, T^{-1}]$ with

$$\Delta(T) = T \otimes T, \quad \epsilon(T) = 1, \quad S(T) = T^{-1}.$$

For any affine algebraic group G, there is an isomorphism

$$\chi \mapsto T \circ \chi : \mathrm{Hom}(G, \mathbb{G}_m) \to \{\text{group-like elements in } k[G]\}.$$

Let G be an affine algebraic group, and let m be a group-like element in $k[G]$. For a k-algebra R, $G(R)$ is $\mathrm{Hom}_{k\text{-alg}}(k[G], R)$, and so m defines a map $g \mapsto g(m) : G(R) \to R$. For any k-vector space V, the maps

$$(g, v) \mapsto g(m) \cdot v : G(R) \times V(R) \to V(R)$$

define a representation of G on V; we then say that G ***acts on*** V ***through*** m. Let $\rho : G \to \mathrm{GL}_V$ be a representation of G on a finite-dimensional k-vector space V. For each group-like element $m \in k[G]$, there is a largest subspace V_m of V on which G acts through m, and G is diagonalizable if and only if every representation decomposes into a direct sum $V = \bigoplus_{m \in M} V_m$.[21] Thus, to give a representation of a diagonalizable group $G = D(M)$ on a vector space amounts to giving an M-grading of the vector space.

[20] In the nonstandard terminology of AAG.

[21] Let $\rho : G \to \mathrm{GL}_V$ be a representation of G. Then $V = \bigoplus_m V_m$ if and only if V has a basis for which $\rho(G) \subset \mathbb{D}$ (the group of invertible diagonal matrices). Therefore, G is diagonalizable if and only if each of its representations are diagonalizable.

Fix an algebraic closure k^{al} of k and let $\Gamma = \mathrm{Gal}(k^{\mathrm{al}}/k)$. An affine algebraic group G over k is said to be of ***multiplicative type*** if $G_{k^{\mathrm{al}}}$ is diagonalizable. The functor

$$G \mapsto X^*(G) = \mathrm{Hom}(G_{k^{\mathrm{al}}}, \mathbb{G}_m)$$

defines a contravariant equivalence from the category of algebraic groups of multiplicative type over k to the category of finitely generated abelian groups with a continuous action of Γ. Because $X^*(G)$ is finitely generated, "continuous" simply means that some open subgroup of Γ acts trivially. To give a representation of a group of multiplicative type G on a k-vector space V is to give a $X^*(G)$-grading

$$V \otimes_k k^{\mathrm{al}} = \bigoplus\nolimits_{\chi \in X^*(G)} V_\chi$$

such that Γ permutes the subspaces V_χ according to the rule,

$$\sigma V_\chi = V_{\sigma\chi}.$$

A group G of multiplicative type is connected if and only if $X^*(G)$ is torsion-free, in which case G is called a ***torus split*** if Γ acts trivially on $X^*(G)$).

For a finite field extension K/k, we write $(\mathbb{G}_m)_{K/k}$ for the affine algebraic group

$$R \mapsto (K \otimes R)^\times$$

over k (***torus over*** k ***obtained by restriction of scalars from*** $\mathbb{G}_m$ ***over*** K). It is the torus corresponding to the Γ-module $\mathbb{Z}^{\mathrm{Hom}_k(K, k^{\mathrm{al}})}$, i.e., a character of $(\mathbb{G}_m)_{K/k}$ is a finite sum

$$\sum\nolimits_{\sigma: K \to k^{\mathrm{al}}} n(\sigma)\sigma, \quad n(\sigma) \in \mathbb{Z}, \ (\sigma \text{ runs over the } k\text{-algebra homomorphisms})$$

which acts by sending $c \otimes r \in (K \otimes R)^\times$ to $\prod_\sigma \sigma(c)^{n(\sigma)} \cdot r \in (k^{\mathrm{al}} \otimes R)^\times$. To give a representation of $(\mathbb{G}_m)_{K/k}$ on a k-vector space V is to give a decomposition $k^{\mathrm{al}} \otimes_k V = \bigoplus_{\sigma: K \to k^{\mathrm{al}}} V_\sigma$ such that $\tau V_\sigma = V_{\tau\sigma}$ for all $\tau \in \mathrm{Gal}(k^{\mathrm{al}}/k)$. For example, let $\mathbb{S} = (\mathbb{G}_m)_{K/k}$. To give a representation of $\mathbb{S}$ on a real vector space V is to give a decomposition $\mathbb{C} \otimes_{\mathbb{R}} V = V_+ \oplus V_-$ such that $V_- = \iota V_+$.

Let k^{al} be an algebraic closure of k, and let $\Gamma = \mathrm{Gal}(k^{\mathrm{al}}/k)$. For any affine algebraic group G, the pairing

$$(\chi, \mu) \mapsto \langle \chi, \mu \rangle \stackrel{\mathrm{def}}{=} \chi \circ \mu \colon X^*(G) \times X_*(G) \to \mathrm{End}(\mathbb{G}_m) \simeq \mathbb{Z}$$

is bi-additive and Γ-equivariant, i.e.,

$$\langle \sigma\chi, \sigma\mu \rangle = \langle \chi, \mu \rangle, \quad \chi \in X^*(G), \quad \mu \in X_*(G), \quad \sigma \in \mathrm{Gal}(k^{\mathrm{al}}/k).$$

For groups G of multplicative type, it is non-degenerate in the sense that

$$\mu \mapsto \langle \cdot, \mu \rangle \colon X_*(G) \to \mathrm{Hom}(X^*(G), \mathbb{Z}) \quad (\mathbb{Z}\text{-module homomorphisms})$$

is an isomorphism of $\mathbb{Z}[\Gamma]$-modules.

Let $\rho \colon G \to \mathrm{GL}_V$ be a representation of an algebraic group G. Then ρ applied to the "universal element"

$$\mathrm{id}_{k[G]} \in \mathrm{End}_{k\text{-alg}}(k[G]) = G(k[G])$$

is a linear map

$$k[G] \otimes_k V \xrightarrow{\rho(\mathrm{id}_{k[G]})} k[G] \otimes_k V$$

whose restriction to V,

$$\tilde{\rho}\colon V \to k[G] \otimes_k V$$

determines ρ. An endomorphism α of the k-vector space V is an endomorphism of the representation (V, ρ) if and only if the diagram

$$\begin{array}{ccc} V & \xrightarrow{\tilde{\rho}} & k[G] \otimes_k V \\ {\scriptstyle\alpha}\downarrow & & {\scriptstyle\mathrm{id}\otimes\alpha}\downarrow \\ V & \xrightarrow{\tilde{\rho}} & k[G] \otimes_k V \end{array}$$

commutes. This is a linear condition on α, and so, for any field K containing k,

$$\mathrm{End}(V_K, \rho_K) = \mathrm{End}(V, \rho) \otimes_k K. \tag{27}$$

PROPOSITION 4.1 *Let G be a group of multiplicative type over a field k of characteristic zero. For any representation $\rho\colon G \to \mathrm{GL}_V$,*

$$[\mathrm{End}(V, \rho)\colon \mathbb{Q}]_{red} = \dim V.$$

PROOF. If G is diagonalizable, then $V = \bigoplus_m V_m$ (sum over the group-like elements of $k[G]$), and

$$\mathrm{End}(V, \rho) \simeq \prod\nolimits_m \mathrm{End}_{k\text{-linear}}(V_m) \approx \prod\nolimits_m M_{\dim(V_m)}(k),$$

from which the statement follows. In the general case, G becomes diagonalizable over a finite extension K of k, and

$$\dim_k V = \dim_K(V \otimes_k K) = [\mathrm{End}(V, \rho) \otimes_k K\colon K]_{\mathrm{red}} \overset{(1)}{=} [\mathrm{End}(V, \rho)\colon \mathbb{Q}]_{\mathrm{red}}. \qquad \square$$

CM-pairs and tori

Recall that $\mathbb{S}$ is the real torus with $\mathbb{S}(\mathbb{R}) = \mathbb{C}^\times$. There are characters z and $\overline{z}$ of $\mathbb{S}$ inducing the maps $z \mapsto z$ and $z \mapsto \overline{z}$ respectively on the real points of $\mathbb{S}$,

$$\mathbb{C}^\times = \mathbb{S}(\mathbb{R}) \subset \mathbb{S}(\mathbb{C}) \rightrightarrows \mathbb{G}_m(\mathbb{C}) = \mathbb{C}^\times.$$

Let μ be the cocharacter of $\mathbb{S}$ such that

$$\begin{cases} z \circ \mu &= \mathrm{id}_{\mathbb{G}_m} \\ \overline{z} \circ \mu &= 1 \end{cases}.$$

The characters $z, \overline{z}$ of $\mathbb{S}$ define an isomorphism

$$\mathbb{S}_{\mathbb{C}} \xrightarrow{(z,\overline{z})} \mathbb{G}_m \times \mathbb{G}_m \tag{28}$$

and μ is the cocharacter of $\mathbb{S}_{\mathbb{C}}$ such that $\mu(x)$ maps to $(x, 1)$ in $\mathbb{G}_m \times \mathbb{G}_m$.

Let (E,Φ) be a CM-pair, and let $T^E = (\mathbb{G}_m)_{E/\mathbb{Q}}$. As noted in §1 (3), Φ defines an isomorphism $E\otimes_{\mathbb{Q}}\mathbb{R}\to\prod_{\varphi\in\Phi}\mathbb{C}$, and hence an isomorphism[22]

$$T^E_{\mathbb{R}} \simeq \mathbb{S}^{\Phi}. \tag{29}$$

Define

$$h_{\Phi}\colon \mathbb{S}\to T^E_{\mathbb{R}}$$

to be the homomorphism whose composite with (29) is

$$z\mapsto (z,\dots,z).$$

The isomorphism $E\otimes_{\mathbb{Q}}\mathbb{C}\simeq\prod_{\varphi\in I}\mathbb{C}$, $I=\mathrm{Hom}(E,\mathbb{C})$, defines an isomorphism

$$T^E_{\mathbb{C}} \simeq (\mathbb{G}_m)^I\ .$$

The cocharacter

$$\mu_{\Phi} \overset{\text{def}}{=} h_{\Phi}\circ\mu\colon \mathbb{G}_{m\mathbb{C}}\to T^E_{\mathbb{C}}$$

corresponding to h_{Φ} satisfies

$$\mu_{\Phi}(z)_{\varphi} = \begin{cases} z & \text{if} \quad \varphi\in\Phi \\ 1 & \text{if} \quad \varphi\notin\Phi. \end{cases}$$

Recall that the reflex field E^* of (E,Φ) is the subfield of $\mathbb{C}$ generated by the elements

$$\sum\nolimits_{\varphi\in\Phi}\varphi(a),\quad a\in E.$$

It can also be described as the field of definition of μ_{Φ}.

The reflex norm in terms of tori

Let (E,Φ) be a CM-pair, and let $T^{E^*} = (\mathbb{G}_m)_{E^*/\mathbb{Q}}$ and $T^E = (\mathbb{G}_m)_{E/\mathbb{Q}}$. The composite of the homomorphisms

$$\mathbb{G}_{m/E^*}\overset{\mu_{\Phi}}{\longrightarrow} T^E_{/E^*}\overset{\mathrm{Nm}_{E^*/\mathbb{Q}}}{\longrightarrow} T^E$$

is the reflex norm N_{Φ}. Thus, for $a\in E^{*\times}$,

$$N_{\Phi}(a) = \mathrm{Nm}_{E^*\otimes_{\mathbb{Q}}E/E}\,\mu_{\Phi}(a).$$

Complex multiplication in terms of tori

Let A be an abelian variety, and let $V/\Lambda\simeq A$ be its canonical parametrization. Then

$$\begin{aligned}\Lambda &\simeq H_1(A,\mathbb{Z})\\ \Lambda\otimes\mathbb{R} &\simeq H_1(A,\mathbb{R})\\ \Lambda\otimes\mathbb{R}\simeq V &\simeq \mathrm{Tgt}_0(A)\end{aligned}$$

and so

$$H_1(A,\mathbb{R})\simeq\mathrm{Tgt}_0(A).$$

In particular, $H_1(A,\mathbb{R})$ acquires the structure of a complex vector space from its identification with $\mathrm{Tgt}_0(A)$. Also $\mathrm{End}(A)$ (resp. $\mathrm{End}^0(A)$) consists of the endomorphisms of $\Lambda\simeq H_1(A,\mathbb{Z})$ (resp. $H_1(A,\mathbb{Q})$) whose linear extensions to $H_1(A,\mathbb{R})\simeq\mathrm{Tgt}_0(A)$ are $\mathbb{C}$-linear.

[22] By $\mathbb{S}^{\Phi}$ we mean a product of copies of $\mathbb{S}$ indexed by Φ.

PROPOSITION 4.2 *An abelian variety A has complex multiplication if and only if there exists a torus $T \subset \mathrm{GL}_{H_1(A,\mathbb{Q})}$ such that $T(\mathbb{R})$ contains all homotheties $v \mapsto zv\colon H_1(A,\mathbb{R}) \to H_1(A,\mathbb{R})$, $z \in \mathbb{C}^\times$.*

PROOF. If A has complex multiplication, then there exists an étale $\mathbb{Q}$-algebra $E \subset \mathrm{End}^0(A)$ for which $H_1(A,\mathbb{Q})$ is a free E-module of rank 1. The action of $E \otimes \mathbb{R}$ on $H_1(A,\mathbb{R})$ commutes with that of $\mathbb{C}$, and so $\mathbb{C}$ is contained in the centralizer of $E \otimes \mathbb{R}$ in $\mathrm{End}_{\mathbb{R}}(H_1(A,\mathbb{R}))$, which is $E \otimes \mathbb{R}$ itself. Therefore we can take $T = (\mathbb{G}_m)_{E/\mathbb{Q}} \subset \mathrm{GL}_{H_1(A,\mathbb{Q})}$.

Conversely, let $\rho\colon T \hookrightarrow \mathrm{GL}_{H_1(A,\mathbb{Q})}$ be a subtorus. If $\mathbb{C}^\times \subset T(\mathbb{R})$, then $\mathrm{End}^0(A) \supset \mathrm{End}(H_1(A,\mathbb{Q}),\rho)$, and Proposition 4.1 shows that A has complex multiplication. □

Mumford-Tate groups

By a ***rational Riemann pair*** (V,J), we mean a finite-dimensional $\mathbb{Q}$-vector space V together with a complex structure J on $V \otimes \mathbb{R}$. By ***Riemann form*** on (V,J), we mean an alternating bilinear form ψ on V such that

- ◇ $\psi(Jx,Jy) = \psi(x,y)$ for all $x, y \in V_{\mathbb{R}}$, and
- ◇ $\psi(x,Jy) > 0$ for all nonzero x in $V_{\mathbb{R}}$.

Then $\psi_J(x,y) \stackrel{\text{def}}{=} \psi_{\mathbb{R}}(x,Jy)$ is a symmetric positive-definite form on $V_{\mathbb{R}}$.

Let $\mathbb{S} = (\mathbb{G}_m)_{\mathbb{C}/\mathbb{R}}$, so that $\mathbb{S}(\mathbb{R}) = \mathbb{C}^\times$. There is a homomorphism $h\colon \mathbb{S} \to \mathrm{GL}_{V_{\mathbb{R}}}$ such that $h(z)$ acts on $V_{\mathbb{R}}$ as multiplication by z.

LEMMA 4.3 *Let (V,J) be a rational Riemann pair. The following conditions on an algebraic subgroup G of GL_V are equivalent:*

(a) *$H(\mathbb{R})$ contains the homotheties $v \mapsto zv$, $z \in \mathbb{C}^\times$;*
(b) *$H(\mathbb{Q})$ contains the homotheties $v \mapsto zv$, $z \in \mathbb{Q}^\times$, and $H(\mathbb{R})$ contains J;*
(c) *H contains $h(\mathbb{S})$.*

PROOF. Certainly (a) implies (b). If $H(\mathbb{Q})$ contains the homotheties $v \mapsto zv$, $z \in \mathbb{Q}^\times$, then $H \supset \mathbb{G}_m$. As $h(\mathbb{S})$ is generated by $\mathbb{G}_m$ and J, (b) implies (c). Finally, (c) implies (a) because $h(\mathbb{S})(\mathbb{R}) = \mathbb{C}^\times$. □

DEFINITION 4.4 The ***Mumford-Tate group*** of a rational Riemann pair (V,J) is the smallest algebraic subgroup of GL_V satisfying the equivalent conditions of Lemma 4.3. The ***Mumford-Tate group*** of a complex abelian variety is the Mumford-Tate group of the associated rational Riemann pair $(H_1(A,\mathbb{Q}),J)$.

Thus, $\mathrm{MT}(A)$ is the smallest algebraic subgroup G of $\mathrm{GL}_{H_1(A,\mathbb{Q})}$ such that $G(\mathbb{R})$ contains all homotheties

$$v \mapsto zv\colon H_1(A,\mathbb{R}) \to H_1(A,\mathbb{R}), \quad z \in \mathbb{C}^\times. \tag{30}$$

If G_1 and G_2 are algebraic subgroups of GL_V satisfying the conditions of (4.3), then $G_1 \cap G_2$ has the same property, and so there is certainly is a smallest subgroup with this property.

PROPOSITION 4.5 *A $\mathbb{Q}$-subspace W of V is stable under $G = \mathrm{MT}(V,J)$ if and only if $W \otimes \mathbb{R}$ is a $\mathbb{C}$-subspace of $V \otimes \mathbb{R}$.*

PROOF. Recall (e.g., AAG 13.13), that there exists an algebraic subgroup H of GL_V, called the stabilizer of W, such that

$$H(R) = \{\alpha \in \mathrm{GL}(V \otimes R) \mid \alpha(W \otimes R) = W\}, \quad \text{all } \mathbb{Q}\text{-algebras } R. \tag{31}$$

Let W be a $\mathbb{Q}$-subspace of V and let H be the stabilizer of W in GL_V. Then

$$\begin{aligned} W \otimes \mathbb{R} \text{ is a } \mathbb{C}\text{-subspace of } H_1(A,\mathbb{R}) &\iff H(\mathbb{R}) \text{ contains the homotheties } v \mapsto zv,\ z \in \mathbb{C}, \\ &\iff H \supset \mathrm{MT}(V,J), \\ &\iff W \text{ is stable under } \mathrm{MT}(V,J). \end{aligned}$$

□

PROPOSITION 4.6 *The Mumford-Tate group of a Riemann pair is connected, and it is reductive if the riemann pair is polarizable.*

PROOF. As $\mathbb{S}$ is connected, if $G_{\mathbb{R}} \supset h(\mathbb{S})$, then $(G^\circ)_{\mathbb{R}} \overset{\text{AAG 8.15}}{=} (G_{\mathbb{R}})^\circ \supset h(\mathbb{S})$, which shows that the smallest G is connected.

Every subspace W of V stable under $\mathrm{MT}(V,J)$ has a complement stable under $\mathrm{MT}(A)$, namely, its orthogonal complement for some Riemann form. Now use that any affine algebraic group with a faithful semisimple representation is reductive (fairly easy; see Deligne and Milne 1982, p143). □

COROLLARY 4.7 *An abelian variety has complex multiplication if and only if its Mumford-Tate group is commutative (in which case, it is a torus).*

PROOF. The only connected commutative reductive groups are tori, and so this follows from Proposition 4.2. □

PROPOSITION 4.8 *For abelian varieties $A_1, \dots, A_n$,*

$$\mathrm{MT}(A_1 \times \cdots \times A_n) \subset \mathrm{MT}(A_1) \times \cdots \times \mathrm{MT}(A_n),$$

and the projections $\mathrm{MT}(A_1 \times \cdots \times A_n) \to \mathrm{MT}(A_i)$ are surjective.

PROOF. To get the inclusion, we identify the two vector spaces

$$H_1(A_1 \times \cdots \times A_n, \mathbb{Q}) \simeq H_1(A_1,\mathbb{Q}) \oplus \cdots \oplus H_1(A_n,\mathbb{Q}).$$

Then the statements are obvious from the definition of the Mumford-Tate group. □

Infinity types

Let Ω be a Galois extension of $\mathbb{Q}$ (for example, $\Omega = \mathbb{Q}^{\mathrm{al}}$). Recall that a complex conjugation on Ω is any involution defined by complex conjugation on $\mathbb{C}$ and an embedding $\Omega \hookrightarrow \mathbb{C}$.

Let K be a number field. The set of maps $\mathrm{Hom}(K,\Omega) \to \mathbb{Z}$ is an abelian group, which we denote by $\mathbb{Z}^{\mathrm{Hom}(K,\Omega)}$. We sometimes regard $\mathbb{Z}^{\mathrm{Hom}(K,\Omega)}$ as the free abelian group on $\mathrm{Hom}(K,\Omega)$, and regard $f\colon \mathrm{Hom}(K,\Omega) \to \mathbb{Z}$ as a finite sum

$$\sum\nolimits_{\rho: K \to \Omega} f(\rho)\rho, \quad f(\rho) \in \mathbb{Z}.$$

We let $\sigma \in \mathrm{Gal}(\Omega/\mathbb{Q})$ act on $\mathbb{Z}^{\mathrm{Hom}(K,\mathbb{Q})}$ according to the rule

$$\sigma f = \sum f(\rho) \cdot \sigma \circ \rho = \sum f(\sigma^{-1} \circ \rho) \cdot \rho.$$

PROPOSITION 4.9 *Let K be a number field, and assume Ω contains all conjugates of K. Let $\Gamma = \mathrm{Hom}(K, \Omega)$. The following three conditions on a map $f\colon \Gamma \to \mathbb{Z}$ are equivalent:*

(a) *$f(\rho)+f(\iota\circ\rho)$ is constant (independent of $\rho\colon K \to \Omega$ and of the complex conjugation ι on Ω);*

(b) *let K' be the composite of the CM-subfields[23] of K, and fix a complex conjugation ι on Ω; then*

  i) *$f(\rho)$ depends only on $\rho|K'$ and*

  ii) *$f(\rho) + f(\iota \circ \rho)$ is constant (independent of ρ).*

(c) *for a fixed complex conjugation ι on Ω, and for all $\sigma \in \mathrm{Gal}(\Omega/\mathbb{Q})$,*

$$(\sigma - 1)(\iota + 1) f = 0 = (\iota + 1)(\sigma - 1) f. \tag{32}$$

PROOF. (a) $\Longrightarrow$ (b). We may replace Ω with the composite of the conjugates of K in Ω, and so assume that Ω is of finite degree. Suppose first that Ω contains a CM-subfield, so that K' is the largest such subfield. For any $\rho\colon K \to \Omega$, $\rho K'$ is the subfield of ρK fixed by all commutators $[\sigma, \iota]$ where $\sigma \in \mathrm{Gal}(\Omega/\mathbb{Q})$ and ι is the fixed complex conjugation on Ω (see 1.6). Hence two embeddings $K \to \Omega$ agree on K' if and only if they differ by such a commutator.[24]

We are given that

$$f(\rho) + f(\iota\rho) = f(\rho) + f(\sigma\iota\sigma^{-1}\rho), \text{ all } \rho\colon K \to \Omega, \sigma \in \mathrm{Gal}(\Omega/\mathbb{Q}).$$

On replacing ρ with $\iota\rho$ in this, we find that

$$f(\rho) = f([\sigma, \iota] \circ \rho), \text{ all } \rho\colon K \to \Omega, \sigma \in \mathrm{Gal}(\Omega/\mathbb{Q}),$$

and so $f(\rho)$ depends only on $\rho|K'$.

Next suppose that Ω doesn't contain a CM-field, and let K' be the largest totally real subfield. The same argument as above shows that $f(\rho)$ depends only on $\rho|K'$, and so $2f(\rho) = f(\rho) + f(\iota \circ \rho) =$constant. Hence $f(\rho)$ is independent of ρ.

(c) $\Longrightarrow$ (b). The two equalities can be rewritten as

$$\begin{aligned}(\sigma\iota - \iota + \sigma - 1) f &= 0 \\ (\iota\sigma - \iota + \sigma - 1) f &= 0.\end{aligned} \tag{33}$$

Their difference gives

$$\sigma\iota f = \iota\sigma f \text{ for all } \sigma \in \mathrm{Gal}(\Omega/K). \tag{34}$$

When evaluated at ρ, the (33) becomes

$$f(\sigma^{-1}\rho) + f(\iota\sigma^{-1}\rho) = f(\rho) + f(\iota\rho). \tag{35}$$

Equation (34) shows that $f(\rho)$ depends only on $\rho|K'$ (as in the proof of (a) $\Longrightarrow$ (b)), and (35) shows that $f(\rho) + f(\iota\rho)$ is independent of ρ.

(b) $\Longrightarrow$ (a,c). Suppose first that K is a CM-field. Then (b)(ii) implies (a), because $\iota \circ \rho = \rho \circ \iota_E$ for every complex conjugation ι of Ω. Similarly, it implies (c).

Next suppose that K isn't a CM-field. Then (b)(i) says f arises by extension from a function on K', for which (a) and (c) hold. It follows that (a) and (c) hold for f itself. □

[23] *Thus, $K = \mathbb{Q}$ if there are no CM-subfields of K.*

[24] Let $\rho, \rho'\colon K \to \Omega$ be two embeddings. The obvious isomorphism $\rho K \to \rho' K$ extends to an automorphism τ of Ω, and ρ and ρ' agree on K' if and only if τ fixes $\rho K'$, i.e., $\tau = [\sigma, \iota]$ for some $\sigma \in \mathrm{Gal}(\Omega/\mathbb{Q})$.

DEFINITION 4.10 An ***infinity type*** on K with values in Ω is an element $f \in \mathbb{Z}^{\mathrm{Hom}(K,\Omega)}$ satisfying the equivalent conditions of (4.9).

The negative of the constant value $f(\rho) + f(\iota \circ \rho)$ is called the ***weight*** of f:

$$w(f) = -f(\rho) - f(\iota \circ \rho) \text{ for all } \rho, i.$$

Note that the weight is additive

$$w(\textstyle\sum_i f_i) = \sum_i w(f_i)$$

and that a CM-type on a field K is exactly an infinity type of weight -1.

We now write $I(K)$ for the group of infinity types with values in $\mathbb{Q}^{\mathrm{al}}$.

PROPOSITION 4.11 *Let K be a number field, and let K' be the composite of the CM-subfields of K. Then*

$$f \mapsto \textstyle\sum f(\rho|K')\rho \colon I(K') \to I(K)$$

is an isomorphism. In particular, if K doesn't contain a CM-field, then

$$\mathbb{Z} = I(\mathbb{Q}) \to I(K)$$

is an isomorphism.

PROOF. Immediate from the description of $I(K)$ given in (4.9b). □

It remains to determine $I(K)$ in the case that K is CM.

PROPOSITION 4.12 *Let K be a CM-field, and let $\{\varphi_1, \dots, \varphi_g\}$ be a CM-type on K. Define CM-types*

$$\begin{aligned} \phi_i &= \varphi_i + \textstyle\sum_{j \neq i} \iota \circ \varphi_j, \quad i = 1, \dots, n, \\ \overline{\phi} &= \textstyle\sum_{1 \le j \le n} \iota \circ \varphi_j. \end{aligned}$$

Then $\{\phi_1, \dots, \phi_n, \overline{\phi}\}$ is a basis for the $\mathbb{Z}$-module $I(K)$.

PROOF. Let $f \in I(K)$. Then

$$f = \textstyle\sum_{1 \le j \le n} f(\varphi_i)\phi_i - \Big(w(f) + \sum_{1 \le i \le n} f(\varphi_i)\Big)\overline{\phi},$$

because the two sides agree on each φ_i and have the same weight. This shows that $\{\phi_1, \dots, \phi_n, \overline{\phi}\}$ spans $I(K)$, and it is obvious that it is linearly independent. □

PROPOSITION 4.13 *For any CM-field K, there is a commutative diagram*

$$\begin{array}{ccc} I(K) & \xrightarrow{\quad 1+\iota \quad} & I(K) \\ & {\scriptstyle -w} \searrow \quad \nearrow & \\ & \mathbb{Z} & \end{array}$$

where the unmarked arrow sends $m \in \mathbb{Z}$ to the constant function with value m.

PROOF. For any $f \in I(K)$ and $\rho\colon K \to \mathbb{Q}^{\mathrm{al}}$,

$$((1+\iota)f)(\rho) = f(\rho) + f(\iota\rho) = -w(f),$$

i.e., $(1+\iota)f$ is the constant function with value $-w(f)$. □

PROPOSITION 4.14 *For any CM-field K with totally real subfield F, there is an exact sequence*

$$0 \longrightarrow I(K) \xrightarrow[(f,w(f))]{f\mapsto} \mathbb{Z}^{\mathrm{Hom}(K,\mathbb{Q}^{\mathrm{al}})} \times \mathbb{Z} \xrightarrow[f|F+m]{(f,m)\mapsto} \mathbb{Z}^{\mathrm{Hom}(F,\mathbb{Q}^{\mathrm{al}})} \longrightarrow 0 \qquad (36)$$

PROOF. Obvious. □

Consider number fields $K \subset L$. An infinity type f on K extends to an infinity type f_L on L by the rule:

$$f_L(\rho) = f(\rho|L).$$

Define

$$I = \varinjlim I(K)$$

(limit over all subfields of $\mathbb{Q}^{\mathrm{al}}$; equivalently, over all CM-subfields of $\mathbb{Q}^{\mathrm{al}}$). In a natural way, I can be identified with the group of locally constant homomorphisms $f\colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q}) \to \mathbb{Z}$ such that

$$f(\rho) + f(\sigma\iota\sigma^{-1}\rho) \text{ is constant (independent of } \sigma, \rho \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})),$$

and with the group of locally constant homomorphism $f\colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{cm}}/\mathbb{Q}) \to \mathbb{Z}$ such that

$$f(\rho) + f(\iota\rho) \text{ is constant (independent of } \rho \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{cm}}/\mathbb{Q})).$$

Such functions f are called infinity types on $\mathbb{Q}^{\mathrm{al}}$ or $\mathbb{Q}^{\mathrm{cm}}$ respectively.

REMARK 4.15 Let K be a CM-field with largest totally real subfield F, and let f be an infinity type on K. For $a \in F^\times$ and embedding $\rho\colon K \to \mathbb{Q}^{\mathrm{al}}$, $\iota\rho(a) = \rho(a)$, and so

$$\rho(a)^{f(\rho)} \cdot \iota\rho(a)^{f(\iota\rho)} = \rho(a)^{f(\rho)+f(\iota\rho)} = \rho(a)^{-w(f)}.$$

Therefore,

$$\begin{aligned} f(a) &\overset{\text{def}}{=} \textstyle\prod_{\rho\colon K\to\mathbb{Q}^{\mathrm{al}}} \rho(a)^{f(\rho)} \\ &= \textstyle\prod_{\rho\colon F\to\mathbb{Q}^{\mathrm{al}}} \rho(a)^{-w(f)} \\ &= \mathrm{Nm}_{F/\mathbb{Q}}(a)^{-w(f)}. \end{aligned}$$

In particular, f maps $\mathcal{O}_F^\times$ into $\{\pm 1\}$. The unit theorem (ANT 5.1) shows that $\mathcal{O}_F^\times$ is of finite index in $\mathcal{O}_K^\times$, and so f is trivial on a subgroup of finite index in $\mathcal{O}_K^\times$.

The Serre group

DEFINITION AND UNIVERSAL PROPERTY

For a number field $K \subset \mathbb{Q}^{\mathrm{al}}$ we define the ***Serre group*** S^K of K to be the quotient of $(\mathbb{G}_m)_{K/\mathbb{Q}}$ such that

$$X^*(S^K) = I(K) \subset \mathbb{Z}^{\mathrm{Hom}(K,\mathbb{Q}^{\mathrm{al}})}.$$

More explicitly, S^K is the quotient of $(\mathbb{G}_m)_{K/\mathbb{Q}}$ by its subgroup

$$\bigcap\nolimits_{f\in I(K)} \mathrm{Ker}(f\colon (\mathbb{G}_m)_{K/\mathbb{Q}} \to \mathbb{G}_m).$$

It is an algebraic torus over $\mathbb{Q}$.

REMARK 4.16 As $I(K)$ is finitely generated, (4.15) shows that the kernel of

$$K^\times \to S^K(\mathbb{Q}) \tag{37}$$

contains a subgroup of $\mathcal{O}_K^\times$ of finite index. We shall see later (4.22) that S^K is the quotient of $(\mathbb{G}_m)_{K/\mathbb{Q}}$ by the Zariski closure of any sufficiently small subgroup of $\mathcal{O}_K^\times$.

Write ρ_0 for the given inclusion of K into $\mathbb{Q}^{\mathrm{al}}$. We let μ^K denote the cocharacter of S^K that acts on characters as $f \mapsto f(\rho_0)$.

LEMMA 4.17 *Let T be an algebraic torus over $\mathbb{Q}$. The following conditions on a cocharacter μ of T are equivalent:*

(a) *for every complex conjugation ι' of $\mathbb{Q}^{\mathrm{al}}$, $(\iota'+1)\mu$ is defined over $\mathbb{Q}$;*
(b) *μ is defined over some CM-subfield of $\mathbb{Q}^{\mathrm{al}}$, and $(\iota+1)\mu$ is defined over $\mathbb{Q}$;*
(c) *for all $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$,*

$$(\sigma-1)(\iota+1)\mu = 0 = (\iota+1)(\sigma-1)\mu. \tag{38}$$

PROOF. Similar to that of (4.9). (Note that requiring that $(\sigma-1)(\iota+1)\mu = 0$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ amounts to requiring that $(\iota+1)\mu$ be defined over $\mathbb{Q}$.) □

DEFINITION 4.18 Any one of the equivalent conditions in (4.17) will be called the ***Serre condition***.

For an algebraic torus T that splits over a CM-field, the Serre condition simply says that the weight

$$w(\mu) \overset{\mathrm{def}}{=} -(\iota+1)\mu$$

of μ is defined over $\mathbb{Q}$.

PROPOSITION 4.19 *The cocharacter μ^K of S^K satisfies the Serre condition. For any algebraic torus T defined over $\mathbb{Q}$ and cocharacter μ defined over K and satisfying the Serre condition, there is a unique homomorphism $\rho\colon S^K \to T$ (defined over $\mathbb{Q}$) such that*

$$\rho_{\mathbb{Q}^{\mathrm{al}}} \circ \mu^K = \mu. \tag{39}$$

PROOF. Recall that

$$\mu \mapsto \langle \cdot, \mu \rangle \colon X_*(S^K) \to \mathrm{Hom}(X^*(S^K), \mathbb{Z})$$

is an isomorphism of $\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})]$-modules. Because the characters of S^K satisfy (32), its cocharacters satisfy (38).

Let T be a torus over $\mathbb{Q}$, and let $\mu \in X_*(T)$. For $\chi \in X^*(T)$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$, define

$$f_\chi(\sigma) = \langle \sigma^{-1}\chi, \mu \rangle.$$

Then, for $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$,

$$f_{\tau\chi}(\sigma) \stackrel{\mathrm{def}}{=} \langle \sigma^{-1}\tau\chi, \mu \rangle = f_\chi(\tau^{-1}\sigma) = (\tau f_\chi)(\sigma).$$

It follows that if T is split by K, then $f_\chi(\sigma)$ depends only on $\sigma|K$. Moreover, if μ satisfies the Serre condition, then f is an infinity type on K. Therefore, we get a $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$-equivariant homomorphism

$$\chi \mapsto f_\chi \colon X^*(T) \to X^*(S^K),$$

which corresponds to a homomorphism

$$\rho \colon S^K \to T.$$

For σ_0 the given inclusion of K into $\mathbb{Q}^{\mathrm{al}}$,

$$f_\chi(\sigma_0) = \langle \mu, \chi \rangle,$$

i.e.,

$$\langle \mu^K, f_\chi \rangle = \langle \mu, \chi \rangle,$$

which proves (39). □

THE NORM MAP.

PROPOSITION 4.20 *For any inclusion of number fields $K \subset L$, there is a unique homomorphism*

$$\mathrm{Nm}_{L/K} \colon S^L \to S^K$$

such that

$$\mathrm{Nm}_{L/K} \circ \mu^L = \mu^K.$$

PROOF. For an infinity type f on K, define $f_L(\sigma) = f(\sigma|K)$. Then f_L is an infinity type on L, and the map $f \mapsto f_L \colon I(K) \to I(L)$ gives rise to the map $\mathrm{Nm}_{L/K}$. Alternatively, when L splits S^K, we can apply Proposition 4.19. □

Therefore, an inclusion of number fields gives rise to a commutative diagram

$$\begin{array}{ccc} (\mathbb{G}_m)_{L/\mathbb{Q}} & \twoheadrightarrow & S^L \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ (\mathbb{G}_m)_{K/\mathbb{Q}} & \twoheadrightarrow & S^K \end{array} \tag{40}$$

We define the ***Serre group*** (S, μ_{can}) to be the inverse limit

$$(S, \mu_{\text{can}}) = \varprojlim (S^K, \mu^K)$$

where K runs over the subfields of $\mathbb{Q}^{\text{al}}$ (or only the CM-subfields, see (4.23) below). The character group of S is I, and μ corresponds to $f \mapsto f(1)$.

PROPOSITION 4.21 *For any torus T defined over $\mathbb{Q}$ and cocharacter μ satisfying the Serre condition, there is a unique homomorphism $\rho\colon S \to T$ (defined over $\mathbb{Q}$) such that*

$$\rho_{\mathbb{Q}^{\text{al}}} \circ \mu_{\text{can}} = \mu.$$

PROOF. Apply Proposition 4.19. □

DESCRIPTION OF THE SERRE GROUP IN TERMS OF ARITHMETIC SUBGROUPS

Let K be a CM-field. We saw in (4.15) that the kernel of any infinity type f on K contains a subgroup of finite index in $\mathcal{O}_K^\times$. As $I(K)$ is finitely generated, it follows that the kernel of

$$K^\times \to S^K(\mathbb{Q})$$

contains a subgroup N of finite index in $\mathcal{O}_K^\times$. The next theorem shows the kernel of $(\mathbb{G}_m)_{K/\mathbb{Q}} \to S^K$ is the smallest algebraic subgroup of $(\mathbb{G}_m)_{K/\mathbb{Q}}$ containing any such an N.

THEOREM 4.22 *The Serre group of K is the quotient of $(\mathbb{G}_m)_{K/\mathbb{Q}}$ by the Zariski closure of any sufficiently small arithmetic subgroup of $(\mathbb{G}_m)_{K/\mathbb{Q}}(\mathbb{Q}) = K^\times$.*

PROOF. To be added (cf. Serre 1968, pII-9, Exercise 1). □

CALCULATION OF THE SERRE GROUP

PROPOSITION 4.23 *Let $K \subset \mathbb{Q}^{\text{al}}$ be a number field, and let K' be the composite of the CM-subfields of K. Then*

$$\text{Nm}_{K/K'}\colon S^K \to S^{K'}$$

is an isomorphism. In particular, if K doesn't contain a CM-field, then

$$\text{Nm}_{K/\mathbb{Q}}\colon S^K \to S^{\mathbb{Q}} = \mathbb{G}_m$$

is an isomorphism.

PROOF. According to (4.9), the inclusion $I(K') \hookrightarrow I(K)$ is a bijection, which implies the statement. □

SOME EXACT SEQUENCES

For simplicity, from now on we take $K \subset \mathbb{Q}^{\text{al}}$ to be a CM-field. There are homomorphisms

$\cdot$	$X^*(\cdot)$
$w^K\colon \mathbb{G}_m \to S^K$	$f \mapsto w(f)\colon I(K) \to \mathbb{Z}$
$\mu^K\colon \mathbb{G}_m \to S^K_{\mathbb{Q}^{\text{al}}}$	$f \mapsto f(1)\colon I(K) \to \mathbb{Z}$
$t^K\colon S^K \to \mathbb{G}_m$	$m \mapsto m\colon \mathbb{Z} \to I(K)$

Note that

$$t \circ w = -2$$
$$t \circ \mu = 1.$$

PROPOSITION 4.24 *For any CM-field K, the homomorphism $\mathrm{Nm}_{K/\mathbb{Q}}\colon (\mathbb{G}_m)_{K/\mathbb{Q}} \to \mathbb{G}_m$ factors through S^K, and gives rise to a commutative diagram*

$$\begin{array}{ccc} S^K & \xrightarrow{1+\iota} & S^K \\ & {\scriptstyle \mathrm{Nm}_{K/\mathbb{Q}}} \searrow \quad \nearrow {\scriptstyle -w^K} & \\ & \mathbb{G}_m & \end{array} \tag{41}$$

PROOF. Apply Proposition 4.13. □

For $a \in K^\times$, let $[a]$ be the image of a in $S^K(\mathbb{Q})$. For such points, the commutativity of (41) becomes the commutativity of

$$\begin{array}{ccccc} K^\times & \longrightarrow & S^K(\mathbb{Q}) & \xrightarrow{1+\iota} & S^K(\mathbb{Q} \\ & & {\scriptstyle \mathrm{Nm}_{K/\mathbb{Q}}} \searrow & \nearrow {\scriptstyle -w^K} & \\ & & \mathbb{Q}^\times & & \end{array} \qquad \begin{array}{ccccc} a & \longmapsto & [a] & \xmapsto{1+\iota} & [a\overline{a}]) \\ & & {\scriptstyle \mathrm{Nm}_{K/\mathbb{Q}}} \searrow & \nearrow {\scriptstyle -w^K} & \\ & & \mathrm{Nm}_{K/\mathbb{Q}}(a) & & \end{array}$$

PROPOSITION 4.25 *For any CM-field K and largest real subfield F, there is an exact sequence*

$$0 \to (\mathbb{G}_m)_{F/\mathbb{Q}} \xrightarrow{\binom{\text{incl.}}{\mathrm{Nm}_{K/\mathbb{Q}}}} (\mathbb{G}_m)_{E/\mathbb{Q}} \times \mathbb{G}_m \xrightarrow{(can., w^K)} S^K \to 1 \tag{42}$$

PROOF. Apply Proposition 4.14. □

In more detail, there is a commutative diagram

$$\begin{array}{ccccccccc} & & & & 1 & & 1 & & \\ & & & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{Ker} & \longrightarrow & (\mathbb{G}_m)_{F/\mathbb{Q}} & \xrightarrow{\mathrm{Nm}_{F/\mathbb{Q}}} & \mathbb{G}_m & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow{\scriptstyle w^K} & & \\ 1 & \longrightarrow & \mathrm{Ker} & \longrightarrow & (\mathbb{G}_m)_{K/\mathbb{Q}} & \longrightarrow & S^K & \longrightarrow & 1 \\ & & & & \downarrow & & \downarrow & & \\ & & & & (\mathbb{G}_m)_{K/\mathbb{Q}}/(\mathbb{G}_m)_{F/\mathbb{Q}} & \xrightarrow{\simeq} & S^K/w^K(\mathbb{G}_m) & \longrightarrow & 1 \\ & & & & \downarrow & & \downarrow & & \\ & & & & 1 & & 1 & & \end{array}$$

from which (42) can be extracted.

Abelian varieties of CM-type

Let (V, J) be a rational Riemann pair. Then

$$V \otimes_{\mathbb{Q}} \mathbb{C} = V_+ \oplus V_-$$

where $V_\pm$ are the ± 1 eigenspaces of J acting on $V \otimes_{\mathbb{Q}} \mathbb{C}$. Let $\mu = \mu_{(V,J)}$ be the cocharacter of $\mathrm{GL}_{V_{\mathbb{C}}}$ such that $\mu(z)$ acts as z on V_+ and as 1 on V_-. Then that $\iota\mu(z)$ acts as 1 on V_+ and as z on V_-, and so $\mu + \iota\mu$ is the cocharacter sending z to the homothety $v \mapsto zv$. In particular, it is defined over $\mathbb{Q}$.

When (V, J) is the rational Riemann pair of an abelian variety, we write μ_A for $\mu_{(V,J)}$.

PROPOSITION 4.26 *Let K be a CM-subfield of $\mathbb{Q}^{\mathrm{al}}$.*

(a) *For an abelian variety A of CM-type, μ_A is defined over K if and only if the reflex field of A is contained in K, in which case there is a unique homomorphism $\rho_A : S^K \to \mathrm{MT}(A)$ such that $\rho_A \circ \mu_{\mathrm{can}} = \mu_A$.*

(b) *For each abelian variety A of CM-type with reflex field contained in K, the homomorphism ρ_A is surjective, and, as A varies, the ρ_A define an isomorphism $\rho^K : S^K \to \varprojlim \mathrm{MT}(A)$.*

PROOF. (a) The maps ρ_A are surjective, and so $S \to \varprojlim \mathrm{MT}(A)$ is surjective. It is injective because the CM-types generate the character group of S. □

COROLLARY 4.27 *For any abelian variety A of CM-type, there is a unique homomorphism $\rho_A : S \to \mathrm{MT}(A)$ such that $\rho_A \circ \mu_{\mathrm{can}} = \mu_A$. Each ρ_A is surjective, and the ρ_A realize S as the inverse limit of the groups $MT(A)$.*

PROOF. Obvious from the proposition. □

5 Motives

The Hodge structure of an abelian variety

Discuss the Hodge structure on the cohomology of an abelian variety. Define the Hodge classes. Show that the Mumford-Tate group is the subgroup fixing the Hodge classes.

Abelian motives

Use the Hodge classes to define a category of abelian motives (in a feeble sense), i.e., write out the Grothendieck construction using the Hodge classes as correspondences.

Hodge structures

The usual stuff, including the Mumford-Tate group.

CM-motives

A rational Hodge structure is of ***CM-type*** if it is polarizable and its Mumford-Tate group is commutative (hence a torus).

PROPOSITION 5.1 *A rational Hodge structure (V,h) is of CM-type if and only if there exists a homomorphism $\rho\colon S \to \mathrm{GL}_V$ such that $\rho_{\mathbb{C}} \circ \mu^S = \mu_h$ (in which case ρ is unique).*

PROOF. O.K.. □

PROPOSITION 5.2 *The map $(V,\rho) \mapsto (V, \rho_{\mathbb{R}} \circ h)$ defines an equivalence from the category of representations of S to the category of Hodge structures of CM-type.*

PROOF. O.K.. □

PROPOSITION 5.3 *The functor H_B defines an equivalence from the category of CM motives to the category of CM Hodge structures.*

PROOF. O.K.. □

ASIDE 5.4 There are similar results for the category of all abelian motives, but they are much more complicated. Specifically, there is a pro-algebraic group G over $\mathbb{Q}$ together with a cocharacter μ_{can} such that

- ◇ the functor H_B defines an equivalence from the category of abelian motives to the category of Hodge structures whose Mumford-Tate group is a quotient of (G, μ_{can}) (abelian Hodge structures);
- ◇ the functor $(V,\rho) \mapsto (V, \rho_{\mathbb{R}} \circ h_{\mathrm{can}})$ defines an equivalence from the category of representations of G to the category of abelian Hodge structures.

For a description of (G, μ_{can}), based on work of Deligne, Satake, et al, see Milne 1994.

Chapter II

The arithmetic theory

6 Abelian varieties and their good reductions

We now define an ***abelian variety*** over a field k to be a complete algebraic variety over k together with a group structure defined by regular maps. The following hold (e.g., Milne 1986, 7.1, 2.2).

- ◇ Every abelian variety is projective.
- ◇ Let A and B be abelian varieties. Every regular map $A \to B$ sending 0_A to 0_B is a homomorphism. In particular, the algebraic group structure on A is uniquely determined by the zero element and is commutative (because it is equal to its opposite).

Complex abelian varieties and complex tori

The next proposition shows that, when $k = \mathbb{C}$, the definition of "abelian variety" in this chapter essentially agrees with that in the last chapter.

PROPOSITION 6.1 *For any abelian variety A over $\mathbb{C}$, $A(\mathbb{C})$ is a complex torus admitting a Riemann form. The map $A \mapsto A(\mathbb{C})$ defines an equivalence from the category of abelian varieties over $\mathbb{C}$ to the category of complex tori admitting a Riemann form.*

PROOF. (SKETCH; SEE MUMFORD 1970, I 3, FOR THE DETAILS.) Clearly $A(\mathbb{C})$ is a complex Lie group, which is compact and connected because A is complete and connected. Therefore it is a complex torus (2.1).

For abelian varieties A, B, the map $\mathrm{Hom}(A, B) \to \mathrm{Hom}(A(\mathbb{C}), B(\mathbb{C}))$ is obviously injective, and it is surjective by Chow's theorem[1]. It remains to show that the essential image of the functor consists of the complex tori admitting a Riemann form.

Let $M \simeq V/\Lambda$ be a complex torus (and its canonical uniformization). We have to show that there exists an ample[2] invertible sheaf $\mathcal{L}$ on M if and only if there exists Riemann form. Recall that the isomorphism classes of invertible sheaves on a manifold (or variety) X are classified by $H^1(X, \mathcal{O}_X^\times)$, and that the first chern class of an invertible sheaf is the image of its cohomology class under the boundary map

$$H^1(X, \mathcal{O}_X^\times) \to H^1(X, \mathbb{Z})$$

[1] Recall that the smooth case of Chow's theorem says that every projective complex manifold has a unique structure of a nonsingular projective algebraic variety, and every holomorphic map of projective complex manifolds is regular for these structures (Shafarevich 1994, VIII 3.1).

[2] Recall that this means that, for some $n > 0$, the sections of $\mathcal{L}^{\otimes n}$ give an embedding of M as a closed complex submanifold (hence, subvariety) of projective space.

defined by the exponential sequence

$$0 \to \mathbb{Z} \to \mathcal{O}_X \xrightarrow{e^{2\pi i(\cdot)}} \mathcal{O}_X^\times \to 0.$$

Let ψ be an alternating $\mathbb{Z}$-bilinear form $\Lambda \times \Lambda \to \mathbb{Z}$ such that

$$\psi(Ju, Jv) = \psi(u, v), \quad u, v \in V,$$

and let

$$(u|v) = \psi(u, Jv) - i\psi(u, v)$$

be the corresponding hermitian form on V (so ψ is a Riemann form if and only if $(\cdot|\cdot)$ is positive definite). One can show that there exists a map

$$\alpha\colon \Lambda \to \mathbb{C}^\times, \quad |\alpha(z)| = 1,$$

such that

$$\alpha(u+v) = e^{i\pi\cdot(u|v)} \cdot \alpha(u) \cdot \alpha(v), \quad \text{all } u, v \in \Lambda, \tag{43}$$

and for any such α,

$$u \mapsto e_u, \quad e_u(z) = \alpha(u) \cdot e^{\pi(z|u) + \frac{1}{2}\pi(u|u)},$$

is a one-cocycle on V with coefficients in $\mathcal{O}_V^\times$ whose image under the boundary map

$$H^1(A, \mathcal{O}_V^\times) \to H^2(A, \mathbb{Z}) \simeq \left(\bigwedge^2 H_1(A, \mathbb{Z})\right)^\vee$$

is ψ. Let $\mathcal{L}(\psi, \alpha)$ be the invertible sheaf defined by this cocycle. The following hold.

> Theorem of Appell-Humbert: Every invertible sheaf on A is isomorphic to $\mathcal{L}(\psi, \alpha)$ for a uniquely determined pair (ψ, α).
>
> Theorem of Lefschetz: If $(\ |\ )$ is positive definite, then the space of holomorphic sections of $\mathcal{L}(\psi, \alpha)^{\otimes n}$ gives an embedding of M as a closed complex submanifold of projective space for each $n \geq 3$; conversely, if $\mathcal{L}(\psi, \alpha)^{\otimes n}$ gives such an embedding for some $n > 0$, then $(\ |\ )$ is positive definite.

Thus, M admits an ample invertible sheaf if and only if it admits a Riemann form. □

REMARK 6.2 Let A be an abelian variety with complex multiplication by E over an algebraically closed field k of characteristic zero.[3] Then $\mathrm{Tgt}_0(A) \simeq \bigoplus_{\varphi \in \Phi} k_\varphi$ (as an $E \otimes_{\mathbb{Q}} k$-module) where $\Phi \subset \mathrm{Hom}(E, k)$ and k_φ is a one-dimensional k-vector space on which E acts through φ. It follows from (18) that $\mathrm{Hom}(E, k) = \Phi \sqcup \iota\Phi$ for *every* complex conjugation ι on k. In particular, this applies with $k = \mathbb{C}$: a complex abelian variety A with complex multiplication by E defines a subset $\Phi \subset \mathrm{Hom}(E, \mathbb{C})$ such that $\mathrm{Hom}(E, \mathbb{C}) = \Phi \sqcup \sigma\iota\sigma^{-1}\Phi$ for all automorphisms σ of $\mathbb{C}$.

EXERCISE 6.3 Let E be a number field, and let Φ be a subset of $\mathrm{Hom}(E, \mathbb{C})$. Show that the following conditions on (E, Φ) are equivalent:

[3] Recall that this means that E is a $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(A)$ of degree $2\dim A$ (not necessarily a CM-algebra).

(a) there exists an abelian variety A over $\mathbb{C}$ with complex multiplication by E such that $\mathrm{Tgt}_0(A) \simeq \bigoplus_{\varphi\in\Phi} \mathbb{C}_\varphi$ (as an $E \otimes_{\mathbb{Q}} \mathbb{C}$-module);
(b) $\mathrm{Hom}(E,\mathbb{C}) = \Phi \sqcup \sigma\iota\sigma^{-1}\Phi$ for all automorphisms σ of $\mathbb{C}$;
(c) there exists a CM-subfield E_0 of E and a CM-type Φ_0 on E_0 such that $\Phi = \{\varphi \mid \varphi|E_0 \in \Phi_0\}$;
(d) $|\Phi| = [E:\mathbb{Q}]/2$ and there exists a CM-subfield E_0 of E such that no two of the φ in Φ are complex conjugates on E_0.

(Cf. Shimura and Taniyama 1961, 5.2, Theorem 1.)

Specialization of abelian varieties

Let $k \subset K$ be algebraically closed fields, and let X be a smooth complete variety over K. A variety X_0 over k is called a ***specialization*** of X if there exists a commutative diagram with cartesian squares

$$\begin{array}{ccccc} X & \longrightarrow & \mathcal{X} & \longleftarrow & X_0 \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}\, K & \longrightarrow & \mathrm{Spec}\, R & \longleftarrow & \mathrm{Spec}\, k \end{array} \tag{44}$$

in which

- R is a normal finitely generated k-subalgebra of K and
- $\mathcal{X}$ is flat of finite type over R and X_0 is a smooth complete variety over k (equivalently, $\mathcal{X}$ is a smooth proper R-scheme (Hartshorne 1977, III 10.2, ...).

Every X has a specialization to k: since the polynomials defining X have only finitely many coefficients, X has a model over a subfield L of K that is finitely generated over k; this model extends to a smooth proper model over Spec R for some normal finitely generated k-algebra R with field of fractions L; according to the Hilbert Nullstellensatz, there is a k-algebra homomorphism $R \to k$, and we can take X_0 to be the base change of $\mathcal{X}$.

In the diagram (44), let $p \in \mathcal{X}(R)$ and let p and p_0 be its images in $X(K)$ and $X_0(k)$. Then $\mathrm{Tgt}_p(\mathcal{X})$ is a free R-module of rank $\dim X$, and the maps in (44) induce isomorphisms

$$\mathrm{Tgt}_p(X) \xleftarrow{\simeq} \mathrm{Tgt}_p(\mathcal{X}) \otimes_R K, \quad \mathrm{Tgt}_p(\mathcal{X}) \otimes_R k \xrightarrow{\simeq} \mathrm{Tgt}_{p_0}(X_0) \tag{45}$$

[Add explanation that tangent spaces commute with base change, at least for smooth maps.]

The good reduction of abelian varieties

In this section, I review in as elementary fashion as possible, the theory of the good reduction of abelian varieties. Since most results have been incorporated into the theory of Néron models, those familiar with that theory[4] can skip the explanations.

Let R be a discrete valuation ring with field of fractions K and residue field k. We say that an abelian variety over K has ***good reduction*** if it is the generic fibre of an abelian scheme[5] $\mathcal{A}$ over R; then $A_0 \overset{\text{def}}{=} \mathcal{A} \otimes_R k$ is an abelian variety over k.We assume K has characteristic zero and that k is perfect (although, this is not really necessary).

[4]By which I mean those who have read the proofs in either Néron 1964 or Bosch et al. 1990. Note that, except for (6.12), the present results are used in Néron's theory, and so to deduce them from the main statements of that theory would be circular.

[5]An ***abelian scheme over a scheme*** S is a smooth proper scheme over S together with a group structure.

PROPOSITION 6.4 *Let $\mathcal{A}$ be an abelian scheme over R with generic fibre A. For any smooth R-scheme X, every morphism $X_K \to A$ extends uniquely to a morphism $X \to \mathcal{A}$, i.e., $\mathcal{A}$ represents the functor on smooth R-schemes $X \mapsto A(X_K)$.*

PROOF. This follows from the next lemma and the following consequence of the valuative criterion of properness (Hartshorne 1977, II 4.7):[6]

> Let $Y \to S$ be a proper map, and let $X \to S$ be a smooth map; every S-morphism $X \smallsetminus Z \to Y$ with Z of pure codimension one in X extends uniquely to an S-morphism $X \to Y$.

LEMMA 6.5 *Let $S = \operatorname{Spec} R$, with R a discrete valuation ring, and let G be a smooth group scheme over S. For any smooth scheme X over S and rational map $f\colon X \to G$, the set of points where f is not defined has pure codimension one in X.*

PROOF. Note that the set where f is defined will be open in each fibre of X/S. Define F to be the rational map $X \times X \to G$, $(x, y) \mapsto f(x)f(y)^{-1}$. If f is defined at $x \in X$ (meaning in an open neighbourhood of x), then F is defined at $(x, x) \in X \times X$, and $F(x, x) = e$. Conversely, if F is defined at (x, x), then it will be defined on (x, U) for some open set U. After possibly replacing U a smaller open set, f will be defined on U, and so the formula $f(x) = F(x, u)f(u)$, $u \in U$ shows that f is defined at x. Thus f is defined at x if and only if F is defined at (x, x).

The rational map F defines a map $\mathcal{O}_{G,e} \xrightarrow{\varphi} k(X \times X)$. Since F sends (x, x) to e (if defined at (x, x)), we see that F is defined at (x, x) if and only if $\operatorname{Im}(\varphi) \subset \mathcal{O}_{X\times X,(x,x)}$.

Now $X \times X$ is smooth over S, and hence is normal. Thus the divisor of an element of $k(X \times X)^\times$ is defined, and we have that

$$\mathcal{O}_{X\times X,p} = \{f \in k(X \times X)^\times \mid f \text{ does not have a pole at } p\}. \qquad \square$$

COROLLARY 6.6 *Let A and B be abelian varieties over K, and let $\mathcal{A}$ and $\mathcal{B}$ be abelian schemes over R with generic fibres A and B respectively. The restriction map*

$$\operatorname{Hom}_R(\mathcal{A}, \mathcal{B}) \to \operatorname{Hom}_K(A, B)$$

is a bijection. In particular, $\mathcal{B}$ (if it exists) is unique up to a unique isomorphism.

PROOF. The proposition shows that the restriction map $\operatorname{Mor}_R(\mathcal{A}, \mathcal{B}) \to \operatorname{Mor}_K(A, B)$ is bijective, and it is easy to see that homomorphisms correspond to homomorphisms. $\square$

PROPOSITION 6.7 *Let $\lambda\colon A \to A^\vee$ be a polarization on A; then the extension $\mathcal{A} \to \mathcal{A}^\vee$ of λ is a polarization on $\mathcal{A}$ (and hence reduces to a polarization on $\mathcal{A}_0$).*

PROOF. See Artin 1986, 4.4, and Chai and Faltings 1990. $\square$

[6] Add a proof of the deduction in this footnote.

An elliptic curve has good reduction at a prime ideal $\mathfrak{p}$ of R if and only if it can be defined by a homogeneous polynomial $F(X_0, X_1, X_2)$ with coefficients in R which, when read modulo $\mathfrak{p}$, defines an elliptic curve over $R/\mathfrak{p}$ (cf. Silverman 1986, VII; Silverman 1994, IV 5.3). In particular, this means that, when it has good reduction, the elliptic curve extends to a smooth closed subscheme of $\mathbb{P}^2_R$. We now prove a similar result for abelian varieties.

Recall (Mumford 1999, II §8, p127) that the ***specialization map*** $\rho\colon \mathbb{P}^n(K^{\mathrm{al}}) \to \mathbb{P}^n(k^{\mathrm{al}})$ is defined as follows: represent $P \in \mathbb{P}^n(K^{\mathrm{al}})$ by $(a_0\colon \ldots \colon a_n)$ where each $a_i \in R^{\mathrm{al}}$ and not all a_i lie in $\mathfrak{m}^{\mathrm{al}}$; then $\rho(P)$ is represented by $(\overline{a}_0\colon \ldots \colon \overline{a}_n)$.

LEMMA 6.8 *For any closed subvariety X of $\mathbb{P}^n_K$, the Zariski closure $\mathcal{X}$ of X in $\mathbb{P}^n_R$ has the property that*

$$\mathcal{X} \cap \mathbb{P}^n_K = X \quad \textit{(intersection inside } \mathbb{P}^n_R\textit{)},$$

and $\mathcal{X}$ is the unique flat subscheme of $\mathbb{P}^n_R$ with this property; moreover,

$$\rho(X(K^{\mathrm{al}})) = \mathcal{X}(k^{\mathrm{al}}).$$

PROOF. Let $\mathfrak{a}$ be the homomogeneous ideal in $K[X_0, \ldots, X_n]$ of polynomials zero on X, and let

$$\mathfrak{a}' = \mathfrak{a} \cap R[X_0, \ldots, X_n].$$

Then

$$\mathcal{X} = \operatorname{Proj} R[X_0, \ldots, X_n]/\mathfrak{a}'$$

with its natural inclusion into $\mathbb{P}^n_R$ and map $X \to \mathcal{X}$ has the required properties (Mumford 1999, II §8, Proposition 2). □

PROPOSITION 6.9 *Let A be an abelian variety over K with good reduction. For a suitable choice of a closed immersion $A \hookrightarrow \mathbb{P}^n_K$, the closure $\mathcal{A}$ of A in $\mathbb{P}^n_R$ is an abelian scheme.*

PROOF. Let $\mathcal{A}$ be an abelian scheme over R whose general fibre is A. According to 6.7, there is a divisor D on A whose Zariski closure $\overline{D}$ on $\mathcal{A}$ is ample. Let $\mathcal{A} \hookrightarrow \mathbb{P}^n_R$ be the closed immersion defined by $\overline{D}$, and let $A \hookrightarrow \mathbb{P}^n_K$ be its generic fibre. Then the closure of A in $\mathbb{P}^n_R$ is $\mathcal{A}$. □

PROPOSITION 6.10 *Let A be an abelian variety over K with good reduction. If $\mathcal{O}_K$ is henselian (for example, if K is complete), then for any m prime to the characteristic of k, the specialization map defines an isomorphism $A(K)_m \to A(k)_m$.*

PROOF. Let $\mathbb{Z}/m\mathbb{Z}$ denote the constant group scheme over R (disjoint union of copies of Spec R indexed by $\{0, \ldots, m-1\}$). Then

$$\mathcal{A}(R)_m \simeq \operatorname{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathcal{A}) \overset{(6.5)}{\simeq} \operatorname{Hom}(\mathbb{Z}/m\mathbb{Z}, A) \simeq \mathcal{A}(K)_m.$$

The map $m\colon \mathcal{A} \to \mathcal{A}$ is étale (e.g., Milne 1986, 20.7). Using this and Hensel's lemma, one shows that the kernel of $\mathcal{A}(R) \to A(k)$ is uniquely divisible by m, and so $\mathcal{A}(R)_m \to \mathcal{A}(k)_m$ is a bijection. □

Extend the valuation on K to an algebraic closure $\overline{K}$ of K, and let $I \subset D \subset \operatorname{Gal}(\overline{K}/K)$ be the inertia and decomposition groups. Then $D/I \simeq \operatorname{Gal}(k^{\mathrm{al}}/k)$, and the ring of integers of $\overline{K}^I$ is henselian (if $\mathcal{O}_K$ is henselian, then $\overline{K}^I$ is a maximal unramified extension K^{un} of K).

COROLLARY 6.11 *With the above notations, $A(\overline{K}^I)_m = A(K^{\mathrm{al}})_m$ for all m prime to the characteristic of k.*

PROOF. The group $A(\overline{K}^I)_m \simeq A(k^{\mathrm{al}})_m$ has $m^{2\dim A}$ elements. □

Hence, when A has good reduction, the representation ρ_ℓ of $\mathrm{Gal}(K^{\mathrm{al}}/K)$ on $T_\ell A$ is ***unramified*** (i.e., trivial on the inertia subgroup I) for ℓ different from the characteristic of k.

THEOREM 6.12 (NÉRON CRITERION) *If $T_\ell A$ is unramified for some ℓ different from the characteristic of k, then A has good reduction.*

PROOF. For elliptic curves, this was known to Ogg and Shafarevich. As Serre observed, for abelian varieties it follows fairly directly from the existence of Néron models (Serre and Tate 1968, Theorem 1). Recall that a smooth group scheme $\mathcal{A}$ over R with generic fibre A is a ***Néron model*** for A if it represents the functor on smooth R-schemes $X \mapsto A(X_K)$. Such a model always exists (Néron 1964, Artin 1986, or Bosch et al. 1990); it is obviously unique (up to a unique isomorphism). When A has good reduction, and so extends to an abelian scheme $\mathcal{A}$ over R, Proposition 6.4 shows that $\mathcal{A}$ is a Néron model for A; conversely, when the Néron model is proper, it is an abelian scheme and so A has good reduction.

Let $\mathcal{A}$ be the Néron model for A, and let A_0 be its special fibre. For m distinct from the characteristic of k, the reduction map defines an isomorphism

$$A(K^{\mathrm{al}})^I_m \simeq A(k^{\mathrm{al}})_m$$

(see 6.10). Thus, if I acts trivially on $T_\ell A$, then

$$A(k^{\mathrm{al}})_{\ell^n} \simeq A(K^{\mathrm{al}})_{\ell^n} \approx (\mathbb{Z}/\ell^n\mathbb{Z})^{2\dim A}, \quad \text{all } n. \tag{46}$$

Every commutative algebraic group, for example, A_0, has a composition series whose quotients are a finite group F, a unipotent group U, a torus T, and an abelian variety B. Now $F(k^{\mathrm{al}})(\ell)$ is finite, $U(k^{\mathrm{al}})(\ell) = 0$, and $T(k^{\mathrm{al}})(\ell) \approx (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\dim T}$. Thus (46) can hold only if A_0 is an abelian variety, in which case $\mathcal{A}$ is proper. □

An abelian variety over K is said to have ***potential good reduction*** if it acquires good reduction over a finite extension of K. According to (6.11) and (6.12), a necessary and sufficient condition for this is that the image of the inertia group under ρ_ℓ is finite.

COROLLARY 6.13 *Suppose that the k is finite and that for some $\ell \neq p = \mathrm{char}\, k$, the image of ρ_ℓ is commutative. Then A has potential good reduction.*

PROOF. We may assume that K is a complete local field. Because the image of ρ_ℓ is commutative, local class field theory (CFT I 1.1) shows that the image I of the inertia group in $\mathrm{Aut}(T_\ell A)$ is a quotient of $\mathcal{O}_K^\times$. But $1 + p\mathcal{O}_K$ is a pro-p-group of finite index in $\mathcal{O}_K^\times$, and so I has a pro-p-subgroup P of finite index. On the other hand, $1 + \ell \cdot \mathrm{End}(T_\ell A)$ is a pro-ℓ-subgroup of $\mathrm{Aut}(T_\ell A)$ of finite index. As $\ell \neq p$, the subgroups P and $1 + \ell \cdot \mathrm{End}(T_\ell A)$ intersect trivially, and so P maps injectively into the finite group $\mathrm{Aut}(T_\ell A/\ell T_\ell A)$. It follows that I is finite. □

COROLLARY 6.14 *An abelian variety has good reduction if it is isogenous to an abelian variety with good reduction.*

PROOF. Suppose A is isogenous to an abelian variety B with good reduction. Then there exists an isogeny $A \to B$, and any such isogeny defines an injective map $T_\ell A \to T_\ell B$. As $T_\ell B$ is unramified, so also is $T_\ell A$. □

7 Abelian varieties with complex multiplication

Definition of a CM abelian variety

Let A be an abelian variety over a field k. If k can be embedded in $\mathbb{C}$, then $\mathrm{End}^0(A)$ acts faithfully on $H_1(A(\mathbb{C}),\mathbb{Q})$, which has dimension $2\dim A$, and so (see 1.2),

$$[\mathrm{End}^0(A)\colon\mathbb{Q}]_{\mathrm{red}} \le 2\dim A. \tag{47}$$

In general, for $\ell \neq \mathrm{char}\, k$, $\mathrm{End}^0(A)\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ acts faithfully on $V_\ell A$ (e.g., Milne 1986, 12.5), which again implies (47). When equality holds in (47), we say that A has ***complex multiplication over*** k (or be an abelian variety of ***CM-type over*** k, or be a ***CM abelian variety over*** k).

REMARK 7.1 Although we are interested here only in the case that k has characteristic zero, this definition makes sense also in characteristic p. A theorem of Tate shows that every abelian variety over a finite field k has complex multiplication over k (Tate 1966), and a theorem of Grothendieck shows that every abelian variety with complex multiplication over an algebraically closed field k of characteristic p is isogenous to an abelian variety defined over a finite field (Oort 1973, Yu 2004).

EXERCISE 7.2 Let ℓ be a prime different from $\mathrm{char}\, k$. Show that A has complex multiplication over k if and only if the centralizer of $\mathrm{End}^0(A)$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)$ is commutative, in which case it equals $C(A)\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ where $C(A)$ is the centre of $\mathrm{End}^0(A)$.

Complex multiplication by a $\mathbb{Q}$-algebra

Let A be an abelian variety over a field k, and let E be an étale $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(A)$. Recall that

$$[E\colon\mathbb{Q}] \overset{(1.3)}{\le} [\mathrm{End}^0(A)\colon\mathbb{Q}]_{\mathrm{red}} \overset{(47)}{\le} 2\dim A.$$

Equalities hold throughout if and only if A has complex multiplication and E is maximal, in which case we say that A has ***complex multiplication by*** E ***over*** k.[7] More generally, we say that (A,i) is an ***abelian variety with complex multiplication by*** E ***over*** k if i is an injective homomorphism from a $\mathbb{Q}$-algebra E of degree $2\dim A$ into $\mathrm{End}^0(A)$.[8]

Let A have complex multiplication by E over k, and let

$$R = \mathcal{O}^A = E\cap\mathrm{End}(A).$$

Then R is an ***order*** in E, i.e., it is simultaneously a subring and a lattice in E. It is a subring of $\mathcal{O}_E$ with integral closure $\mathcal{O}_E$. The ring R doesn't change under base field extension, i.e., for any field $k'\supset k$,

$$R = E\cap\mathrm{End}(A_{k'}).$$

To see this, note that, because E/R is torsion, it suffices to show that $\mathrm{End}(A_{k'})/\mathrm{End}(A)$ is torsion free. But if α is an endomorphism of A that becomes divisible by m over k', then it

[7] Shimura frequently complicates things by defining a number field to be a subfield of $\mathbb{C}$. Thus, let A be a simple abelian variety with complex multiplication, and let $E=\mathrm{End}^0(A)$. Where we write "A has complex multiplication by E", Shimura chooses an isomorphism $i\colon E\xrightarrow{\approx} E'\subset\mathbb{C}$ of E with a subfield E' of $\mathbb{C}$, and writes "(A,i^{-1}) has complex multiplication by E'".

[8] In particular, this means that $i(1)=\mathrm{id}_A$.

is divisible by m over k (because, to say that α is divisible by m in $\mathrm{End}(A)$ means that it is zero on A_m, as multiplication by m defines an isomorphism $A/A_m \to A$; cf. Milne 1986, 12.6).

Let $g = \dim A$, and let ℓ be a prime not equal to $\mathrm{char}\, k$. Then $T_\ell A$ is a $\mathbb{Z}_\ell$-module of rank $2g$ and $V_\ell A$ is a $\mathbb{Q}_\ell$-vector space of dimension $2g$. The action of R on $T_\ell A$ extends to actions of $R_\ell \stackrel{\text{def}}{=} R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ on $T_\ell A$ and of $E_\ell \stackrel{\text{def}}{=} \mathbb{Q}_\ell \otimes_{\mathbb{Q}} E$ on $V_\ell A$.

PROPOSITION 7.3 *(a) The E_ℓ-module $V_\ell A$ is free of rank* 1.

(b) We have

$$R_\ell = E_\ell \cap \mathrm{End}(T_\ell A).$$

PROOF. (a) We have already noted that E_ℓ acts faithfully on $V_\ell A$, and this implies that $V_\ell A$ is free of rank 1 (see 1.2).

(b) Let α be an element of E_ℓ such that $\alpha(T_\ell A) \subset T_\ell A$. For some m, $\ell^m \alpha \in R_\ell$, and if $\beta \in R$ is chosen to be very close ℓ-adically to $\ell^m \alpha$, then $\beta T_\ell A \subset \ell^m T_\ell A$, which means that β vanishes on A_{ℓ^m}. Hence $\beta = \ell^m \alpha_0$ for some $\alpha_0 \in \mathrm{End}(A) \cap E = R$. Now α and α_0 are close in E_ℓ; in particular, we may suppose $\alpha - \alpha_0 \in R_\ell$, and so $\alpha \in R_\ell$. □

COROLLARY 7.4 *The commutants of R in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)$, $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell A)$, $\mathrm{End}^0(A)$, and $\mathrm{End}(A)$ are, respectively, E_ℓ, R_ℓ, F, and R.*

PROOF. Any endomorphism of $V_\ell A$ commuting with R commutes with E_ℓ, and therefore lies in E_ℓ, because of (7.3a).

Any endomorphism of $T_\ell A$ commuting with R extends to an endomorphism of $V_\ell A$ preserving $T_\ell A$ and commuting with R, and so lies in $E_\ell \cap \mathrm{End}(T_\ell A) = R_\ell$.

Let C be the commutant of E in $\mathrm{End}^0(A)$. Then E is a subalgebra of C, so $[E\colon \mathbb{Q}] \leq [C\colon \mathbb{Q}]$, and $C \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is contained in the commutant E_ℓ of E in $\mathrm{End}(V_\ell A)$, so $[E\colon \mathbb{Q}] \geq [C\colon \mathbb{Q}]$. Thus $E = C$.

Finally, the commutant R in $\mathrm{End}(A)$ contains R and is contained in $C \cap \mathrm{End}(A) = E \cap \mathrm{End}(A) = R$. □

COROLLARY 7.5 *Let (A, i) have complex multiplication by E, and let $R = i^{-1}(\mathrm{End}(A))$. Then any endomorphism of A commuting with $i(a)$ for all $a \in R$ is of the form $i(b)$ for some $b \in R$.*

PROOF. Apply the preceding corollary to $i(E) \subset \mathrm{End}^0(A)$. □

REMARK 7.6 If ℓ does not divide $(\mathcal{O}_E\colon R)$, then R_ℓ is a product of discrete valuation rings, and $T_\ell A$ is a free R_ℓ-module of rank 1,[9] but in general this need not be true (Serre and Tate 1968, p502). Similarly, $T_m A \stackrel{\text{def}}{=} \prod_{\ell | m} T_\ell A$ is a free $R_m \stackrel{\text{def}}{=} \prod_{\ell | m} R_\ell$-module of rank 1 if m is relatively prime to $(\mathcal{O}_E\colon R)$. [Make this into a lemma + a remark.]

[9] If ℓ doesn't divide $(\mathcal{O}_E\colon R)$, then the exact sequence

$$0 \to R \to \mathcal{O}_E \to \mathcal{O}_E/R \to 0,$$

when tensored with $\mathbb{Z}_\ell$, gives an isomorphism $R_\ell \simeq \mathcal{O}_E \otimes \mathbb{Z}_\ell$, which is a product of discrete valuation rings, say, $\mathcal{O}_E \otimes \mathbb{Z}_\ell \approx \prod R_i$. Let M_i denote R_i regarded as an R_ℓ-module through the projection $R_\ell \to R_i$. Then every projective R_ℓ-module is isomorphic to $\sum m_i M_i$ for some $m_i \geq 0$. In particular, $T_\ell A \approx \sum m_i M_i$; as $T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is free of rank one over $R_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, each $m_i = 1$.

Specialization

Let (A, i) be an abelian variety with complex multiplication by a CM-algebra E over a field k of characteristic zero. If k contains all conjugates of E, then $\mathrm{Tgt}_0(A) \simeq \prod_{\varphi\in\Phi} k_\varphi$ (as an $E \otimes_{\mathbb{Q}} k$-module) where Φ is a set of $\mathbb{Q}$-algebra homomorphisms $E \hookrightarrow k$ and k_φ is a one-dimensional k-vector space on which $a \in E$ acts as $\varphi(a)$ — we say that (A, i) is of ***CM-type*** (E, Φ). For any complex conjugation ι on k,

$$\Phi \sqcup \iota\Phi = \mathrm{Hom}(E, k)$$

(see 3.11; recall that a complex conjugation on k is any involution induced by an inclusion $k \hookrightarrow \mathbb{C}$ and complex conjugation on $\mathbb{C}$). If $k \subset K$, then a CM-type on E with values in k can be regarded as a CM-type on E with values in K.

PROPOSITION 7.7 *Every specialization of a pair (A, i) of CM-type (E, Φ) is of CM-type (E, Φ).*

PROOF. Obvious from the relation (45) between the tangent spaces. (Cf. Shimura and Taniyama 1961, 12.4, Proposition 26, p109). □

Rigidity

LEMMA 7.8 *For any abelian variety A over an algebraically closed field, the torsion points on A are Zariski dense in A.*

PROOF. Let B be the Zariski closure of the set of torsion points in A. Then B is a complete algebraic subgroup of A, and so its identity component B° is an abelian subvariety of A. For any prime not dividing the index of B° in B and distinct from the characteristic of k, B° has $\ell^{2\dim A}$ points of order ℓ, which shows that $\dim B^\circ = \dim A$. Hence $B^\circ = A$ □

PROPOSITION 7.9 *Let k be an algebraically closed subfield of $\mathbb{C}$. The functor $A \mapsto A_{\mathbb{C}}$ from abelian varieties over k to abelian varieties over $\mathbb{C}$ is fully faithful, and its essential image contains all abelian varieties with complex multiplication.*

PROOF. We shall make repeated use of the obvious fact that the inclusion $A(k) \hookrightarrow A(\mathbb{C})$ induces an isomorphism on the torsion points (because each group has $n^{2\dim A}$ points of order dividing n).

FAITHFUL: Let $f, g\colon A \to A'$ be homomorphisms of abelian varieties over k. If $f_{\mathbb{C}} = g_{\mathbb{C}}$, then f and g agree on $A(\mathbb{C})_{\mathrm{tors}} = A(k)_{\mathrm{tors}}$, and so $f = g$ by (7.8).

FULL: Let A and A' be abelian varieties over k, and let $f\colon A_{\mathbb{C}} \to A'_{\mathbb{C}}$ be a homomorphism. For any automorphism τ of $\mathbb{C}$ fixing k, τf and f agree on $A(\mathbb{C})_{\mathrm{tors}} = A(k)_{\mathrm{tors}}$, and therefore on $A_{\mathbb{C}}$. This implies that f is defined over k (AG 16.9).

ESSENTIAL IMAGE: Let A be a simple CM abelian variety over $\mathbb{C}$, of CM-type (E, Φ) say. Then any specialization A' of A to k is again of CM-type (E, Φ) (see 7.7) and so $A'_{\mathbb{C}}$ is isogenous to A (see 3.13).

Now consider an arbitrary CM abelian variety A over $\mathbb{C}$. It follows from the last paragraph that there exists an abelian variety A' over k and an isogeny $f\colon A'_{\mathbb{C}} \to A$. The kernel of f is a finite subgroup N of $A'(\mathbb{C})_{\mathrm{tors}} = A'(k)_{\mathrm{tors}}$. Let $A'' = A'/N$. Then f defines an isomorphism $A''_{\mathbb{C}} \to A$. □

COROLLARY 7.10 *The functor $A \mapsto A_{\mathbb{C}}$ defines an equivalence from the category of CM abelian varieties over k to the category of CM abelian varieties over $\mathbb{C}$.*

PROOF. Clearly A has complex multiplication if and only if $A_{\mathbb{C}}$ has complex multiplication, and so this follows from the proposition. □

In particular, an abelian variety with complex multiplication over $\mathbb{C}$ has a model over any algebraically closed subfield of $\mathbb{C}$ which is unique up to a unique isomorphism.

PROPOSITION 7.11 *Let A be an abelian variety over $k \subset \mathbb{C}$ with complex multiplication over k^{al}. If A has complex multiplication over k, then k contains the reflex field of A; conversely, if k contains the reflex field and A is simple, then A has complex multiplication over k.*

PROOF. If A has complex multiplication over k, then it has complex multiplication by a CM-algebra E over k. Write $\mathrm{Tgt}_0(A_{\mathbb{C}}) \simeq \prod_{\varphi\in\Phi} \mathbb{C}_\varphi$, where Φ is a CM-type on E and $\mathbb{C}_\varphi$ is a one-dimensional $\mathbb{C}$-vector space on which E acts through φ. Then $\mathrm{Tgt}_0(A)$ is an $E \otimes_{\mathbb{Q}} k$-module such that $\mathrm{Tgt}_0(A) \otimes_k \mathbb{C} \simeq \mathrm{Tgt}_0(A_{\mathbb{C}})$, and so the action of E on $\mathrm{Tgt}_0(A)$ satisfies the condition (5) of Proposition 1.21, which implies that $k \supset E^*$.

Now assume that A is simple. Let $E = \mathrm{End}^0(A_{\overline{k}})$, and let $\mathrm{Tgt}_0(\overline{k}) \simeq \bigoplus_{\varphi\in\Phi} \overline{k}_\varphi$ (usual notation) with $\overline{k}$ the algebraic closure of k in $\mathbb{C}$ and $\Phi \subset \mathrm{Hom}(E, \overline{k})$. Because A is simple, (E, Φ) is primitive (3.13). The group $\mathrm{Gal}(\overline{k}/k)$ acts on E, and we have to show that this action is trivial if $k \supset E^*$. Let $\sigma \in \mathrm{Gal}(\overline{k}/k)$ act on E as σ'. One checks that $\sigma\Phi = \Phi\sigma'$. If $k \supset E^*$, then $\sigma\Phi = \Phi$ (see 1.17), and so $\Phi\sigma' = \Phi$. For any extension σ'' of σ' to a CM-field E_1 containing E and Galois over $\mathbb{Q}$, this implies that σ'' fixes E by (1.10). □

Good reduction

PROPOSITION 7.12 *Let A be an abelian variety over a number field k with complex multiplication. Then A has potential good reduction at all finite primes of k.*

PROOF. After possibly extending k, we may suppose that A has complex multiplication by E over k. Let $R \stackrel{\mathrm{def}}{=} E \cap \mathrm{End}(A)$ and let $\rho_\ell\colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/k) \to \mathrm{Aut}(T_\ell A)$ be the ℓ-adic representation defined by A for some prime ℓ. Because the elements of R are defined over k, they commute with the action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/k)$. Therefore the image of ρ_ℓ is contained in the centralizer of R in $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell A)$, which is $R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ (see 7.4). In particular, it is commutative, and this shows that A has potential good reduction at all primes of k not dividing ℓ (apply 6.13). □

The degrees of isogenies

An isogeny $\alpha\colon A \to B$ defines a homomorphism $\alpha^*\colon k(B) \to k(A)$, and the ***degree*** of α is defined to be $[k(A)\colon \alpha^* k(B)]$.

PROPOSITION 7.13 *Let A be an abelian variety with complex multiplication by E, and let $R = \mathrm{End}(A) \cap E$. An element α of R that is not a zero-divisor is an isogeny of degree $(R\colon \alpha R)$.*

PROOF. If α is not a zero-divisor, then it is invertible in $E \simeq R \otimes_{\mathbb{Z}} \mathbb{Q}$, and so it is an isogeny. Let d be its degree, and choose a prime ℓ not dividing $d \cdot \text{char}(k)$. Then d is the determinant of α acting on $V_\ell A$ (e.g., Milne 1986, 12.9). As $V_\ell A$ is free of rank 1 over $E_\ell \stackrel{\text{def}}{=} E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, this determinant is equal to $\text{Nm}_{E_\ell/\mathbb{Q}_\ell}(\alpha)$, which equals $\text{Nm}_{E/\mathbb{Q}}(\alpha)$. But R is a lattice in E, and so this norm equals $(R\colon \alpha R)$.[10] □

PROPOSITION 7.14 (SHIMURA AND TANIYAMA 1961, I 2.8, THM 1) *Let k be an algebraically closed field of characteristic $p > 0$, and let $\alpha\colon A \to B$ be an isogeny of abelian varieties over k. Assume that $\alpha^*(k(B)) \supset k(A)^q$ for some power $q = p^m$ of p, and let d be the dimension of the kernel of $\text{Tgt}_0(\alpha)\colon \text{Tgt}_0(A) \to \text{Tgt}_0(B)$; then*

$$\deg(\alpha) \le q^d.$$

We offer two proofs, according to the taste and knowledge of the reader.

PROOF OF (7.14) IN TERMS OF VARIETIES AND DIFFERENTIALS

LEMMA 7.15 *Let L/K be a finitely generated extension of fields of characterstic $p > 0$ such that $K \supset L^q$ for some power q of p. Then*

$$[L\colon K] \le q^{\dim \Omega^1_{L/K}}.$$

PROOF. Let $x_1, \dots, x_n$ be a minimal set of generators for L over K. Because $x_i^q \in K$, $[L\colon K] < q^n$, and it remains to prove $\dim \Omega^1_{L/K} \ge n$. For each i, the extension

$$L/K(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$$

is nontrivial and purely inseparable because $L \supset K \supset L^q$. There therefore exists a K-derivation of D_i of L such that $D_i(x_i) \ne 0$ but $D_i(x_j) = 0$ for $j \ne i$, namely, $\frac{\partial}{\partial x_i}$. The D_i are linearly independent, from which the conclusion follows. □

PROOF (OF 7.14) In the lemma, take $L = k(A)$ and $K = \alpha^*(k(B))$. Then $\deg(\alpha) = [L\colon K]$ and $\dim \Omega^1_{L/K} = \dim \text{Ker}(\text{Tgt}_0(\alpha))$, and so the proposition follows. □

PROOF OF (7.14) IN TERMS OF FINITE GROUP SCHEMES

The ***order*** of a finite group scheme $N = \text{Spec } R$ over a field k is $\dim_k R$.

LEMMA 7.16 *The kernel of an isogeny of abelian varieties is a finite group scheme of order equal to the degree of the isogeny.*

PROOF. Let $\alpha\colon A \to B$ be an isogeny. Then (e.g., Milne 1986, 8.1) $\alpha_* \mathcal{O}_A$ is a locally free $\mathcal{O}_B$-module, of rank r say. The fibre of $\alpha_* \mathcal{O}_A$ at 0_B is the affine ring of $\text{Ker}(\alpha)$, which therefore is finite of order r. The fibre of $\alpha_* \mathcal{O}_A$ at the generic point of B is $k(A)$, and so $r = [k(A)\colon \alpha^* k(B)] = \deg(\alpha)$. □

[10] In more detail: let $e_1, \dots, e_n$ be a basis for R as a $\mathbb{Z}$-module, and let $\alpha e_j = \sum_i a_{ij} e_i$. For some $\varepsilon \in V_\ell A$, $e_1\varepsilon, \dots, e_n\varepsilon$ is a $\mathbb{Q}_\ell$-basis for $V_\ell A$. As $\alpha e_j \varepsilon = \sum_i a_{ij} e_i \varepsilon$, we have that $d = \det(a_{ij})$. But $\left|\det(a_{ij})\right| = (R : \alpha R)$ (standard result, which is obvious, for example, if α is diagonal).

PROOF (OF 7.14) The condition on α implies that $\mathrm{Ker}(\alpha)$ is connected, and therefore its affine ring is of the form $k[T_1,\dots,T_s]/(T_1^{p^{r_1}},\dots,T_s^{p^{r_s}})$ for some family $(r_i)_{1\le i\le s}$ of integers $r_i \ge 1$ (Waterhouse 1979, 14.4). Let $q = p^m$. Then each $r_i \le m$ because $\alpha^*(k(B)) \supset k(A)^q$, and

$$s = \dim_k \mathrm{Tgt}_0(\mathrm{Ker}(\alpha)) = \dim_k \mathrm{Ker}(\mathrm{Tgt}_0(\alpha)) = d.$$

Therefore,

$$\deg(\alpha) = \textstyle\prod_{i=1}^{s} p^{r_i} \le p^{ms} = q^d.$$

□

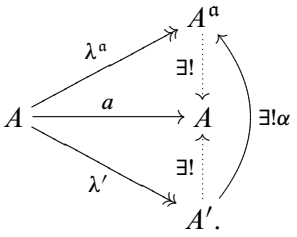
$\mathfrak{a}$-multiplications (1)

Let A be an abelian variety with complex multiplication by E over a field k, and let $R = E \cap \mathrm{End}(A)$. An element of R is an isogeny if and only if it is not a zero-divisor,[11] and an ideal $\mathfrak{a}$ in R contains an isogeny if and only if it is a lattice in E — we call ideals with this property ***lattice ideals***. We wish to attach to each lattice ideal $\mathfrak{a}$ in R an isogeny $\lambda^{\mathfrak{a}}\colon A \to A^{\mathfrak{a}}$ with certain properties. The shortest definition is to take $A^{\mathfrak{a}}$ to be the quotient of A by the finite group scheme

$$\mathrm{Ker}(\mathfrak{a}) = \textstyle\bigcap_{a\in\mathfrak{a}} \mathrm{Ker}(a).$$

However, the formation of quotients by finite group schemes in characteristic p is subtle (Mumford 1970, p109-123)[12], and was certainly not available to Shimura and Taniyama. In this subsection, we give the original elementary definition, and in the next, we give a functorial definition.

DEFINITION 7.17 Let A be an abelian variety with complex multiplication by E over a field k, and let $\mathfrak{a}$ be a lattice ideal in R. A surjective homomorphism $\lambda^{\mathfrak{a}}\colon A \to A^{\mathfrak{a}}$ is an $\mathfrak{a}$-***multiplication*** if every homomorphism $a\colon A \to A$ with $a \in \mathfrak{a}$ factors through $\lambda^{\mathfrak{a}}$, and $\lambda^{\mathfrak{a}}$ is universal for this property, in the sense that, for every surjective homomorphism $\lambda'\colon A \to A'$ with the same property, there is a homomorphism $\alpha\colon A' \to A^{\mathfrak{a}}$, necessarily unique, such that $\alpha \circ \lambda' = \lambda^{\mathfrak{a}}$:



An abelian variety B for which there exists an $\mathfrak{a}$-multiplication $A \to B$ is called an $\mathfrak{a}$-***transform*** of A.

EXAMPLE 7.18 (a) If $\mathfrak{a}$ is principal, say, $\mathfrak{a} = (a)$, then $a\colon A \to A$ is an $\mathfrak{a}$-multiplication (obvious from the definition) — this explains the name "$\mathfrak{a}$-multiplication". More generally, if $\lambda\colon A \to A'$ is an $\mathfrak{a}$-multiplication, then

$$A \xrightarrow{a} A \xrightarrow{\lambda} A'$$

[11] Recall that E is an étale $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(A)$, i.e., a product of fields, say $E = \prod E_i$. Obviously $E = R \otimes_{\mathbb{Z}} \mathbb{Q}$, and $R \subset E$. An element $\alpha = (\alpha_i)$ of R is not zero-divisor if and only if each component α_i of α is nonzero, or, equivalently, α is an invertible element of E.

[12] Compare the proof of (7.20) with that of Mumford 1970, III, Theorem 1, p111.

is an $\mathfrak{a}a$-multiplication for any $a \in E$ such that $\mathfrak{a}a \subset R$ (obvious from the construction in 7.20 below).

(b) Let (E, Φ) be a CM-pair, and let $A = \mathbb{C}^{\Phi}/\Phi(\Lambda)$ for some lattice Λ in E. For any lattice ideal $\mathfrak{a}$ in $R \stackrel{\text{def}}{=} \text{End}(A) \cap E$,

$$\begin{aligned} \text{Ker}(\mathfrak{a}) &= \{z + \Phi(\Lambda) \mid az \in \Phi(\Lambda) \text{ all } a \in \mathfrak{a}\} \\ &\simeq \mathfrak{a}^{-1}/R \end{aligned}$$

where $\mathfrak{a}^{-1} = \{a \in E \mid a\mathfrak{a} \subset R\}$. The quotient map $\mathbb{C}^{\Phi}/\Phi(\Lambda) \to \mathbb{C}^{\Phi}/\Phi(\mathfrak{a}^{-1}\Lambda)$ is an $\mathfrak{a}$-multiplication.

REMARK 7.19 (a) The universal property shows that an $\mathfrak{a}$-multiplication, if it exists, is unique up to a unique isomorphism.

(b) Let $a \in \mathfrak{a}$ be an isogeny; because a factors through $\lambda^{\mathfrak{a}}$, the map $\lambda^{\mathfrak{a}}$ is an isogeny.

(c) The universal property, applied to $\lambda^{\mathfrak{a}} \circ a$ for $a \in R$, shows that, $A^{\mathfrak{a}}$ has complex multiplication by E over k, and $\lambda^{\mathfrak{a}}$ is an E-isogeny. Moreover, $R \subset \text{End}(A^{\mathfrak{a}}) \cap E$, but the inclusion may be strict unless $R = \mathcal{O}_E$.[13]

(d) If $\lambda: A \to B$ is an $\mathfrak{a}$-multiplication, then so also is $\lambda_{k'}: A_{k'} \to B_{k'}$ for any $k' \supset k$. This follows from the construction in (7.20) below.

PROPOSITION 7.20 *An $\mathfrak{a}$-multiplication exists for each lattice ideal $\mathfrak{a}$.*

PROOF. Choose a set of generators $a_1, ..., a_n$ of $\mathfrak{a}$, and define $A^{\mathfrak{a}}$ to be the image of

$$x \mapsto (a_1 x, \ldots): A \to A^n. \tag{48}$$

For any $a = \sum_i r_i a_i \in \mathfrak{a}$, the diagram

$$A \xrightarrow{\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}} A^n \xrightarrow{(r_1, \cdots, r_n)} A, \qquad a: A \to A$$

shows that $a: A \to A$ factors through $\lambda^{\mathfrak{a}}$.

Let $\lambda': A \to A'$ be a quotient map such that each a_i factors through λ', say, $\alpha_i \circ \lambda' = a_i$. Then the composite of

$$A \xrightarrow{\lambda'} A' \xrightarrow{\alpha = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}} A^n \tag{49}$$

is $x \mapsto (a_1 x, \ldots): A \to A^n$, which shows that $\alpha \circ \lambda' = \lambda^{\mathfrak{a}}$. □

REMARK 7.21 A surjective homomorphism $\lambda: A \to B$ is an $\mathfrak{a}$-multiplication if and only if every homomorphism $a: A \to A$ defined by an element of $\mathfrak{a}$ factors through λ and one (hence every) family $(a_i)_{1 \le i \le n}$ of generators for $\mathfrak{a}$ defines an isomorphism of B onto the image of A in A^n. Alternatively, a surjective homomorphism $\lambda: A \to B$ is an $\mathfrak{a}$-multiplication if it maps $k(B)$ isomorphically onto the composite of the fields $a^*k(A)$ for $a \in \mathfrak{a}$ — this is the original definition (Shimura and Taniyama 1961, 7.1).

[13] Over $\mathbb{C}$ (at least), A is E-isogenous to an abelian variety with $\text{End}(A) \cap E = \mathcal{O}_E$ (see 3.9), but every such isogeny is an $\mathfrak{a}$-multiplication for some $\mathfrak{a}$ (see below).

PROPOSITION 7.22 *Let A be an abelian variety with complex multiplication by E over k, and let $\lambda\colon A \to B$ and $\lambda'\colon A \to B'$ be $\mathfrak{a}$ and $\mathfrak{a}'$-multiplications. There exists an E-isogeny $\alpha\colon B \to B'$ such that $\alpha \circ \lambda = \lambda'$ if only if $\mathfrak{a} \supset \mathfrak{a}'$.*

PROOF. If $\mathfrak{a} \supset \mathfrak{a}'$, then $a\colon A \to A$ factors through λ when $a \in \mathfrak{a}'$, and so α exists by the universality of λ'. For the converse, note that there are natural (projection) maps $A^{\mathfrak{a}+\mathfrak{a}'} \to A^{\mathfrak{a}}, A^{\mathfrak{a}'}$. If there exists an E-isogeny α such that $\alpha \circ \lambda^{\mathfrak{a}} = \lambda^{\mathfrak{a}'}$, then $A^{\mathfrak{a}+\mathfrak{a}'} \to A^{\mathfrak{a}}$ is injective, which implies that $\mathfrak{a} + \mathfrak{a}' = \mathfrak{a}$ by (7.27) below.[14] □

COROLLARY 7.23 *Let $\lambda\colon A \to B$ and $\lambda'\colon A \to B'$ be $\mathfrak{a}$ and $\mathfrak{a}'$-multiplications; if there exists an E-isomorphism $\alpha\colon B \to B'$ such that $\alpha \circ \lambda = \lambda'$, then $\mathfrak{a} = \mathfrak{a}'$.*

PROOF. The existence of α implies that $\mathfrak{a} \supset \mathfrak{a}'$, and the existence of its inverse implies that $\mathfrak{a}' \supset \mathfrak{a}$. □

COROLLARY 7.24 *Let $a \in \mathrm{End}(A) \cap E$. If $a\colon A \to A$ factors through an $\mathfrak{a}$-multiplication, then $a \in \mathfrak{a}$.*

PROOF. The map $a\colon A \to A$ is an (a)-multiplication, and so if there exists an E-isogeny α such that $\alpha \circ \lambda^{\mathfrak{a}} = a$, then $\mathfrak{a} \supset (a)$. □

REMARK 7.25 Let $\lambda\colon A \to B$ be an $\mathfrak{a}$-multiplication. Let $a_1, \dots, a_n$ be a basis for $\mathfrak{a}$, and let $a_i = \alpha_i \circ \lambda$. In the diagram

$$A \xrightarrow{\lambda} B \xrightarrow{\alpha} A^n \qquad \alpha = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

(a : $A \to A^n$)

α maps B isomorphically onto the image of a. For any prime ℓ different from the characteristic of k, we get a diagram

$$T_\ell A \xrightarrow{T_\ell\lambda} T_\ell B \xrightarrow{T_\ell\alpha} T_\ell A^n \qquad (T_\ell a : T_\ell A \to T_\ell A^n)$$

in which $T_\ell\alpha$ maps $T_\ell B$ isomorphically onto the image of $T_\ell a$.

PROPOSITION 7.26 *If $\lambda\colon A \to A'$ is an $\mathfrak{a}$-multiplication, and $\lambda'\colon A' \to A''$ is an $\mathfrak{a}'$-multiplication, then $\lambda' \circ \lambda$ is an $\mathfrak{a}'\mathfrak{a}$-multiplication.*

PROOF. Let $\mathfrak{a} = (a_1, ..., a_m)$, and let $\mathfrak{a}' = (a'_1, ..., a'_m)$; then $\mathfrak{a}'\mathfrak{a} = (\dots, a'_i a_j, \dots)$, and one can show that A'' is isomorphic to the image of A under $x \mapsto (\dots, a'_i a_j x, \dots)$ (alternatively, use (7.36) and (50)). □

PROPOSITION 7.27 *For any $\mathfrak{a}$-multiplication λ, $\deg(\lambda) = (\mathcal{O}_E\colon \mathfrak{a})$ provided $\mathfrak{a}$ is invertible (locally free of rank 1).*

[14] Small problem here: need to check $\mathfrak{a} + \mathfrak{a}'$ is projective (or else assume $R = \mathcal{O}_E$, which is all we really need). However, it seems to me that one should be able to prove (7.22) without counting degrees. Note that, in order to prove (7.22), it suffices to prove (7.24).

PROOF. When $\mathfrak{a}$ is principal, $\mathfrak{a} = (a)$, we proved this in (7.13). Next note that if a prime l doesn't divide $(R\colon \mathfrak{a})$, then it doesn't divide $\deg \lambda^{\mathfrak{a}}$. For, by the Chinese remainder theorem, there exists an $a \in \mathfrak{a}$ such that l doesn't divide $(R\colon (a))$;[15] write $(a) = \mathfrak{a}\mathfrak{b}$; then $\deg(\lambda^{\mathfrak{a}}) \deg(\lambda^{\mathfrak{b}}) = \deg \lambda^{(a)} = (\mathcal{O}_E\colon (a))$.

Let $\mathfrak{a} = \bigcap \mathfrak{q}$ be the primary decomposition of $\mathfrak{a}$. Because the nonzero prime ideals in R are maximal, the $\mathfrak{q}$ are relatively prime. Therefore, $\mathfrak{a} = \prod \mathfrak{q}$, and $R/\mathfrak{a} \simeq \prod R/\mathfrak{q}$ (Chinese remainder theorem). As $\mathfrak{a}$ is projective, $R/\mathfrak{a}$ has projective dimension ≤ 1; it follows that each $R/\mathfrak{q}$ has projective dimension ≤ 1, and so $\mathfrak{q}$ is projective. After (7.26), we may therefore suppose $\mathfrak{a}$ to be primary for some prime ideal $\mathfrak{p}$. Let $\mathfrak{p} \cap \mathbb{Z} = (p)$. The localization R_p of R relative to the multiplicative set $R \smallsetminus (p)$ is semilocal and noetherian. The ideal $\mathfrak{a}_p \overset{\text{def}}{=} \mathfrak{a}R_p$ is projective, and therefore free, say $\mathfrak{a}_p = (a/s)$ with $a \in \mathfrak{a}$ and $s \in \mathbb{Z}$ not divisible by p. Then $(a) = \mathfrak{a}\mathfrak{b}$ with $\mathfrak{b}$ an ideal such that $\mathfrak{b} \cap \mathbb{Z}$ is prime to p. As $\mathfrak{a}$ is $\mathfrak{p}$-primary, some power of p lies in $\mathfrak{a}$ and so $\deg(\lambda^{\mathfrak{a}})$ and $(R\colon \mathfrak{a})$ are both powers of p. On the other hand, $\deg(\lambda^{\mathfrak{b}})$ and $(R\colon \mathfrak{b})$ are both relatively prime to p. As

$$\begin{aligned} \deg(\lambda^{\mathfrak{a}}) \cdot \deg(\lambda^{\mathfrak{b}}) &= \deg(\lambda^{(a)}) \\ (R\colon \mathfrak{a})(R\colon \mathfrak{b}) &= (R\colon (a)) \quad (\text{as } \mathfrak{a} + \mathfrak{b} = R) \end{aligned}$$

and

$$\deg(\lambda^{(a)}) \overset{(7.13)}{=} (R\colon (a))$$

the statement follows.[16] □

COROLLARY 7.28 *Let $\mathfrak{a}$ be an invertible ideal in R. An E-isogeny $\lambda\colon A \to B$ is an $\mathfrak{a}$-multiplication if and only if* $\deg(\lambda) = (R\colon \mathfrak{a})$ *and the maps $a\colon A \to A$ for $a \in \mathfrak{a}$ factor through λ.*

PROOF. We only have to prove the sufficiency of the conditions. According to the definition (7.17), there exists an E-isogeny $\alpha\colon B \to A^{\mathfrak{a}}$ such that $\alpha \circ \lambda = \lambda^{\mathfrak{a}}$. Then $\deg(\alpha)\deg(\lambda) = \deg(\lambda^{\mathfrak{a}})$, and so α is an isogeny of degree 1, i.e., an isomorphism. □

PROPOSITION 7.29 *Let E be a CM-algebra, and let A and B be abelian varieties with complex multiplication by E over an algebraically closed field k of characteristic zero. If A and B are E-isogenous, then there exists a lattice ideal $\mathfrak{a}$ and an $\mathfrak{a}$-multiplication $A \to B$.*

PROOF. After (7.10), it suffices to prove this for $k = \mathbb{C}$. Because A and B are E-isogenous, they have the same type Φ. After choosing E-basis elements for $H_1(A, \mathbb{Q})$ and $H_1(B, \mathbb{Q})$, we have isomorphisms

$$\mathbb{C}^{\Phi}/\Phi(\mathfrak{a}) \to A(\mathbb{C}), \quad \mathbb{C}^{\Phi}/\Phi(\mathfrak{b}) \to B(\mathbb{C}).$$

[15] If l doesn't divide $(R\colon \mathfrak{a})$, then $R = \mathfrak{a} + (l)$, and so there exists an $a \in \mathcal{O}_E$ such that

$$\begin{aligned} a &\equiv 0 \mod \mathfrak{a} \\ a &\equiv 1 \mod l. \end{aligned}$$

[16] When $R = \mathcal{O}_E$, the proof is a little easier. According to the Chinese remainder theorem, there exists an $a \in \mathcal{O}_E$ such that $(a) = \mathfrak{a}\mathfrak{b}$ with $(\mathcal{O}_E\colon \mathfrak{a})$ and $(\mathcal{O}_E\colon \mathfrak{b})$ relatively prime. [Take a to be any element of $\mathcal{O}_E$ satisfying an appropriate congruence condition for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_E$ such that $(\mathcal{O}_E\colon \mathfrak{p})$ is not prime to $(\mathcal{O}_E\colon \mathfrak{a})$.] Then

$$\deg(\lambda^{\mathfrak{a}})\deg(\lambda^{\mathfrak{b}}) = \deg(\lambda^{(a)}) = (\mathcal{O}_E\colon (a)) = (\mathcal{O}_E\colon \mathfrak{a})(\mathcal{O}_E\colon \mathfrak{b}).$$

The only primes dividing $\deg(\lambda^{\mathfrak{a}})$ (resp. $\deg(\lambda^{\mathfrak{b}})$) are those dividing $(\mathcal{O}_E\colon \mathfrak{a})$ (resp. $(\mathcal{O}_E\colon \mathfrak{b})$), and so we must have $\deg(\lambda^{\mathfrak{a}}) = (\mathcal{O}_E\colon \mathfrak{a})$ and $\deg(\lambda^{\mathfrak{b}}) = (\mathcal{O}\colon \mathfrak{b})$.

Changing the choice of basis elements changes the ideals by principal ideals, and so we may suppose that $\mathfrak{a} \subset \mathfrak{b}$. The quotient map $\mathbb{C}^\Phi/\Phi(\mathfrak{a}) \to \mathbb{C}^\Phi/\Phi(\mathfrak{b})$ is an $\mathfrak{a}\mathfrak{b}^{-1}$-multiplication. □

PROPOSITION 7.30 *Let A be an abelian variety with multiplication by E over a number field k, and assume that A has good reduction at a prime $\mathfrak{p}$ of k. The reduction to $k_0 \overset{\text{def}}{=} \mathcal{O}_k/\mathfrak{p}$ of any $\mathfrak{a}$-multiplication $\lambda\colon A \to B$ is again an $\mathfrak{a}$-multiplication.*

PROOF. Let $a_1, \dots, a_n$ be a basis for $\mathfrak{a}$, and let $a_i = \alpha_i \circ \lambda$. In the diagram

$$A \xrightarrow{\lambda} B \xrightarrow{\alpha} A^n \qquad \alpha = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

(a : $A \to A^n$)

α maps B isomorphically onto the image of a. Let $\mathcal{A}$ and $\mathcal{B}$ be abelian schemes over $\mathcal{O}_\mathfrak{p}$ with general fibre A and B. Then the diagram extends uniquely to a diagram over $\mathcal{O}_\mathfrak{p}$ (see 6.6), and reduces to a similar diagram over k_0, which proves the proposition. (For an alternative proof, see 7.32.) □

$\mathfrak{a}$-multiplications (2)

In this subsection, R is a commutative ring.

PROPOSITION 7.31 *Let A be a commutative algebraic group A over a field k with an action of R. For any finitely presented R-module M, the functor*

$$\underline{A}^M(T) = \operatorname{Hom}_R(M, A(T)) \qquad (T \text{ a } k\text{-scheme})$$

is represented by a commutative algebraic group A^M over k with an action of R. Moreover,

$$A^{M \otimes_R N} \simeq (A^M)^N. \tag{50}$$

If M is projective and A is an abelian variety, then A^M is an abelian variety (of dimension $r \dim A$ if M is locally free of rank r).

PROOF. If $M = R^n$, then $\underline{A}^M$ is represented by A^n. The functor $M \mapsto \underline{A}^M$ transforms cokernels to kernels, and so a presentation

$$R^m \to R^n \to M \to 0,$$

realizes $\underline{A}^M$ as a kernel

$$0 \to \underline{A}^M \to A^n \to A^m.$$

Define A^M to be the kernel in the sense of algebraic groups.

For the second statement, use that there is an isomorphism of functors

$$\operatorname{Hom}_R(N, \operatorname{Hom}_R(M, A(T))) \simeq \operatorname{Hom}_R(M \otimes_R N, A(T)).$$

For the final statement, if M is projective, it is a direct summand of a free R-module of finite rank. Thus A^M is a direct factor of a product of copies of A, and so is an abelian variety. Assume that M is of constant rank r. For an algebraic closure $\overline{k}$ of k and a prime $\ell \neq \operatorname{char} k$,

$$\begin{aligned} A^M(\overline{k})_\ell &= \operatorname{Hom}_R(M, A(\overline{k})_\ell) \\ &\simeq \operatorname{Hom}_{R_\ell}(M_\ell, A(\overline{k})_\ell), \quad R_\ell \overset{\text{def}}{=} \mathbb{Z}_\ell \otimes R, \quad M_\ell \overset{\text{def}}{=} \mathbb{Z}_\ell \otimes_\mathbb{Z} M. \end{aligned}$$

But M_ℓ is free of rank r over R_ℓ (because R is semi-local), and so the order of $A^M(\overline{k})_\ell$ is $l^{2r \dim A}$. Thus A^M has dimension $r \dim A$. □

REMARK 7.32 The proposition (and its proof) applies over an arbitrary base scheme S. Moreover, the functor $A \mapsto A^M$ commutes with base change (because $A \mapsto \underline{A}^M$ obviously does). For example, if $\mathcal{A}$ is an abelian scheme over the ring of integers $\mathcal{O}_k$ in a local field k and M is projective, then $\mathcal{A}^M$ is an abelian scheme over $\mathcal{O}_k$ with general fibre $(\mathcal{A}_k)^M$.

PROPOSITION 7.33 *Let R act on an abelian variety A over a field k. For any finitely presented R-module M and $\ell \neq \operatorname{char} k$,*

$$T_\ell(A^M) \simeq \operatorname{Hom}_{R_\ell}(M_\ell, T_\ell A), \quad R_\ell \stackrel{\text{def}}{=} \mathbb{Z}_\ell \otimes R, \quad M_\ell \stackrel{\text{def}}{=} \mathbb{Z}_\ell \otimes_{\mathbb{Z}} M.$$

PROOF. As in the proof of (7.31),

$$A^M(\overline{k})_{\ell^n} \simeq \operatorname{Hom}_{R_\ell}(M_\ell, A(\overline{k})_{\ell^n}).$$

Now pass to the inverse limit over n. □

Let $R = \operatorname{End}_R(A)$. For any R-linear map $\alpha: M \to R$ and $a \in A(T)$, we get an element

$$x \mapsto \alpha(x) \cdot a: M \to A(T)$$

of $\underline{A}^M(T)$. In this way, we get a map $\operatorname{Hom}_R(M, R) \to \operatorname{Hom}_R(A, A^M)$.

PROPOSITION 7.34 *If M is projective, then* $\operatorname{Hom}_R(M, R) \simeq \operatorname{Hom}_R(A, A^M)$.

PROOF. When $M = R$, the map is simply $R \simeq \operatorname{End}_R(A)$. Similarly, when $M = R^n$, the map is an isomorphism. In the general case, $M \oplus N \approx R^n$ for some projective module N, and we have a commutative diagram

$$\begin{array}{ccc} \operatorname{Hom}_R(M, R) \oplus \operatorname{Hom}_R(N, R) & \longrightarrow & \operatorname{Hom}_R(A, A^M) \oplus \operatorname{Hom}_R(A, A^N) \\ \wr\| & & \wr\| \\ \operatorname{Hom}_R(R^n, R) & \xrightarrow{\simeq} & \operatorname{Hom}_R(A, A^n). \end{array}$$

□

PROPOSITION 7.35 *Let A be an abelian variety over a field k, and let R be a commutative subring of* $\operatorname{End}(A)$ *such that $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a product of fields and $[R: \mathbb{Z}] = 2 \dim A$. For any invertible ideal $\mathfrak{a}$ in R, the map $\lambda^{\mathfrak{a}}: A \to A^{\mathfrak{a}}$ corresponding to the inclusion $\mathfrak{a} \hookrightarrow A$ is an isogeny with kernel $A_{\mathfrak{a}} \stackrel{\text{def}}{=} \bigcap_{a \in \mathfrak{a}} \operatorname{Ker}(a)$.*

PROOF. The functor $M \mapsto A^M$ sends cokernels to kernels, and so the exact sequence

$$0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$$

gives rise to an exact sequence

$$0 \to A^{R/\mathfrak{a}} \to A \xrightarrow{\lambda^{\mathfrak{a}}} A^{\mathfrak{a}}.$$

Clearly $A^{R/\mathfrak{a}} = A_{\mathfrak{a}}$, and so it remains to show that $\lambda^{\mathfrak{a}}$ is surjective, but for a prime ℓ such that $\mathfrak{a}_\ell = R_\ell$, $T_\ell(\lambda^{\mathfrak{a}})$ is an isomorphism by (**??**), from which this follows. □

COROLLARY 7.36 *Under the hypotheses of the proposition, the homomorphism*

$$\lambda^{\mathfrak{a}}\colon A \to A^{\mathfrak{a}}$$

corresponding to the inclusion $\mathfrak{a} \hookrightarrow R$ *is an* $\mathfrak{a}$*-multiplication.*

PROOF. A family of generators $(a_i)_{1\le i\le n}$ for $\mathfrak{a}$ defines an exact sequence

$$R^m \to R^n \to \mathfrak{a} \to 0$$

and hence an exact sequence

$$0 \to A^{\mathfrak{a}} \to A^n \to A^m.$$

The composite of

$$R^n \to \mathfrak{a} \to R$$

is $(r_i) \mapsto \sum r_i a_i$, and so the composite of

$$A \xrightarrow{\lambda^{\mathfrak{a}}} A^{\mathfrak{a}} \hookrightarrow A^n$$

is $x \mapsto (a_i x)_{1\le i\le n}$. As $\lambda^{\mathfrak{a}}$ is surjective, it follows that $A^{\mathfrak{a}}$ maps onto the image of A in A^n, and so $\lambda^{\mathfrak{a}}$ is an $\mathfrak{a}$-multiplication (as shown in the proof of 7.20). □

REMARK 7.37 Corollary 7.36 fails if $\mathfrak{a}$ is not invertible. Then $A^{\mathfrak{a}}$ need not be connected, $A \to (A^{\mathfrak{a}})^\circ$ is the $\mathfrak{a}$-multiplication, and $A^{\mathfrak{a}}/(A^{\mathfrak{a}})^\circ \simeq \operatorname{Ext}^1_R(R/\mathfrak{a}, A)$ (see Waterhouse 1969, Appendix).

$\mathfrak{a}$-multiplications (3)

Let $\lambda\colon A \to B$ be an $\mathfrak{a}$-multiplication, and let $a \in \mathfrak{a}^{-1} \overset{\text{def}}{=} \{a \in E \mid a\mathfrak{a} \in R\}$. Then $\lambda \circ a \in \operatorname{Hom}(A, B)$ (rather than $\operatorname{Hom}^0(A, B)$). To see this, choose a basis for $a_1, \dots, a_n$ for $\mathfrak{a}$, and note that the composite of the "homomorphisms"

$$A \xrightarrow{a} A \xrightarrow{x\mapsto(\dots,a_i x,\dots)} A^n$$

is a homomorphism into $A^{\mathfrak{a}} \subset A^n$.

PROPOSITION 7.38 *Let A have complex multiplication by E over k.*

(a) Let $\lambda\colon A \to B$ be an $\mathfrak{a}$-multiplication. Then the map

$$a \mapsto \lambda^{\mathfrak{a}} \circ a\colon \mathfrak{a}^{-1} \to \operatorname{Hom}_R(A, B)$$

is an isomorphism. In particular, every R-isogeny $A \to B$ is a $\mathfrak{b}$-multiplication for some ideal $\mathfrak{b}$.

(b) Assume $\mathcal{O}_E = \operatorname{End}(A) \cap E$. For any lattice ideals $\mathfrak{a} \subset \mathfrak{b}$ in $\mathcal{O}_E$,

$$\operatorname{Hom}_{\mathcal{O}_E}(A^{\mathfrak{a}}, A^{\mathfrak{b}}) \simeq \mathfrak{a}^{-1}\mathfrak{b}.$$

[Better to state this in terms of invertible modules.]

PROOF. (a) In view of (7.36), the first statement is a special case of (7.34). For the second, recall (7.18) that $\lambda^{\mathfrak{a}} \circ a$ is an $\mathfrak{a}a$-multiplication.

(b) Recall that $A^{\mathfrak{b}} \simeq (A^{\mathfrak{a}})^{\mathfrak{a}^{-1}\mathfrak{b}}$ (see 7.26), and so this follows from (a). □

In more down-to-earth terms, any two E-isogenies $A \to B$ differ by an E-"isogeny" $A \to A$, which is an element of E. When λ is an $\mathfrak{a}$-multiplication, the elements of E such that $\lambda \circ a$ is an isogeny (no quotes) are exactly those in $\mathfrak{a}^{-1}$.

PROPOSITION 7.39 *Let A have complex multiplication by $\mathcal{O}_E$ over an algebraically closed field k of characteristic zero. Then $\mathfrak{a} \mapsto A^{\mathfrak{a}}$ defines an isomorphism from the ideal class group of $\mathcal{O}_E$ to the set of isogeny classes of abelian varieties with complex multiplication by $\mathcal{O}_E$ over k with the same CM-type as A.*

PROOF. Proposition (7.38) shows that every abelian variety isogenous to A is an $\mathfrak{a}$-transform for some ideal $\mathfrak{a}$, and so the map is surjective. As $a\colon A \to A$ is an (a)-multiplication, principal ideals ideals map to A. Finally, if $A^{\mathfrak{a}}$ is $\mathcal{O}_E$-isomorphic to A, then

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

and so $\mathfrak{a}$ is principal. [Better to state this in terms of invertible modules.] □

PROPOSITION 7.40 *Let A and B be abelian varieties with multiplication by $\mathcal{O}_E$ over a number field k, and assume that they have good reduction at a prime $\mathfrak{p}$ of k. If A and B are isogenous, every $\mathcal{O}_E$-isogeny $\mu\colon A_0 \to B_0$ lifts to an $\mathfrak{a}$-multiplication $\lambda\colon A \to B$ for some lattice ideal $\mathfrak{a}$, possibly after a finite extension of k. In particular, μ is an $\mathfrak{a}$-multiplication (over a finite extension).*

PROOF. Since A and B are isogenous, there is an $\mathfrak{a}$-multiplication $\lambda\colon A \to B$ for some lattice ideal $\mathfrak{a}$ by (7.29) (after a finite extension of k). According to Proposition 7.30, $\lambda_0\colon A_0 \to B_0$ is also an $\mathfrak{a}$-multiplication. Hence the reduction map

$$\mathrm{Hom}_{\mathcal{O}_E}(A, B) \to \mathrm{Hom}_{\mathcal{O}_E}(A_0, B_0)$$

is an isomorphism because both are isomorphic to $\mathfrak{a}^{-1}$, via λ and λ_0 respectively (7.38). Therefore, μ lifts to an isogeny $\lambda'\colon A \to B$, which is a $\mathfrak{b}$-multiplication (see 7.38). □

NOTES Most of the definitions and results on $\mathfrak{a}$-multiplications go back to Shimura and Taniyama 1961, but sometimes with inessential hypotheses. The functorial definition (7.31) was used for elliptic curves in Serre 1967, p294. Giraud (with Raynaud) extended (7.27) to the case of arbitrary orders R in $\mathcal{O}_E$ (Giraud 1968, Proposition 2, Remark 1).

8 The Shimura-Taniyama formula

Review of numerical norms

Let K be a number field. For a fractional ideal $\mathfrak{a} = \prod \mathfrak{p}_i^{m_i}$ of K,

$$\mathrm{Nm}_{K/\mathbb{Q}}(\mathfrak{a}) \stackrel{\text{def}}{=} \prod (p_i)^{m_i f(\mathfrak{p}_i/p_i)}, \quad (p_i) = \mathfrak{p}_i \cap \mathbb{Z}.$$

The ***numerical norm*** $\mathbb{N}\mathfrak{a} = \mathbb{N}_{K/\mathbb{Q}}\mathfrak{a}$ of a nonzero ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is $\stackrel{\text{def}}{=} (\mathcal{O}_K : \mathfrak{a})$. Recall that

$$(\mathbb{N}\mathfrak{a}) = \mathrm{Nm}_{K/\mathbb{Q}}\,\mathfrak{a}.$$

In particular, for $\mathfrak{a} = (a)$,

$$\mathbb{N}\mathfrak{a} = \left|\mathrm{Nm}_{K/\mathbb{Q}}\, a\right| = (\mathcal{O}_K : a\mathcal{O}_K).$$

As $\mathrm{Nm}_{K/\mathbb{Q}}$ is a homomorphism, so also is $\mathbb{N}$:

$$(\mathcal{O}_K : \mathfrak{a})(\mathcal{O}_K : \mathfrak{b}) = (\mathcal{O}_K : \mathfrak{a}\mathfrak{b}).$$

For example, if $\mathfrak{p}$ is prime and $(p) = \mathfrak{p} \cap \mathbb{Z}$, then

$$\begin{aligned} \mathrm{Nm}_{K/\mathbb{Q}}\,\mathfrak{p} &= (p^{f(\mathfrak{p}/p)}) \\ \mathbb{N}\mathfrak{p} &= p^{f(\mathfrak{p}/p)}. \end{aligned}$$

Cf. ANT 4.1, 4.2. Similar statements apply to ideals in products of number fields. In the next subsection, we sometimes don't distinguish a positive integer from the ideal it generates. [Omit this subsection.]

Statement and proof

THEOREM 8.1 *Let A be an abelian variety with complex multiplication by a CM-algebra E over a finite extension k of $\mathbb{Q}_p$. Suppose that k contains all conjugates of E and that A has good reduction at the prime ideal $\mathfrak{P}$ of $\mathcal{O}_k$.*[17] *Assume (i) that p is unramified in E and (ii) that* $\mathrm{End}(A) \cap E = \mathcal{O}_E$.

(a) *There exists an element $\pi \in \mathcal{O}_E$ inducing the Frobenius endomorphism on the reduction of A.*

(b) *The ideal generated by π factors as follows*

$$(\pi) = \prod\nolimits_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\,\mathfrak{P}) \tag{51}$$

where $\Phi \subset \mathrm{Hom}(E, k)$ is the CM-type of A.

[17] *To recall, the hypotheses mean that E is a $\mathbb{Q}$-subalgebra of* $\mathrm{End}^0(A)$ *of degree* $2\dim A$, *and that* $\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(E, k)$ *has* $[E:\mathbb{Q}]$ *elements. Then*

$$\mathrm{Tgt}_0(A) \simeq \prod\nolimits_{\varphi \in \Phi} k_\varphi \qquad \text{(as } E \otimes_{\mathbb{Q}} k\text{-modules)}$$

where Φ is a subset of $\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(E, k)$ *and k_φ is a one-dimensional k-vector space on which E acts through φ.*

PROOF. Let A_0 be the reduction of A to $k_0 \stackrel{\text{def}}{=} \mathcal{O}_k/\mathfrak{P}$, and let

$$q = |k_0| = (\mathcal{O}_k : \mathfrak{P}) = p^{f(\mathfrak{P}/p)}.$$

(a) The ring $\mathrm{End}(A_0) \cap E$ is an order in E containing $\mathrm{End}(A) \cap E$. As the latter is the maximal order $\mathcal{O}_E$, so must be the former. The Frobenius endomorphism of A_0 commutes with all endomorphisms of A_0, and so the statement follows from (7.4).

(b) Let $T = \mathrm{Tgt}_0(A)$. It is an $E \otimes_{\mathbb{Q}} k$-space, and T has a k-basis $(e_\varphi)_{\varphi\in\Phi}$ such that $ae_\varphi = \varphi(a)e_\varphi$ for $a \in E$. Moreover, $\mathcal{T} \stackrel{\text{def}}{=} \mathrm{Tgt}_0(\mathcal{A})$ is a lattice in T such that $\mathcal{T}/\mathfrak{P}\mathcal{T} \simeq \mathrm{Tgt}_0(A_0)$ (see (45)). Because p is unramified in E, the e_φ can be scaled to an $\mathcal{O}_{\mathfrak{P}}$-basis for $\mathcal{T}$ such that $ae_\varphi = \varphi(a)e_\varphi$ for $a \in \mathcal{O}_E$.[18]

Because $\pi\overline{\pi} = q$, the ideal (π) is divisible only by primes dividing p. Let

$$(\pi) = \prod\nolimits_{v|p} \mathfrak{p}_v^{m_v}, \quad m_v \geq 0,$$

and, for h the class number of E, let

$$\mathfrak{p}_v^{m_v h} = (\gamma_v), \quad \gamma_v \in \mathcal{O}_E. \tag{52}$$

Let

$$\begin{aligned} \Phi_v &= \{\varphi \in \Phi \mid \varphi^{-1}(\mathfrak{P}) = \mathfrak{p}_v\}, \\ d_v &= |\Phi_v|. \end{aligned}$$

The kernel of γ_v on T is spanned by the e_φ for which $\varphi(\gamma_v) \in \mathfrak{P}$, i.e., such that γ_v lies in the prime ideal $\varphi^{-1}(\mathfrak{P})$. But $\mathfrak{p}_v$ is the only prime ideal in $\mathcal{O}_E$ containing γ_v, and so

$$\mathrm{Ker}(T \xrightarrow{\gamma_v} T) = \langle e_\varphi \mid \varphi \in \Phi_v\rangle.$$

Since $\pi^h : A_0 \to A_0$ factors through γ_v, we have that $\gamma_v^* k_0(A_0) \supset (\pi^h)^* k_0(A_0) = k_0(A_0)^{q^h}$, and so Proposition 7.14 shows that

$$\deg(A_0 \xrightarrow{\gamma_v} A_0) \leq q^{hd_v}.$$

As

$$\deg(A_0 \xrightarrow{\gamma_v} A_0) \stackrel{(7.13)}{=} \mathrm{Nm}_{E/\mathbb{Q}}\, \gamma_v \stackrel{(52)}{=} \mathrm{Nm}_{E/\mathbb{Q}}(\mathfrak{p}_v^{hm_v})$$

we see that

$$\mathrm{Nm}_{E/\mathbb{Q}}(\mathfrak{p}_v^{m_v}) \leq q^{d_v}. \tag{53}$$

On taking the product over v, we find that

$$\mathrm{Nm}_{E/\mathbb{Q}}(\pi) \leq q^{\sum_{v|p} d_v} \leq q^g.$$

But

$$\mathrm{Nm}_{E/\mathbb{Q}}(\pi) \stackrel{(7.13)}{=} \deg(A_0 \xrightarrow{\pi} A_0) = q^g,$$

[18] Since $\mathcal{O}_E$ is unramified at p, $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is étale over $\mathbb{Z}_p$, and so $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathcal{O}_{\mathfrak{P}}$ is étale over $\mathcal{O}_{\mathfrak{P}}$. In fact, the isomorphism $E \otimes_{\mathbb{Q}} k \simeq \prod_{\sigma: E\to k} k_\sigma$ induces an isomorphism $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathcal{O}_{\mathfrak{P}} \simeq \prod_{\sigma: E\to k} \mathcal{O}_\sigma$ where $\mathcal{O}_\sigma$ denotes $\mathcal{O}_{\mathfrak{P}}$ regarded as a $\mathcal{O}_E$-algebra via σ. Thus, the finitely generated projective $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathcal{O}_{\mathfrak{P}}$-modules are direct sums of $\mathcal{O}_\sigma$'s, from which the statement follows. For a more explicit proof, see Shimura 1999, 13.2.

and so equality holds everywhere.

Equality in (53) shows that

$$\begin{aligned}\mathrm{Nm}_{E/\mathbb{Q}}(\mathfrak{p}_v^{m_v}) &= \left(\mathrm{Nm}_{k/\mathbb{Q}}\mathfrak{P}\right)^{d_v}\\ &= \prod\nolimits_{\varphi\in\Phi_v}\left(\mathrm{Nm}_{k/\mathbb{Q}}\,\mathfrak{P}\right)\\ &= \prod\nolimits_{\varphi\in\Phi_v}\left(\mathrm{Nm}_{E/\mathbb{Q}}(\varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\mathfrak{P}))\right)\\ &= \mathrm{Nm}_{E/\mathbb{Q}}\left(\prod\nolimits_{\varphi\in\Phi_v}\varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\mathfrak{P})\right).\end{aligned}$$

From the definition of Φ_v, we see that $\prod_{\varphi\in\Phi_v}\varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\mathfrak{P})$ is a power of $\mathfrak{p}_v$, and so this shows that

$$\mathfrak{p}_v^{m_v} = \prod\nolimits_{\varphi\in\Phi_v}\varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\,\mathfrak{P}). \tag{54}$$

On taking the product over v, we obtain the required formula. □

COROLLARY 8.2 *With the hypotheses of the theorem, for all primes $\mathfrak{p}$ of E dividing p,*

$$\mathrm{ord}_{\mathfrak{p}}(\pi) = \sum\nolimits_{\varphi\in\Phi,\,\varphi^{-1}(\mathfrak{P})=\mathfrak{p}} f(\mathfrak{P}/\varphi\mathfrak{p}). \tag{55}$$

PROOF. The formula is a restatement of (54). □

COROLLARY 8.3 *With the hypotheses of the theorem, for all primes v of E dividing p,*

$$\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)} = \frac{|\Phi\cap H_v|}{|H_v|} \tag{56}$$

where $H_v = \{\rho\colon E\to k \mid \rho^{-1}(\mathfrak{P}) = \mathfrak{p}_v\}$ and $q = (\mathcal{O}_k\colon\mathfrak{P})$.

PROOF. Because p is unramified in E, $\mathrm{ord}_v(p) = 1$ for the primes v of E dividing p, and so

$$\mathrm{ord}_v(q) = f(\mathfrak{P}/p).$$

On the other hand (see (55)),

$$\mathrm{ord}_v(\pi) = \sum\nolimits_{\varphi\in\Phi\cap H_v} f(\mathfrak{P}/\varphi\mathfrak{p}_v),$$

and so

$$\frac{\mathrm{ord}_v(\pi)}{\mathrm{ord}_v(q)} = \sum\nolimits_{\varphi\in\Phi\cap H_v}\frac{1}{f(\mathfrak{p}_v/p)} = |\Phi\cap H_v|\cdot\frac{1}{|H_v|}.$$

□

REMARK 8.4 The argument in the proof of (8.3) shows that (56) is equivalent to (55), even without assuming that p is unramified in E (without that assumption, both of $\mathrm{ord}_v(q)$ and $|H_v|$ have to be multiplied by $e(\mathfrak{p}_v/p)$).

We let $[M]_R$ denote the class of an R-module M of finite length in the Grothendieck group of such modules. For example, if R is a product of Dedekind domains, then every R-module of finite length M has a composition series

$$M\supset\cdots\supset M_i\supset M_{i-1}\supset\cdots\supset 0,\quad M_i/M_{i-1}\approx R/\mathfrak{p}_i,\quad \mathfrak{p}_i \text{ maximal ideal},$$

and the map $M\mapsto\prod_i\mathfrak{p}_i^{-1}$ defines an isomorphism of the Grothendieck group with the group of fractional ideals.

COROLLARY 8.5 *With the hypotheses of the theorem,*

$$[\mathrm{Tgt}_0(A_0)]_{\mathcal{O}_E} = [\mathcal{O}_E/\pi\mathcal{O}_E]_{\mathcal{O}_E}. \tag{57}$$

PROOF. Let $\kappa = \mathcal{O}_k/\mathfrak{P}$. Then

$$\mathrm{Tgt}_0(A_0) \simeq \sum\nolimits_{\varphi\in\Phi} \kappa_\varphi$$

where κ_φ is a one-dimensional κ-vector space on which $\mathcal{O}_E$ acts through φ.[19] If $\varphi^{-1}(\mathfrak{P}) = \mathfrak{p}$, then $\kappa_\varphi \approx (\mathcal{O}_E/\varphi\mathfrak{p})^{q/(\mathcal{O}_E:\varphi\mathfrak{p})}$, and so κ_φ contributes $\mathfrak{p}^{q/(\mathcal{O}_E:\varphi\mathfrak{p})} = \mathfrak{p}^{f(\mathfrak{P}/p)/f(\varphi\mathfrak{p}/p)} = \mathfrak{p}^{f(\mathfrak{P}/\varphi\mathfrak{p})}$ to $[\mathrm{Tgt}_0(A_0)]_{\mathcal{O}_E}$. Thus, (57) is a restatement of (55). □

REMARK 8.6 (a) In the statement of Theorem 8.1, k can be a number field.

(b) The conditions in the statement are unnecesarily strong. For example, the formula holds without the assumption that p be unramified in E. See Theorem 9.3 below.

(c) When E is a subfield of k, Theorem 8.1 can be stated in terms of the reflex CM-type cf. Shimura and Taniyama 1961, §13.

Let (E,Φ) be a CM-pair, and let $E^* \subset \mathbb{Q}^{\mathrm{al}}$ be the reflex field. Recall (§1) that, for any number field k, $E^* \subset k \subset \mathbb{Q}^{\mathrm{al}}$, the reflex norm defines a homomorphism $N_{k,\Phi}$ from the group of fractional ideals of k to that of E; if k contains all conjugates of E, then

$$N_{k,\Phi}(\mathfrak{a}) = \prod\nolimits_{\varphi\in\Phi} \varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\,\mathfrak{a})$$

(see 1.26). Thus, the Shimura-Taniyama formula (51) says that

$$(\pi) = N_{k,\Phi}(\mathfrak{P}).$$

Recall (1.23) that $N_{k,\Phi}(\mathfrak{P}) = N_\Phi(\mathrm{Nm}_{k/E^*}\,\mathfrak{P})$.

COROLLARY 8.7 *Let (E,Φ) be a CM-pair, and let A be an abelian variety of CM-type (E,Φ) over a number field*[20] *k which is a Galois extension of $\mathbb{Q}$. Suppose that A has good reduction at the prime ideal $\mathfrak{P}$ of $\mathcal{O}_k$. Let $\mathfrak{P}\cap\mathcal{O}_{E^*} = \mathfrak{p}$ and $\mathfrak{p}\cap\mathbb{Z} = (p)$. Assume that (i) p is unramified in E; (ii) $\mathrm{End}(A)\cap E = \mathcal{O}_E$; (iii) $\mathfrak{P}$ is unramified over E^*.*

(a) *Let σ be the Frobenius element $(\mathfrak{P}, k/E^*)$; then there exists an $\mathfrak{a}$-multiplication $\alpha\colon A \to \sigma A$ over a finite extension of k such that $\alpha_0\colon A_0 \to A_0^{(q)}$ is the q-power Frobenius map, where $q = (\mathcal{O}_{E^*}\colon\mathfrak{p})$.*

(b) *Moreover,*

$$\mathfrak{a} = N_\Phi(\mathfrak{p}). \tag{58}$$

PROOF. As σ fixes E^*, A and σA have the same CM-type, and so they become isogenous over a finite extension of k. Therefore, (a) holds by (7.40). Moreover, $\sigma^{f-1}\alpha\circ\cdots\circ\sigma\alpha\circ\alpha = \pi$, where $f = [\kappa(\mathfrak{P})\colon\kappa(\mathfrak{p})]$; therefore,

$$\mathfrak{a}^f = N_\Phi(\mathrm{Nm}_{k/E^*}\,\mathfrak{P}) = N_\Phi(\mathfrak{p}^f) = N_\Phi(\mathfrak{p})^f,$$

which implies (58). □

[19] With the notations of the proof of Theorem 8.1, $\kappa_\varphi = k_0 e_\varphi$ and $\kappa = k_0$.

[20] *Thus, k contains the reflex field E^*.*

EXERCISE 8.8 Adapt the proof of Theorem 8.9 below to give a direct proof of Theorem 8.1 (with fewer assumptions).

The original proof of the Shimura-Taniyama formula, which we presented above, is the most direct and elementary. However, there other approaches which may add additional insight for those with the appropriate knowledge.

Alternative approach using schemes (Giraud 1968)

Giraud (1968) re-examined the original proof from the perspective of schemes, and sharpened some intermediate results, e.g., (7.27). He proved directly the formula for the tangent space of an abelian variety with complex multiplication over a finite field, and deduced the Shimura-Taniyama formula from it.

In this subsection, A is an abelian variety of dimension g over a field k and R is a commutative subring of $\mathrm{End}(A)$ such that $[R:\mathbb{Z}] = 2g$ and $E \stackrel{\text{def}}{=} R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a product of fields. We make free use of the results from §7 on the functor $M \mapsto A^M$ from finitely generated projective R-modules to abelian varieties.

THEOREM 8.9 (GIRAUD 1968, THÉORÈM 1) *Suppose k is finite, with q elements, and that the q-power Frobenius map $\pi: A \to A$ lies in R. Then*

$$[\mathrm{Tgt}_0(A)]_R = [R/(\pi)]_R \tag{59}$$

(equality of elements of the Grothendieck group of R).

PROOF. Let $(\pi) = \bigcap_{i\in I} \mathfrak{q}_i$ be the primary decomposition of (π). Because nonzero prime ideals in R are maximal, the $\mathfrak{q}_i$ are relatively prime.[21] Therefore, $(\pi) = \prod_{i\in I} \mathfrak{q}_i$, and $R/(\pi) \simeq \prod_{i\in I} R/\mathfrak{q}_i$ (Chinese remainder theorem).

Write $T(A)$ for $\mathrm{Tgt}_0(A)$. We can regard it as a commutative group scheme over k on which R acts. For any finitely generated R-module M,

$$T(A^M) \simeq T(A)^M,$$

as can be seen by using the definition of the tangent space in terms of dual numbers.[22] As $T(A)$ is killed by π, we have $T(A) = T(A)^{R/(\pi)}$, and so

$$T(A) = \bigoplus\nolimits_{i\in I} T_i, \quad T_i \stackrel{\text{def}}{=} T(A)^{R/\mathfrak{q}_i},$$

---

[21] The only prime ideal containing $\mathfrak{q}_i$ is its radical $\mathfrak{p}_i$. As $\mathfrak{p}_i \neq \mathfrak{p}_j$, $\mathfrak{q}_i + \mathfrak{q}_j = R$.

[22] For any k-algebra R,

$$A(R[\varepsilon]) \simeq A(R) \oplus T(A)(R) \qquad (*)$$

Therefore

$$\mathrm{Hom}_R(M, A(R[\varepsilon])) \simeq \mathrm{Hom}_R(M, A(R)) \oplus \mathrm{Hom}_R(M, T(A)(R))$$

i.e,

$$A^M(R[\varepsilon]) \simeq A^M(R) \oplus T(A)^M(R).$$

On replacing A with A^M in (*), we obtain

$$A^M(R[\varepsilon]) \simeq A^M(R) \oplus T(A^M)(R).$$

On comparing these isomorphisms, we find that

$$T(A)^M \simeq T(A^M).$$

is the primary decomposition of $T(A)$. It suffices to prove that, for each $i \in I$,

$$\text{Card}(T_i) = (R\colon \mathfrak{q}_i). \tag{60}$$

In fact, since we know that

$$q^g = \text{Card}(T(A)) = \textstyle\prod_{i\in I} \text{Card}(T_i)$$
$$q^g = \deg(\pi) \overset{(7.13)}{=} (R\colon(\pi)) = \textstyle\prod_{i\in I}(R\colon \mathfrak{q}_i),$$

it suffices to show that, for each $i \in I$,

$$\text{Card}(T_i) \geq (R\colon \mathfrak{q}_i). \tag{61}$$

As (π) is a free R-module, $R/(\pi)$ is of projective dimension ≤ 1. Therefore, each of the direct factors of $R/(\pi)$ has projective dimension ≤ 1, and so $\mathfrak{q}_i$ is projective. Proposition 7.27 shows that $\deg(\lambda^{\mathfrak{q}_i}) = (R\colon \mathfrak{q}_i)$. On the other hand, $M \mapsto T(A)^M$ transforms the exact sequence

$$\mathfrak{q}_i \to R \to R/\mathfrak{q}_i \to 0$$

into the exact sequence

$$0 \to T(A)^{R/\mathfrak{q}_i} \to T(A) \overset{T(\lambda^{\mathfrak{q}_i})}{\longrightarrow} T(A)^{\mathfrak{q}_i},$$

and so Proposition 7.14 shows that $\deg(\lambda^{\mathfrak{q}_i}) \leq \text{Card}(T_i)$. □

PROOF (OF THEOREM 8.1) We saw in the proof of (8.5) that, in the context of (8.1), formulas (51) and (59) are equivalent. □

Alternative approach using p-divisible groups (Tate 1968)

Tate (1968, §5) restated the Shimura-Taniyama formula for p-divisible groups, and proved it in that more general context. His proof also doesn't require that p be unramified in E.

BRIEF REVIEW OF p-DIVISIBLE GROUPS

Define a p-divisible group G, including over a dvr.
Define its height, tangent space, and dimension.
Define the degree of an isogeny.
Note that V_pG is a $\mathbb{Q}_p$-vector space of dimension $h(G)$.

EXAMPLE 8.10 Let $\mathcal{A}$ be an abelian scheme, and let $\mathcal{A}(p) = (A_{p^n})_{n\geq 1}$ be the associated p-divisible group. Then $\mathcal{A} \mapsto \mathcal{A}(p)$ is a functor, and

$$\text{Tgt}_0(\mathcal{A}) \simeq \text{Tgt}_0(\mathcal{A}(p)).$$

The height of $\mathcal{A}(p)$ is $2\dim A$ and the dimension of $\mathcal{A}(p)$ is $\dim A$.

Need also:

- ◇ The degree of the q-power Frobenius map on a p-divisible group G over $\mathbb{F}_q$ is $q^{d(G)}$.
- ◇ The degree of $q\colon G \to G$ on a p-divisible group G over $\mathbb{F}_q$ is $q^{h(G)}$.

p-DIVISIBLE GROUPS WITH COMPLEX MULTIPLICATION

Let k be a finite extension of $\mathbb{Q}_p$, and let G be a p-divisible group G over $\mathcal{O}_k$. A subfield E of $\mathrm{End}^0(G)$ acts faithfully on V_pG, and so has degree $\leq h(G)$ over $\mathbb{Q}_p$. When equality holds, we say that G ***has complex multiplication by*** E ***over*** $\mathcal{O}_k$. Let $\overline{k}$ be an algebraic closure of k. Then

$$\mathrm{Tgt}(G) \otimes_{\mathcal{O}} \overline{k} \simeq \bigoplus\nolimits_{\varphi\in\Phi} \overline{k}_\varphi$$

where $\Phi \subset \mathrm{Hom}_{\mathbb{Q}_p\text{-alg}}(E,\overline{k})$ and where $\overline{k}_\varphi$ is a one-dimensional $\overline{k}$-vector space on which E acts through the homomorphism $\varphi\colon E \to \overline{k}$. We say that G is of type (E,Φ) over $\mathcal{O}_k$.

PROPOSITION 8.11 *Let G be a p-divisible group with complex multiplication by E, and let $R = \mathrm{End}(G) \cap E$. For any $\alpha \in R$, the degree of $\alpha\colon G \to G$ is $(R\colon \alpha R)$.*

PROOF. To be added. □

THEOREM 8.12 (TATE 1968, THÉORÈME 3) *Let G be a p-divisible group of type (E,Φ) over over $\mathcal{O}_k$. Assume that R contains an element π which induces the q-power Frobenius map on G_0 over k_0. Then*

$$\frac{\mathrm{ord}(\pi)}{\mathrm{ord}(q)} = \frac{d(G)}{h(G)} = \frac{|\Phi|}{|H|} \tag{62}$$

where ord *is the valuation on E and $H = \mathrm{Hom}_{\mathbb{Q}_p}(E,\overline{k})$.*

PROOF. We have

$$(\mathcal{O}_k\colon \pi\mathcal{O}_k) \overset{(8.11)}{=} \deg(G \xrightarrow{\pi} G) = \deg(G_0 \xrightarrow{\pi_0} G_0) = q^{d(G)}$$
$$(\mathcal{O}_k\colon q\mathcal{O}_k) \overset{(8.11)}{=} \deg(G \xrightarrow{q} G) = q^{h(G)}.$$

This proves the first equality, and the second is obvious. □

PROOF (OF THEOREM 8.1) We prove the equivalent statement (8.3). With the notations of (8.1), let $\mathcal{A}$ be the abelian scheme over $\mathcal{O}_k$ with general fibre A, and let $\mathcal{A}(p)$ be the associated p-divisible group. Then $E \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \prod_{v|p} E_v$. Write $1 = \sum e_v$ (in $E \otimes_{\mathbb{Q}} \mathbb{Q}_p$) with e_v integral. Then $x \mapsto e_v x$ is an isogeny $\mathcal{A}(p) \to \prod_{v|p} \mathcal{A}(p)_v$. Let

$$H_v = \{\rho\colon E \to k \mid \rho^{-1}(\mathfrak{P}) = \mathfrak{p}_v\} \simeq \{\rho\colon E_v \to k\}.$$

The idempotents e_v also define a decomposition

$$\mathrm{Tgt}_0(\mathcal{A}) \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathrm{Tgt}_0(\mathcal{A}(p)) \simeq \bigoplus\nolimits_{v|p} \mathrm{Tgt}_0(\mathcal{A}(p)_v),$$

and $\mathcal{A}(p)_v$ is of type (E_v,Φ_v) where $\Phi_v = \Phi \cap H_v$. Therefore, for $G = \mathcal{A}(p)_v$, equation (62) becomes equation (56). □

Alternative approach using crystals (Deligne c1968)

In a handwritten manuscript (Deligne nd), Deligne showed how to derive the Shimura-Taniyama formula, as well as the fundamental theorem of complex multiplication over the reflex field, from the theory of canonical liftings of abelian varieties. See the next section.

Alternative approach using Hodge-Tate decompositions (Serre 1968)

Serre (1968) gives some hints for another possible approach to the formula of Shimura and Taniyama in his remark on pages II-28 and II-29.

NOTES The first statement of (51) in print is in Weil's conference talk (Weil 1956b, p21), where he writes "[For this] it is enough to determine the prime ideal decomposition of π .... *But this has been done by Taniyama* (cf. §3 of his contribution to this volume)." (italics in the original). In the mentioned section, Taniyama proves (51) by essentially the same method as we used (Taniyama 1956). However, see the remarks in Honda 1968, p89. [To be rewritten.]

9 The fundamental theorem of complex multiplication over the reflex field.

Review of the reflex norm

Let E be a CM-algebra, and Φ a CM-type on E, say, $\Phi \subset \mathrm{Hom}(E, \overline{\mathbb{Q}})$ where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. By definition, E^* is the smallest subfield of $\overline{\mathbb{Q}}$ such that there exists an $E \otimes_{\mathbb{Q}} E^*$-module V with

$$V \otimes_{E^*} \overline{\mathbb{Q}} \simeq \bigoplus\nolimits_{\varphi \in \Phi} \overline{\mathbb{Q}}_\varphi \qquad \text{(as an } E \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}\text{-module)}$$

where $\overline{\mathbb{Q}}_\varphi$ is a one-dimensional $\overline{\mathbb{Q}}$-vector space on which E acts through φ. The $E \otimes_{\mathbb{Q}} E^*$-module V is then uniquely determined up to isomorphism. Let $T = (\mathbb{G}_m)_{E/\mathbb{Q}}$ and $T^* = (\mathbb{G}_m)_{E^*/\mathbb{Q}}$. Then there is a homomorphism $N_\Phi \colon T^* \to T$ of tori such that $E^{*\times} = T^*(\mathbb{Q}) \to T(\mathbb{Q}) = E^\times$ sends $a \in E^*$ to its determinant as an E-linear automorphism of V. From N_Φ we get compatible homomorphisms on idèles, ideals, etc.. Moreover (1.26):

> Let $k \subset \overline{\mathbb{Q}}$ be a finite extension of E^* containing all conjugates of E. For any prime ideal $\mathfrak{a}$ of k,
>
> $$N_\Phi(\mathrm{Nm}_{k/E^*}\,\mathfrak{a}) = \prod\nolimits_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\,\mathfrak{a}).$$

Preliminaries from algebraic number theory

LEMMA 9.1 *Let $\mathfrak{a}$ be a fractional ideal in E. For any integer $m > 0$, there exists an $a \in E^\times$ such that $a\mathfrak{a} \subset \mathcal{O}_E$ and $(\mathcal{O}_E : a\mathfrak{a})$ is prime to m.*

PROOF. It suffices to find an $a \in E$ such that

$$\mathrm{ord}_v(a) + \mathrm{ord}_v(\mathfrak{a}) \geq 0 \tag{63}$$

for all finite primes v, with equality holding if $v|m$.

Choose a $c \in \mathfrak{a}$. Then $\mathrm{ord}_v(c^{-1}\mathfrak{a}) \leq 0$ for all finite v. For each v such that $v|m$ or[23] $\mathrm{ord}_v(\mathfrak{a}) < 0$, choose an $a_v \in \mathcal{O}_E$ such that

$$\mathrm{ord}_v(a_v) + \mathrm{ord}_v(c^{-1}\mathfrak{a}) = 0$$

(exists by the Chinese remainder theorem). For any $a \in \mathcal{O}_E$ sufficiently close to each a_v (which exists by the Chinese remainder theorem again), ca satisfies the required condition.□

Let k be a number field. For a finite set S of finite primes of k, $I^S(k)$ denotes the group of fractional ideals of k generated by the prime ideals not in S. Assume k is totally imaginary. Then a modulus $\mathfrak{m}$ for k is just an ideal in $\mathcal{O}_k$, and $S(\mathfrak{m})$ denotes the set of finite primes v dividing $\mathfrak{m}$ (i.e., such that $\mathrm{ord}_v(\mathfrak{m}) > 0$). Moreover, $k_{\mathfrak{m},1}$ denotes the group of $a \in k^\times$ such that

$$\mathrm{ord}_v(a - 1) \geq \mathrm{ord}_v(\mathfrak{m})$$

for all finite primes v dividing $\mathfrak{m}$. In other words, a lies in $k_{\mathfrak{m},1}$ if and only if multiplication by a preserves $\mathcal{O}_v \subset k_v$ for all v dividing $\mathfrak{m}$ and acts as 1 on $\mathcal{O}_v/\mathfrak{p}_v^{\mathrm{ord}_v(\mathfrak{m})} = \mathcal{O}_v/\mathfrak{m}$. Finally,

$$C_{\mathfrak{m}}(k) = I^{S(\mathfrak{m})}/i(k_{\mathfrak{m},1})$$

is the ray class group modulo $\mathfrak{m}$. Here i is the map sending an element to its principal ideal. (Cf. CFT V 1.).

[23] Or both!

The fundamental theorem in terms of ideals

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and let A be an abelian variety with complex multiplication by a CM-algebra[24] E over $\overline{\mathbb{Q}}$. Let $\Phi \subset \mathrm{Hom}(E, \overline{\mathbb{Q}})$ be the type of A. Assume $\mathrm{End}(A) \cap E = \mathcal{O}_E$. Fix an integer $m > 0$.

Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$. Because σ fixes E^*, the varieties A and σA are E-isogenous (3.12), and so there exists an $\mathfrak{a}$-multiplication $\alpha\colon A \to \sigma A$ for some ideal $\mathfrak{a} \subset \mathcal{O}_E$ (see 7.29). Recall (7.27) that α has degree $(\mathcal{O}_E\colon \mathfrak{a})$. After possibly replacing α with $\alpha \circ a$ for some $a \in \mathfrak{a}^{-1}$, it will have degree prime to m (apply 9.1). Then α maps A_m isomorphically onto σA_m.[25]

Let $\mathbb{Z}_m = \prod_{\ell|m} \mathbb{Z}_\ell$ and $\mathcal{O}_m = \mathcal{O}_E \otimes \mathbb{Z}_m$. Then $T_m A \stackrel{\text{def}}{=} \prod_{\ell|m} T_\ell A$ is a free $\mathcal{O}_m$-module of rank 1 (see 7.6). The maps

$$x \mapsto \sigma x,\ x \mapsto \alpha x\colon T_m A \to T_m(\sigma A)$$

are both $\mathcal{O}_m$-linear isomorphisms, and so they differ by a homothety by an element β of $\mathcal{O}_m^\times$:

$$\alpha(\beta x) = \sigma x, \quad \text{all } x \in T_m A.$$

For any $b \in \mathcal{O}_E$ sufficiently close to β, $\alpha \circ b$ will agree with σ on A_m. Thus, after replacing α with $\alpha \circ b$, we will have

$$\alpha(x) \equiv \sigma x \mod m, \quad \text{all } x \in T_m A.$$

Now α is an $\mathfrak{a}$-multiplication for an ideal $\mathfrak{a}$ that is well-defined up to an element of $i(E_{m,1})$.

REMARK 9.2 The abelian variety A will have a model, which we again denote A, over some subfield k of $\overline{\mathbb{Q}}$ that is finite and Galois over E^*. After possibly enlarging k, we may suppose that A has complex multiplication by E over k. Let $\mathfrak{P}$ be a prime ideal of k such that

- A has good reduction at $\mathfrak{P}$;
- $\mathfrak{P}$ is unramified over $\mathfrak{p} \stackrel{\text{def}}{=} \mathfrak{P} \cap \mathcal{O}_{E^*}$;
- $p \stackrel{\text{def}}{=} \mathfrak{p} \cap \mathbb{Z}$ is unramified in E.

Let σ be the Frobenius element $(\mathfrak{P}, k/E^*)$, and let $q = (\mathcal{O}_{E^*}\colon \mathfrak{p})$. Corollary 8.7 shows that there exists an $\mathfrak{a}$-multiplication $\alpha\colon A \to \sigma A$ such that $\alpha_0\colon A_0 \to A_0^{(q)}$ is the q-power Frobenius map; moreover, $\mathfrak{a} = N_\Phi(\mathfrak{p})$. For any m prime to p and such that $A_m(k) = A_m(\overline{\mathbb{Q}})$, the homomorphism α agrees with σ on $A_m(k)$ (because it does on $A_{0,m}(k_0) \simeq A_m(k)$).

Let σ' be a second element of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/E^*)$, and let $\alpha'\colon A \to \sigma' A$ be an $\mathfrak{a}'$-multiplication acting as σ' on A_m (which implies that its degree is prime to m). Then $\sigma\alpha'$ is again an $\mathfrak{a}'$-multiplication (obvious from the definition 7.17), and so $\sigma\alpha' \circ \alpha$ is an $\mathfrak{a}\mathfrak{a}'$-multiplication $A \to \sigma'\sigma A$ (see 7.26) acting as $\sigma'\sigma$ on A_m. Therefore, we have a homomorphism $\sigma \mapsto \mathfrak{a}(\sigma)\colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/E^*) \to C_m(E)$. This homomorphism factors through $\mathrm{Gal}(k/E^*)$ for some finite abelian extension k of E^*, which we may take to be the ray class field for a modulus $\mathfrak{m}$ of E^*. Thus, we obtain a well-defined homomorphism

$$C_{\mathfrak{m}}(E^*) \to C_m(E)$$

[24] Is it in fact necessary to assume that E is a CM-algebra in all of this? Later we need a polarization whose Rosati involution is complex conjugation on E, which implies that E is a CM-algebra.

[25] Here $A_m = \mathrm{Ker}(A \xrightarrow{m} A)$. It is an étale group scheme over $\overline{\mathbb{Q}}$, which can be identified with $A_m(\overline{\mathbb{Q}})$.

sending an ideal $\mathfrak{a}^*$ in $I^{S(\mathfrak{m})}(E^*)$ to the ideal of E associated with $\sigma = (\mathfrak{a}^*, k/E^*)$.

THEOREM 9.3 *The above homomorphism is that defined by N_{Φ}.*

PROOF. It suffices to verify this for a set of generators for $C_{\mathfrak{m}}(E^*)$. Let $k \subset \overline{\mathbb{Q}}$ be a field finite and Galois over E^*, containing the ray class field $E^*_{\mathfrak{m}}$, and such that A has a model over k with complex multiplication by E over k for which $A_m(k) = A_m(\overline{\mathbb{Q}})$. Then (9.2) shows that the two homomorphisms agree on the primes $\mathfrak{P} \cap \mathcal{O}_{E^*_{\mathfrak{m}}}$ where $\mathfrak{P}$ is a prime of k satisfying the conditions of (9.2). By Dirichlet's theorem on primes in arithmetic progressions (CFT V 2.5), the classes of these primes exhaust $C_{\mathfrak{m}}$. □

More preliminaries from algebraic number theory

We write art for the reciprocal reciprocity map, i.e., $\mathrm{art}_k(s) = \mathrm{rec}_k(s)^{-1}$ for $s \in \mathbb{A}_k^\times$. When k is totally imaginary, it factors through $\mathbb{A}_{f,k}^\times$, and we also write art_k for the map $\mathbb{A}_{f,k}^\times \to \mathrm{Gal}(k^{\mathrm{ab}}/k)$ that it defines; then

$$\mathrm{art}_k \colon \mathbb{A}_{f,k}^\times \to \mathrm{Gal}(k^{\mathrm{ab}}/k)$$

is surjective with kernel the closure of $k^\times$ (embedded diagonally) in $\mathbb{A}_{f,k}^\times$.

Let $\chi_{\mathrm{cyc}} \colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q}) \to \widehat{\mathbb{Z}}^\times$ be the cyclotomic character:

$$\sigma\zeta = \zeta^{\chi_{\mathrm{cyc}}(\sigma)}$$

for all roots ζ of 1 in $\mathbb{C}$.

LEMMA 9.4 *For any $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$,*

$$\mathrm{art}_{\mathbb{Q}}(\chi_{\mathrm{cyc}}(\sigma)) = \sigma|\mathbb{Q}^{\mathrm{ab}}.$$

PROOF. Exercise (see Milne 2005, §11 (50)). □

LEMMA 9.5 *Let E be a CM-field. For any $s \in \mathbb{A}_{f,E}^\times$,*

$$\mathrm{Nm}_{E/\mathbb{Q}}(s) \in \chi_{\mathrm{cyc}}(\mathrm{art}_k(s)) \cdot \mathbb{Q}_{>0}.$$

PROOF. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/E)$ be such that $\mathrm{art}_E(s) = \sigma|E^{\mathrm{ab}}$. Then

$$\mathrm{art}_{\mathbb{Q}}(\mathrm{Nm}_{E/\mathbb{Q}}(s)) = \sigma|\mathbb{Q}^{\mathrm{ab}}$$

by class field theory, and so

$$\mathrm{art}_{\mathbb{Q}}(\mathrm{Nm}_{E/\mathbb{Q}}(s)) = \mathrm{art}_{\mathbb{Q}}(\chi_{\mathrm{cyc}}(\sigma)).$$

The kernel of $\mathrm{art}_{\mathbb{Q}} \colon \mathbb{A}_f^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ is $\mathbb{A}_f^\times \cap (\mathbb{Q}^\times \cdot \mathbb{R}_{>0}) = \mathbb{Q}_{>0}$ (embedded diagonally). □

LEMMA 9.6 *For any CM-field E, the kernel of $\mathrm{art}_E \colon \mathbb{A}_{f,E}^\times / E^\times \to \mathrm{Gal}(E^{ab}/E)$ is uniquely divisible by all integers, and its elements are fixed by ι_E.*

PROOF. The kernel of art_E is $\overline{E^\times}/E^\times$ where $\overline{E^\times}$ is the closure of $E^\times$ in $\mathbb{A}_{f,E}^\times$. It is also equal to $\overline{U}/U$ for any subgroup U of $\mathcal{O}_E^\times$ of finite index. A theorem of Chevalley (see Serre 1964, 3.5) shows that $\mathbb{A}_{f,E}^\times$ induces the pro-finite topology on U. If we take U to be contained in the real subfield of E and torsion-free, then it is clear that $\overline{U}/U$ is fixed by ι_E and (being isomorphic to $(\widehat{\mathbb{Z}}/\mathbb{Z})^{[E:\mathbb{Q}]/2}$) uniquely divisible. □

LEMMA 9.7 *Let E be a CM-field and let Φ be a CM-type on E. For any $s \in \mathbb{A}_{f,E^*}^\times$,*

$$N_\Phi(s)\cdot \iota_E N_\Phi(s) \in \chi_{\mathrm{cyc}}(\mathrm{art}_{E^*}(s))\cdot \mathbb{Q}_{>0}.$$

PROOF. According to (10),

$$N_\Phi(s)\cdot \iota_E N_\Phi(s) = \mathrm{Nm}_{E^*/\mathbb{Q}}(s),$$

and so we can apply (9.5). □

LEMMA 9.8 *Let E be a CM-field and Φ a CM-type on E. There exists a unique homomorphism* $\mathrm{Gal}(E^{*\mathrm{ab}}/E^*) \to \mathrm{Gal}(E^{\mathrm{ab}}/E)$ *rendering*

$$\begin{array}{ccc} \mathbb{A}_{f,E^*}^\times & \xrightarrow{N_\Phi} & \mathbb{A}_{f,E}^\times \\ \downarrow{\scriptstyle \mathrm{art}_{E^*}} & & \downarrow{\scriptstyle \mathrm{art}_E} \\ \mathrm{Gal}(E^{*\mathrm{ab}}/E^*) & \longrightarrow & \mathrm{Gal}(E^{\mathrm{ab}}/E) \end{array}$$

commutative.

PROOF. As $\mathrm{art}_E\colon \mathbb{A}_{f,E}^\times \to \mathrm{Gal}(E^{\mathrm{ab}}/E)$ is surjective, the uniqueness is obvious. On the other hand, N_Φ maps $E^{*\times}$ into $E^\times$ and is continuous, and so it maps the closure of $E^{*\times}$ into the closure of $E^\times$. □

PROPOSITION 9.9 *Let $s, s' \in \mathbb{A}_{f,E^*}^\times$. If $\mathrm{art}_{E^*}(s) = \mathrm{art}_{E^*}(s')$, then $N_\Phi(s') \in N_\Phi(s)\cdot E^\times$.*

PROOF. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ be such that

$$\sigma|E^{\mathrm{ab}} = \mathrm{art}_{E^*}(s) = \mathrm{art}_{E^*}(s').$$

Then (see 9.5),

$$N_\Phi(s)\cdot \iota_E N_\Phi(s) = \chi_{\mathrm{cyc}}(\sigma)\cdot E^\times = N_\Phi(s')\cdot \iota_E N_\Phi(s').$$

Let $t = N_\Phi(s)/N_\Phi(s') \in \mathbb{A}_{f,E}^\times$. Then $t \in \mathrm{Ker}(\mathrm{art}_E)$ and $t\cdot \iota_E t \in E^\times$. As the map $x \mapsto x\cdot \iota_E x$ is bijective on $\mathrm{Ker}(\mathrm{art}_E)/E^\times$ (see 9.6), this shows that $t \in E^\times$. □

The fundamental theorem in terms of idèles

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and let A be an abelian variety with complex multiplication by a CM-algebra E over $\overline{\mathbb{Q}}$. Let $\Phi \subset \mathrm{Hom}(E, \overline{\mathbb{Q}})$ be the type of A.

Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$. Because σ fixes E^*, there exists an E-isogeny $\alpha\colon A \to \sigma A$ (see 3.12). The maps

$$x \mapsto \sigma x,\ x \mapsto \alpha x\colon V_f(A) \to V_f(\sigma A)$$

are both $\mathbb{A}_{f,E} \stackrel{\text{def}}{=} E \otimes \mathbb{A}_f$-linear isomorphisms. As $V_f(A)$ is free of rank one over $\mathbb{A}_{f,E}$,[26] they differ by a homothety by an element $\eta(\sigma)$ of $\mathbb{A}_{f,E}^\times$:

$$\alpha(\eta(\sigma)x) = \sigma x, \quad \text{all } x \in V_f(A). \tag{64}$$

When the choice of α is changed, $\eta(\sigma)$ is changed only by an element of $E^\times$, and so we have a well-defined map

$$\eta\colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/E^*) \to \mathbb{A}_{f,E}^\times/E^\times. \tag{65}$$

The content of the next theorem, is that $\eta(\sigma)$ equals $N_{\boldsymbol{\Phi}}(s) \mod E^\times$ for any $s \in \mathbb{A}_{f,E^*}^\times$ with $\mathrm{art}_{E^*}(s) = \sigma|E^{*\mathrm{ab}}$.

THEOREM 9.10 *Let A be an abelian variety with complex multiplication by a CM-algebra E over $\overline{\mathbb{Q}}$, and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$. For any $s \in \mathbb{A}_{f,E^*}^\times$ with $\mathrm{art}_{E^*}(s) = \sigma|E^{*\mathrm{ab}}$, there is a unique E-"isogeny" $\alpha\colon A \to \sigma A$ such that $\alpha(N_{\boldsymbol{\Phi}}(s)\cdot x) = \sigma x$ for all $x \in V_f A$.*

REMARK 9.11 (a) It is obvious that α is determined uniquely by the choice of $s \in \mathbb{A}_{f,E}^\times$ such that $\mathrm{rec}(s) = \sigma|E^{*\mathrm{ab}}$. If s is replaced by s', then $N_{\boldsymbol{\Phi}}(s') = a \cdot N_{\boldsymbol{\Phi}}(s)$ with $a \in E^\times$ (see 9.9), and α must be replaced by $\alpha \cdot a^{-1}$.

(b) The theorem is a statement about the E-"isogeny" class of A — if $\beta\colon A \to B$ is an E-"isogeny", and α satisfies the conditions of the theorem for A, then $\sigma\beta\circ\alpha\circ\beta^{-1}$ satisfies the conditions for B.

(c) Let α as in the theorem, let λ be a polarization of A whose Rosati involution induces ι_E on E, and let $\psi\colon V_f A \times V_f A \to \mathbb{A}_f(1)$ be the Riemann form of λ. Then, for $x, y \in V_f A$,

$$(\sigma\psi)(\sigma x, \sigma y) \stackrel{\text{def}}{=} \sigma(\psi(x,y)) = \chi_{\mathrm{cyc}}(\sigma)\cdot\psi(x,y)$$

because $\psi(x,y) \in \mathbb{A}_f(1)$. Thus if α is as in the theorem, then

$$\chi_{\mathrm{cyc}}(\sigma)\cdot\psi(x,y) = (\sigma\psi)(N_{\boldsymbol{\Phi}}(s)\alpha(x), N_{\boldsymbol{\Phi}}(s)\alpha(y)) = (\sigma\psi)(N_{\boldsymbol{\Phi}}(s)\overline{N_{\boldsymbol{\Phi}}(s)}\alpha(x), \alpha(y))$$

and so

$$(c\psi)(x,y) = (\sigma\psi)(\alpha x, \alpha y),$$

with $c = \chi_{\mathrm{cyc}}(\sigma)/N_{E^*/\mathbb{Q}}(s) \in \mathbb{Q}^\times$ (see 9.5).

Let T^{E^*} and T^E be the algebraic tori over $\mathbb{Q}$ with $\mathbb{Q}$-points $E^{*\times}$ and $E^\times$ respectively. The norm $a \mapsto a\cdot\iota_E a$ defines a homomorphism $T^E \to T^F$, and we define T to be the fibre product $T = \mathbb{G}_m \times_{T^F} T^E$:

$$\begin{array}{ccc} T & \longrightarrow & T^E \\ \downarrow & & \downarrow \\ \mathbb{G}_m & \longrightarrow & T^F. \end{array} \tag{66}$$

We begin with two easy lemmas.

[26] Let $R = \mathrm{End}(A) \cap E$. For all ℓ, $V_\ell A$ is free of rank one over $E_\ell \stackrel{\text{def}}{=} E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, and for all ℓ not dividing $(\mathcal{O}_E\colon R)$, $T_\ell A$ is free of rank one over $R_\ell \stackrel{\text{def}}{=} R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ (see 7.6).

LEMMA 9.12 *The map*

$$T(\mathbb{A}_f)/T(\mathbb{Q}) \to T^E(\mathbb{A}_f)/T^E(\mathbb{Q}) = \mathbb{A}_{f,E}^\times/E^\times$$

defined by the homomorphism $T \to T^E$ is injective, and realizes the first group as a topological subspace of the second.

PROOF. Let $a \in T(\mathbb{A}_f)$ map to $b \in T^E(\mathbb{Q})$. To lie in $T(\mathbb{Q})$, b must satisfy a polynomial equation. Because it satisfies this equation in $\mathbb{A}_f$, it satisfies it in $\mathbb{Q} \subset \mathbb{A}_f$.

That $T(\mathbb{A}_f)/T(\mathbb{Q})$ is a topological subspace of $T^E(\mathbb{A}_f)/T^E(\mathbb{Q})$ is obvious: $T(\mathbb{A}_f)$ is certainly a topological subspace of $T^E(\mathbb{A}_f)$, and $T(\mathbb{A}_f)/T(\mathbb{Q})$ and $T^E(\mathbb{A}_f)/T^E(\mathbb{Q})$ are both endowed with the quotient topology. □

LEMMA 9.13 *The space $T(\mathbb{A}_f)/T(\mathbb{Q})$ is Hausdorff.*

PROOF. In fact, $T(\mathbb{Q})$ is even discrete in $T(\mathbb{A}_f)$. Note that $T(\mathbb{Q}) \cap \mathcal{O}_E^\times$, being equal to $T(\mathbb{Q}) \cap \prod_{v \text{ finite}} \mathcal{O}_{E,v}^\times$, is open in $T(\mathbb{Q})$. Moreover, it contains $T(\mathbb{Q}) \cap \mathcal{O}_F^\times$ as a subgroup of finite index. But

$$T(\mathbb{Q}) \cap \mathcal{O}_F^\times = \{a \in \mathcal{O}_F^\times \mid a^2 = \pm 1\}$$

is finite, and so $T(\mathbb{Q}) \cap \mathcal{O}_E^\times$ is finite and open in $T(\mathbb{Q})$. It follows easy that easily that $T(\mathbb{Q})$ is discrete in $T(\mathbb{A}_f)$. In particular, it is closed (Hewitt and Ross 1963, II 5.10). □

Thus, elements a, b of $T(\mathbb{A}_f)/T(\mathbb{Q})$ are equal if $a \in bU$ for all open neighbourhoods U of 1 in $\mathbb{A}_{f,E}^\times/E^\times$.[27]

LEMMA 9.14 *Let $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$. Let s be an element of $\mathbb{A}_{f,E^*}^\times$ such that $\mathrm{art}_{E^*}(s) = \sigma|E^{*\mathrm{ab}}$, and let $\eta(\sigma)$ be an element of $\mathbb{A}_{f,E}^\times$ such that (64) holds for some E-"isogeny" $\alpha\colon A \to \sigma A$. Then $\eta(\sigma)/N_\Phi(s) \mod E^\times$ lies in the subgroup $T(\mathbb{A}_f)/T(\mathbb{Q})$ of $\mathbb{A}_{f,E}^\times/E^\times$.*

PROOF. We know that

$$N_\Phi(s) \cdot \iota_E N_\Phi(s) \overset{(1.24)}{=} \mathrm{Nm}_{\mathbb{A}_{f,E^*}/\mathbb{A}_f}(s) \overset{(9.5)}{=} \chi_{\mathrm{cyc}}(\sigma) \cdot a$$

for some $a \in \mathbb{Q}_{>0}$.

A calculation as in (9.11c) shows that,

$$(c\psi)(x, y) = (\sigma\psi)(\alpha x, \alpha y), \text{ all } x, y \in \mathbb{A}_{f,E}^\times, \tag{67}$$

with $c = \chi_{\mathrm{cyc}}(\sigma)/(\eta(\sigma) \cdot \iota_E \eta(\sigma))$. But it follows from the last paragraph of (2.9) that (67) holds with c a totally positive element of F. Thus

$$\eta(\sigma) \cdot \overline{\eta(\sigma)} = \chi_{\mathrm{cyc}}(\sigma)/c, \quad c \in F_{\gg 0}, \tag{68}$$

where $\overline{\eta(\sigma)} = \iota_E \eta(\sigma)$.

Let $t = \eta(\sigma)/N_\Phi(s)$. Then

$$t\bar{t} = 1/ac \in F_{\gg 0}. \tag{69}$$

Being a totally positive element of F, ac is a local norm from E at the infinite primes, and (69) shows that it is also a local norm at the finite primes. Therefore we can write $ac = e\bar{e}$ for some $e \in E^\times$. Then

$$te \cdot \overline{te} = 1.$$

Thus, $te \in T(\mathbb{A}_f)$, and it represents $t \cdot E^\times$ in $\mathbb{A}_{f,E}^\times/E^\times$. □

[27] Because then $b^{-1}a$ lies in all open neighbourhoods of 1 in $T(\mathbb{A}_f)/T(\mathbb{Q})$.

Note that (1.24) shows that $N_\Phi(s) \in T(\mathbb{A}_f)$, and so the map $\eta\colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/E^*) \to \mathbb{A}_{f,E}^\times/E^\times$ in (65) takes values in the Hausdorff subgroup $T(\mathbb{A}_f)/T(\mathbb{Q})$ of $\mathbb{A}_{f,E}^\times/E^\times$. It is a homomorphism[28], and so it factors through $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/E^*)^{\mathrm{ab}}$. When combined with the Artin map, it gives a homomorphism $\eta'\colon \mathbb{A}_{f,E^*}^\times/E^{*\times} \to \mathbb{A}_{f,E}^\times/E^\times$.

In order to prove Theorem 9.10, it remains to show $N_\Phi(s) \in \eta'(s)U$ for all open neighbourhoods U of 1 in $\mathbb{A}_{f,E}^\times/E^\times$. Choose an integer $m > 0$. For some modulus $\mathfrak{m}$, there exists a commutative diagram

$$\begin{array}{ccc} \mathbb{A}_{f,E^*}^\times/E^{*\times} & \longrightarrow & \mathbb{A}_{f,E}^\times/E^\times \\ \big\downarrow \text{onto} & & \big\downarrow \text{onto} \\ C_{\mathfrak{m}}(E^*) & \longrightarrow & C_m(E) \end{array}$$

in which the vertical maps are given by class field theory (CFT 4.6) and the horizontal maps are given either by N_Φ or by η'. On the bottom row, these maps agree by Theorem 9.3, which implies that they agree on the top row, because the kernels of the homomorphisms $\mathbb{A}_{f,E}^\times/E^\times \to C_m(E)$, as m runs over the positive integers, form a basis for the open neighbourhoods of 1 in $\mathbb{A}_{f,E}^\times/E^\times$ (cf. CFT 4.6).

REMARK 9.15 Theorem 9.10 holds with $\overline{\mathbb{Q}}$ replaced by $\mathbb{C}$, and σ taken to be any automorphism of $\mathbb{C}$ fixing E^*. This follows immediately from the theorem because of (7.10).

EXERCISE 9.16 Rearrange the proof by first showing that the two homomorphisms $\mathrm{Gal}(E^{*\mathrm{ab}}/E^*) \to \mathbb{A}_{f,E}^\times/\overline{E}^\times$ agree; then use the polarization to obtain the stronger result.

The fundamental theorem in terms of uniformizations

Let $(A, i\colon E \hookrightarrow \mathrm{End}^0(A))$ be an abelian variety with complex multiplication over $\mathbb{C}$, and let λ be a polarization of (A, i). Recall (3.11, 3.17) that the choice of a basis element e_0 for $H_0(A, \mathbb{Q})$ determines a uniformization $\theta\colon \mathbb{C}^\Phi \to A(\mathbb{C})$, and hence a quadruple $(E, \Phi; \mathfrak{a}, t)$, called the type of (A, i, λ) relative to θ.

THEOREM 9.17 *Let (A, i, λ) be of type $(E, \Phi; \mathfrak{a}, t)$ relative to a uniformization $\theta\colon \mathbb{C}^\Phi \to A(\mathbb{C})$, and let σ be an automorphism of $\mathbb{C}$ fixing E^*. For any $s \in \mathbb{A}_{f,E^*}^\times$ such that $\mathrm{art}_{E^*}(s) = \sigma|E^{*ab}$, there is a unique uniformization $\theta'\colon \mathbb{C}^{\Phi'} \to (\sigma A)(\mathbb{C})$ of σA such that*

(a) *$\sigma(A, i, \psi)$ has type $(E, \Phi; f\mathfrak{a}, t \cdot \chi_{\mathrm{cyc}}(\sigma)/f\overline{f})$ where $f = N_\Phi(s) \in \mathbb{A}_{f,E}^\times$;*

[28]Choose E-isogenies $\alpha\colon A \to \sigma A$ and $\alpha'\colon A \to \sigma' A'$, and let

$$\begin{aligned} \alpha(sx) &= \sigma x \\ \alpha'(s'x) &= \sigma' x. \end{aligned}$$

Then $\sigma\alpha' \circ \alpha$ is an isogeny $A \to \sigma\sigma' A$, and

$$\begin{aligned} (\sigma\alpha' \circ \alpha)(ss'x) &= (\sigma\alpha')(\alpha(ss'x)) \\ &= (\sigma\alpha')(\sigma(s'x)) \\ &= \sigma(\alpha'(s'x)) \\ &= \sigma\sigma' x. \end{aligned}$$

(b) *the diagram*

$$\begin{array}{ccc} E/\mathfrak{a} & \xrightarrow{\theta_0} & A(\mathbb{C}) \\ \downarrow f & & \downarrow \sigma \\ E/f\mathfrak{a} & \xrightarrow{\theta_0'} & \sigma A(\mathbb{C}) \end{array}$$

commutes, where $\theta_0(x) = \theta((\varphi x)_{\varphi\in\Phi})$ *and* $\theta_0'(x) = \theta'((\varphi x)_{\varphi\in\Phi'})$.

PROOF. According to Theorem 9.10, there exists an isogeny $\alpha\colon A \to \sigma A$ such that $\alpha(N_\Phi(s)\cdot x) = \sigma x$ for all $x \in V_f A$. Then $H_1(\alpha)$ is an E-linear isomorphism $H_1(A,\mathbb{Q}) \to H_1(\sigma A,\mathbb{Q})$, and we let θ' be the uniformization defined by the basis element $H_1(\alpha)(e_0)$ for $H_1(\sigma A,\mathbb{Q})$. The statement now follows immediately from Theorem 9.10 and (9.11c).□

The fundamental theorem in terms of moduli

REVIEW OF THE SETTING

Recall that $\mathbb{S}$ is the real torus with $\mathbb{S}(\mathbb{R}) = \mathbb{C}^\times$. There are characters z and $\overline{z}$ of $\mathbb{S}$ inducing the maps $z \mapsto z$ and $z \mapsto \overline{z}$ respectively on the real points of $\mathbb{S}$,

$$\mathbb{C}^\times = \mathbb{S}(\mathbb{R}) \subset \mathbb{S}(\mathbb{C}) \rightrightarrows \mathbb{G}_m(\mathbb{C}) = \mathbb{C}^\times.$$

Let μ be the cocharacter of $\mathbb{S}$ such that

$$\begin{cases} z\circ\mu &= \mathrm{id}_{\mathbb{G}_m} \\ \overline{z}\circ\mu &= 1 \end{cases}.$$

The characters $z, \overline{z}$ of $\mathbb{S}$ define an isomorphism

$$\mathbb{S}_{\mathbb{C}} \xrightarrow{(z,\overline{z})} \mathbb{G}_m \times \mathbb{G}_m \tag{70}$$

and μ is the cocharacter of $\mathbb{S}_{\mathbb{C}}$ such that $\mu(x)$ maps to $(x,1)$ in $\mathbb{G}_m \times \mathbb{G}_m$.

Let (E,Φ) be a CM-pair, and let $T^E = (\mathbb{G}_m)_{E/\mathbb{Q}}$. As noted in §1, Φ defines an isomorphism $E\otimes_{\mathbb{Q}}\mathbb{R} \to \prod_{\varphi\in\Phi}\mathbb{C}$, and hence an isomorphism[29]

$$T^E_{\mathbb{R}} \simeq \mathbb{S}^\Phi. \tag{71}$$

Define

$$h_\Phi\colon \mathbb{S} \to T^E_{\mathbb{R}}$$

to be the homomorphism whose composite with (71) is

$$z \mapsto (z,\dots,z).$$

The isomorphism $E\otimes_{\mathbb{Q}}\mathbb{C} \simeq \prod_{\varphi\in I}\mathbb{C}$, $I = \mathrm{Hom}(E,\mathbb{C})$, defines an isomorphism

$$T^E_{\mathbb{C}} \simeq (\mathbb{G}_m)^I.$$

The cocharacter

$$\mu_\Phi \overset{\text{def}}{=} h_\Phi\circ\mu\colon \mathbb{G}_{m\mathbb{C}} \to T^E_{\mathbb{C}}$$

[29]By $\mathbb{S}^\Phi$ we mean a product of copies of $\mathbb{S}$ indexed by Φ.

corresponding to h_Φ satisfies

$$\mu_\Phi(z)_\varphi = \begin{cases} z & \text{if} \quad \varphi \in \Phi \\ 1 & \text{if} \quad \varphi \notin \Phi. \end{cases}$$

Recall that the reflex field E^* of (E, Φ) is the subfield of $\mathbb{C}$ generated by the elements

$$\sum\nolimits_{\varphi\in\Phi} \varphi(a), \quad a \in E.$$

It can also be described as the field of definition of μ_Φ.

We are interested in abelian varieties A of CM-type (E, Φ) over fields k containing E^*. Recall that this means that there is given a homomorphism $i\colon E \to \mathrm{End}^0(A)$ such that

$$\mathrm{Tr}(i(a)|\,\mathrm{Tgt}_0(A)) = \sum\nolimits_{\varphi\in\Phi} \varphi(a), \text{ all } a \in E, \tag{72}$$

(equality of elements of k).

STATEMENT AND PROOF

Let (E, Φ) be a CM-pair, and let $T = \mathrm{Ker}(T^E \to T^F/\mathbb{G}_m)$ as in (66). Let V be a one-dimensional E-vector space. Note that T^E acts on V, and $(V, h_\Phi(i))$ is the rational Riemann pair attached to (E, Φ) (cf. 2.5). Let ψ be a rational Riemann form on $(V, h_\Phi(i))$ (cf. 2.9). Thus, ψ is an alternating form $V \times V \to \mathbb{Q}$ such that $(x, y) \mapsto \psi(x, h_\Phi(i)y)$ is a positive definite symmetric form on $V \otimes \mathbb{R}$. Note that T is the subtorus of $\mathrm{GL}(V)$ such that

$$T(R) = \{\alpha \in \mathrm{GL}_{R\otimes_{\mathbb{Q}}E}(V) \mid \exists \mu(\alpha) \in R^\times \text{ such that } \psi(\alpha x, \alpha y) = \mu(\alpha)\psi(x, y)\} \tag{73}$$

for all $\mathbb{Q}$-algebras R.

PROPOSITION 9.18 *For any compact open subgroup K of $T(\mathbb{A}_f)$, the set $T(\mathbb{Q})\backslash T(\mathbb{A}_f)/K$ classifies the isomorphism classes of quadruples $(A, j, \lambda, \eta K)$ in which*

- $\diamond$ A is a complex abelian variety,
- $\diamond$ λ is a polarization of A,
- $\diamond$ j is a homomorphism $E \to \mathrm{End}^0(A)$, and
- $\diamond$ ηK is a K-orbit of E-linear isomorphisms $\eta\colon V(\mathbb{A}_f) \to V_f(A)$ sending ψ to an $\mathbb{A}_f^\times$-multiple of ψ_λ

satisfying the following condition:

> (*) there exists an E-linear isomorphism $a\colon H_1(A, \mathbb{Q}) \to V$ sending ψ_λ to a $\mathbb{Q}^\times$-multiple of ψ.

An isomorphism from one quadruple $(A, j, \lambda, \eta K)$ to a second $(A', j', \lambda', \eta' K)$ is an E-"isogeny" sending λ to a $\mathbb{Q}^\times$-multiple of λ' and η to η' modulo K.

PROOF. Choose an isomorphism $a\colon H_1(A, \mathbb{Q}) \to V$ as in (*), and consider[30]

$$V(\mathbb{A}_f) \xrightarrow{\eta} V_f(A) \xrightarrow{a} V(\mathbb{A}_f).$$

[30]Recall that $V_f A \simeq H_1(A, \mathbb{Q}) \otimes \mathbb{A}_f$.

Then $a \circ \eta$ satisfies (73) with $R = \mathbb{A}_f$, and so $a \circ \eta \in T(\mathbb{A}_f)$. The isomorphism a is determined up to composition with an element of $T(\mathbb{Q})$, and η is determined up to composition with an element of K. Therefore, the class of $a \circ \eta$ in $T(\mathbb{Q})\backslash T(\mathbb{A}_f)/K$ is well-defined. It remains to show that the map $(A, j, \lambda, \eta K) \mapsto [a \circ \eta]$ is surjective and that its fibres are the isomorphism classes, but this is routine. □

THEOREM 9.19 *Let σ be an automorphism of $\mathbb{C}$ fixing E^*. If $(A, j, \lambda, \eta K)$ satisfies (*), then so also does $\sigma(A, j, \lambda, \eta K)$. Moreover, the isomorphism class of $\sigma(A, j, \lambda, \eta K)$ depends only on $\sigma|E^{*\mathrm{ab}}$. For any $s \in \mathbb{A}_{f,E^*}^\times$ such that $\mathrm{art}_{E^*}(s) = \sigma|E^{*\mathrm{ab}}$,*

$$\sigma(A, j, \lambda, \eta K) \approx (A, j, \lambda, \eta f K) \text{ where } f = N_{\Phi}(s).$$

PROOF. This follows immediately from (9.10) and (9.11c). □

REMARK 9.20 Let $\mathcal{M}$ be the set of isomorphism classes quadruples satisfying (*). Proposition 9.18 says that

$$\mathcal{M} \simeq T(\mathbb{Q})\backslash T(\mathbb{A}_f)/K.$$

Theorem 9.19 says that this isomorphism is equivariant for the following action of $\mathrm{Aut}(\mathbb{C}/E^*)$ on the right hand side: for $\sigma \in \mathrm{Aut}(\mathbb{C}/E^*)$, choose an $s \in \mathbb{A}_{f,E^*}^\times$ such that $\mathrm{art}_{E^*}(s) = \sigma|E^{*\mathrm{ab}}$; then, for $a \in T(\mathbb{A}_f)$, $\sigma[a] = [N_{\Phi}(s) \cdot a]$.

REMARK 9.21 In both Proposition 9.18 and Theorem 9.19, it is possible to replace $\mathbb{C}$ with $\mathbb{Q}^{\mathrm{al}}$ (apply 7.10).

Alternative approach using crystals (Deligne c1968)

In a handwritten manuscript (Deligne nd), Deligne showed how to derive the Shimura-Taniyama formula, as well as the fundamental theorem over the reflex field, from the theory of canonical liftings of abelian varieties. The remainder of this section is based on his manuscript. [There may be some sign problems here.]

REVIEW OF THE CRYSTALS ATTACHED TO AN ABELIAN SCHEME

Let A be an abelian scheme of relative dimension g over $W(\mathbb{F}_q)$, the ring of Witt vectors with entries in $\mathbb{F}_q$. To avoid possible problems, we assume $p \neq 2$. We are interested in the crystalline H_1 of A (alias, Dieudonné module).

9.22 Attached to $A_0 \overset{\text{def}}{=} A \bmod p$, there are the following objects.

(a) A free $W(\mathbb{F}_q)$-module $M = M(A_0)$ of rank $2g$ (the crystalline H_1 of A_0, alias the covariant Dieudonné module).

(b) Let σ be the automorphism of $W(\mathbb{F}_q)$ lifting the q-power Frobenius automorphism on $\mathbb{F}_q$, and consider the standard diagram

$$\begin{array}{ccccc} A_0 & \xrightarrow{\text{Frob}} & A_0^{(p)} & \longrightarrow & A_0 \\ & \searrow & \downarrow & & \downarrow \\ & & \operatorname{Spec}\mathbb{F}_q & \xrightarrow{x\mapsto x^q} & \operatorname{Spec}\mathbb{F}_q. \end{array}$$

Then

$$M(A_0^{(p)}) = M \otimes_{W(\mathbb{F}_q),\sigma} W(\mathbb{F}_q) \overset{\text{def}}{=} M^{\sigma^{-1}}.$$

Note that $M^{\sigma^{-1}}$ can be identified with M but with $w \in W(\mathbb{F}_q)$ acting according to the rule

$$w \cdot m = \sigma^{-1}(w) \cdot m.$$

Because M is a covariant functor, there is a $W(\mathbb{F}_q)$-linear map

$$F = M(\text{Frob}): M \to M^{\sigma^{-1}}.$$

(c) Moreover,

$$M/pM = M \otimes_{W(\mathbb{F}_q)} \mathbb{F}_q \simeq \left(H^1_{\text{dR}}(A_0)\right)^\vee \stackrel{\text{def}}{=} H_1^{\text{dR}}(A_0),$$

and hence there is a filtration on M/pM

$$M/pM = F^{-1} \supset F^0 \supset F^1 = 0,$$

dual to the Hodge filtration on $H^1_{\text{dR}}(A_0)$. Here $F^{-1}/F^0 = \text{Tgt}_0(A)$, and so

$$F(M/pM) \subset F^0(M/pM)^{\sigma^{-1}}. \tag{74}$$

(d) There exists a $W(\mathbb{F}_q)$-linear map $V: M^{\sigma^{-1}} \to M$ such that $FV = VF = p$ (because we are considering H_1).

9.23 Attached to A, there is an isomorphism of M with the de Rham homology of $A/W(\mathbb{F}_q)$

$$M \simeq \left(H^1_{\text{dR}}(A)\right)^\vee$$

which is compatible with the isomorphism $M/pM \simeq \left(H^1_{\text{dR}}(A_0)\right)^\vee$ in (9.22c). In particular, there is a filtration on M,

$$M = F^{-1} \supset F^0 \supset F^1 = 0,$$

dual to the Hodge filtration on $H^1_{\text{dR}}(A)$.

APPLICATION TO ABELIAN VARIETIES WITH COMPLEX MULTIPLICATION

Let A be an abelian scheme over $W(\mathbb{F}_q)$, as in the last subsubsection. Assume that the general fibre A_1 of A over $B(\mathbb{F}_q)$ has complex multiplication by the CM-algebra E, and let Φ be its CM-type. Thus

$$\text{Tr}(a|\,\text{Tgt}_0(A)) = \sum\nolimits_{\varphi\in\Phi} \varphi(a), \text{ all } a \in E, \tag{75}$$

(equality of elements of $B(\mathbb{F}_q)$), and E^* is the subfield of $B(\mathbb{F}_q)$ generated by these elements.[31]

Let (M, F) be as in (9.23). The algebra E acts on

$$M[\tfrac{1}{p}] \stackrel{\text{def}}{=} M \otimes_{W(\mathbb{F}_q)} B(\mathbb{F}_q) \simeq H_1^{\text{dR}}(A_1).$$

[31] Note that we get this situation when we start with an abelian variety A with complex multiplication by E over a number field k and a prime ideal $\mathfrak{P}$ in k that is unramified over $(p) \stackrel{\text{def}}{=} \mathbb{Z} \cap \mathfrak{P}$ and at which A has good reduction.

Over E^*, and a fortiori over $B(\mathbb{F}_q)$, we have a homomorphism $\mu_\Phi\colon \mathbb{G}_m \to T^E$, and hence a homomorphism

$$\mu_\Phi\colon B(\mathbb{F}_q)^\times \to (E\otimes_{\mathbb{Q}} B(\mathbb{F}_q))^\times.$$

The module $M[\frac{1}{p}]$ is free of rank one over $E\otimes_{\mathbb{Q}} B(\mathbb{F}_q)$. It follows from (75) that there is a decomposition

$$M[\tfrac{1}{p}] = M[\tfrac{1}{p}]^{-1,0}\oplus M[\tfrac{1}{p}]^{0,-1} \tag{76}$$

such that

$$\begin{cases} \mu_\Phi(x) \text{ acts on } M^{-r,-s} \text{ as multiplication by } x^r, \\ M^{0,-1} = F^0(M[\frac{1}{p}]). \end{cases}$$

Let $\mathcal{O}^A = \mathrm{End}(A)\cap E$, and let $\mathcal{O}^A_p = \mathcal{O}^A\otimes_{\mathbb{Z}}\mathbb{Z}_p$. If $\mu_\Phi(p)\in \mathcal{O}^A_p\otimes W(\mathbb{F}_q)$, for example, if $\mathcal{O}^A$ is maximal at p, then (76) gives[32]

$$M = M^{-1,0}\oplus M^{0,-1},\quad M^{r,s}\stackrel{\text{def}}{=} M\cap M[\tfrac{1}{p}]^{r,s}. \tag{77}$$

PROPOSITION 9.24 *Suppose that*
(a) $\mu_\Phi(p)\in \mathcal{O}^A_p\otimes W(\mathbb{F}_q)$
(b) *the residue field of* $E^*\subset B(\mathbb{F}_q)$ *is* $\mathbb{F}_p$.
Then A_0 *is ordinary, and* A *is the canonical lifting of* A_s

PROOF. From (b) we have that

$$E^* = B(\mathbb{F}_p)\subset B(\mathbb{F}_q),$$

and so μ_Φ defines a homomorphism

$$\mu_\Phi\colon B(\mathbb{F}_p)^\times \to (E\otimes_{\mathbb{Q}} B(\mathbb{F}_p))^\times.$$

The decomposition (77), which exists because of (a), is compatible with F because the action of E (contrary to that of $E\otimes_{\mathbb{Q}} B(\mathbb{F}_q)$) commutes with F. From (74), we find that

$$F(M^{-1,0})\subset p(M^{-1,0})^{\sigma^{-1}}$$
$$F^n(M^{-1,0})\subset q(M^{-1,0}).$$

We have written $q = p^n$, so that F^n is the q-power Frobenius endomorphism of A_0. Therefore, the p-adic valuations of half of the eigenvalues of the Frobenius are $\geq n$, which implies A_0 is ordinary, and

$$\begin{cases} F(M^{-1,0}) &= p(M^{-1,0})^{\sigma^{-1}} \\ F(M^{0,-1}) &= (M^{0,-1})^{\sigma^{-1}}. \end{cases} \tag{78}$$

The decomposition (77) corresponds to a decomposition of $T_p(A)$, which, by (78), shows that A is the canonical lifting of A_0. □

One pulls also from (4), under the hypothesis (a,b) of Proposition 1

[32]Let $x\in M[\frac{1}{p}]$ decompose into $x = x_0 + x_1$ with $x_0\in M[\frac{1}{p}]^{0,-1}$ and $x_1\in M[\frac{1}{p}]^{-1,0}$, and set $\alpha = \mu(p)$. Then $\alpha^r x = x_0 + p^r x_1$, and so, if $x\in M$, then $\alpha^r x\to x_0$ as $r\to\infty$ which implies that $x_0\in M\cap M[\frac{1}{p}]^{0,-1} = M^{0,-1}$. Therefore also $x_1 = x - x_0\in M\cap M[\frac{1}{p}]^{-1,0} = M^{-1,0}$.

COROLLARY 9.25 *Under the hypotheses (a,b) of Proposition 9.24, the canonical lifting of $A^{(p)}$ is the abelian variety p-isogenous to A with the "Dieudonné module"*

$$M(A^{(p)}) = \mu_{\Phi}(p) \cdot M(A).$$

PROOF. Follows from (78). □

REMARK 9.26 The converse of Proposition 9.24 is true.

MODULI

We now let (E, Φ) be a CM-pair with $\Phi \subset \mathrm{Hom}(E, \mathbb{C})$ (so that now $E^* \subset \mathbb{C}$). Let k be a finite Galois extension of E^* with Galois group G. Let V be a free E-module of rank 1, and $V_{\mathbb{Z}}$ be a lattice in V stable under $\mathcal{O}_E$. Let K be a compact open subgroup of $\mathbb{A}_{E,f}^{\times}$ that leaves $V_{\widehat{\mathbb{Z}}} \overset{\text{def}}{=} V_{\mathbb{Z}} \otimes \widehat{\mathbb{Z}}$ invariant.

When B is an abelian variety, we write $B \otimes \mathbb{Q}$ for the abelian variety up to isogeny underlying it; put

$$\widehat{T}(B) = \prod\nolimits_{\ell} T_{\ell}(B),$$
$$\widehat{V}(B \otimes \mathbb{Q}) = \widehat{T}(B) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Note that B is determined by the pair $(B \otimes \mathbb{Q}, \widehat{T}(B) \subset \widehat{V}(B \otimes \mathbb{Q}))$.

Let ${}_K M(k)$, or simply M, be the set of *geometric* isomorphism classes ($\alpha \sim \beta$ if α is isomorphic to β after an extension of scalars) of objects $(A, \lambda, \overline{\eta})$ consisting of

- ◇ an abelian variety up to isogeny A/k, with complex multiplication by E satisfying (72);
- ◇ a polarization λ of A (i.e., an isogeny $\lambda\colon A \to A^{\vee}$ defined by an ample line bundle);
- ◇ a class mod K, $\overline{\eta}$, of E-linear isomorphisms.

$$\eta\colon V \otimes_{\mathbb{Q}} \mathbb{A}_f \to \widehat{V}(A)$$

Thus, for any $\eta \in \overline{\eta}$, $\overline{\eta} = \eta K$. We require the *class* to be defined over k, not its elements.

Denote by $A^{\overline{\eta}}$ the abelian variety endowed with an isomorphism $A^{\overline{\eta}} \otimes \mathbb{Q} \to A \otimes \mathbb{Q}$ such that

$$\widehat{T}(A^{\overline{\eta}}) = \eta(V_{\widehat{\mathbb{Z}}})$$

(the right hand side is independent of $\eta \in \overline{\eta}$). It has complex multiplication by $\mathcal{O}_E$.

The group $\mathbb{A}_E^{\times}$ acts on M (through its quotient $\mathbb{A}_{E,f}^{\times}$) according to the rule:

$$(A, \lambda, \overline{\eta}) \cdot a = (A, \lambda, \overline{\eta}a), \quad a \in \mathbb{A}_{E,f}^{\times}.$$

Let $F \subset E$ be a product of the largest totally real subfields of the factors of E. Then $c \in F^{\times}$ acts on M according to the rule:

$$c \cdot (A, \lambda, \overline{\eta}) = (A, c\lambda, c\overline{\eta})$$

where

$$c\lambda = \lambda \circ c = c^{\dagger} \circ \lambda\colon A \to A^{\vee}.$$

The Galois group G acts on M and commutes with the actions of $\mathbb{A}_{E,f}^{\times}$ and $F^{\times}$. The commutative group $F^{\times} \times \mathbb{A}_{E,f}^{\times}$ acts transitively on M, and so G acts through its largest abelian quotient G^{ab}.

Denote by $[A, \lambda, \overline{\eta}] \in M$ the geometric isomorphism class of $(A, \lambda, \overline{\eta})$. The set of primes of E^* that are unramified and have degree 1 (i.e., have residue field the prime field) has density 1. In order to calculate the action of G^{ab} on M, it suffices therefore to calculate

$$\sigma_v([A, \lambda, \overline{\eta}]) \qquad (\sigma_v \text{ the Frobenius map at } v)$$

for the primes v of E^* such that

(a) $E_v^* = \mathbb{Q}_p$ (p the residue characteristic at v);
(b) $p \neq 2$ and v is unramified in E;
(c) $K \supset (\mathcal{O}_{E,p})^{\times}$;
(d) $A^{\overline{\eta}}$ has good reduction at the primes of k above the v.

We now fix such a v.

Since we are interested only in the *geometric* isomorphism classes, we may, when calculating $\sigma_v([A, \lambda, \overline{\eta}])$ extend scalars from k to $k_{v'}$ for $v'|v$. We are then in the situation of Proposition 9.24. Thanks to (c), to give $\overline{\eta}$ amounts to giving

- $A^{\overline{\eta}}$ and
- an isomorphism class $\overline{\eta}_n \colon V_{\mathbb{Z}}/nV_{\mathbb{Z}} \to A_n^{\overline{\eta}} \pmod K$ for any sufficiently large *n prime to p*.

After Proposition 9.24, $\sigma_v([A, \lambda, \overline{\eta}])$ is defined by the isomorphism class of the canonical lifting of $(A_0, \lambda_0, \overline{\eta})^{(p)}$. The canonical lifting of $A_0^{(p)}$ is $A^{\mu_\Phi(p)\overline{\eta}}$, and so

$$\sigma_v(A, \lambda, \overline{\eta}) \approx (A, p\lambda, \overline{\eta}\mu_\Phi(p)). \tag{79}$$

Consider now the set $\overline{M}$ of geometric isomorphism classes of objects $(A, \overline{\lambda}, \overline{\eta})$ as above, except that now $\overline{\lambda}$ is a *homogeneous* polarization (i.e., given up to a factor in $\mathbb{Q}^{\times}$).

The homomorphism $N_\Phi \colon T^{E^*} \to T^E$ is that deduced from $\mu_\Phi \colon \mathbb{G}_{mE^*} \to T_{E^*}^E$ by taking the norm:

$$T^{E^*} \xrightarrow{\mathrm{Res}_{E^*/\mathbb{Q}}(\mu_\Phi)} \mathrm{Res}_{E^*/\mathbb{Q}}(T_{E^*}^E) \xrightarrow{\mathrm{Norm}} T^E.$$

Let $\varphi \colon \mathbb{A}_{E^*}^{\times} \to \mathrm{Gal}(E^{*\mathrm{al}}/E^*)^{\mathrm{ab}}$ be the reciprocity homomorphism of global class field theory.

PROPOSITION 9.27 *The action of* $\mathrm{Gal}(E^{*\mathrm{al}}/E^*)^{\mathrm{ab}}$ *on* $\overline{M}$ *is given by the following rule: let* $e \in \mathbb{A}_{E^*}^{\times}$ *have finite component* $e_f \in \mathbb{A}_{E^*,f}^{\times}$; *then*

$$\varphi(e)[A, \overline{\lambda}, \overline{\eta}) = [A, \overline{\lambda}, \overline{\eta}N_\Phi(e_f)].$$

PROOF. This formula is compatible with (79), and so it suffices to check that it defines an action of the abelian Galois group, i.e., that for $c \in E^{*\times}$, we have

$$[A, \overline{\lambda}, \overline{\eta}] \approx [A, \overline{\lambda}, \overline{\eta}N_\Phi(c)].$$

The isomorphism is given by $N_\Phi(c) \colon A \to A$ (note that $N_{E/F}(N_\Phi(c)) = N_{E^*/\mathbb{Q}}(c) \in \mathbb{Q}^{\times}$, so that $\overline{\lambda}$ is respected). □

For $K \subset \mathbb{A}_{E,f}^{\times}$, sufficiently small, the objects $(A, \lambda, \overline{\eta})$ have no nontrivial automorphisms. In the proposition, pass to the inductive limit over k, up to the algebraic closure of E^*, then pass to the projective limit over K. One finds the following variant.

PROPOSITION 9.28 *Let $\overline{E}^*$ be an algebraic closure of E^* and let M^+ be the set of isomorphism classes of objects $(A, \overline{\lambda}, \overline{\eta})$ (A as above, over k, η an E-linear isomorphism of $\widehat{V}(A)$ with $V \otimes \mathbb{A}_f$, and $\overline{\lambda}$ a homogeneous polarization). Then the action of $\mathrm{Gal}(\overline{E}^*/E^*)$ on M^+ is abelian, and for $e \in \mathbb{A}_{E^*}^\times$ with finite component $e_f \in \mathbb{A}_{E^*}^\times$, we have*

$$\varphi(e)\left([A, \overline{\lambda}, \overline{\eta}]\right) = [A, \overline{\lambda}, N_{\Phi}(e_f)\overline{\eta}].$$

10 The fundamental theorem of complex multiplication

The first three subsections are based on Tate 1981 and the last section on Deligne 1981.

We begin by reviewing some notations. We let $\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{A}_f = \widehat{\mathbb{Z}} \otimes \mathbb{Q}$. For a number field k, $\mathbb{A}_{f,k} = \mathbb{A}_f \otimes_{\mathbb{Q}} k$ is the ring of finite adèles and $\mathbb{A}_k = \mathbb{A}_{f,k} \times (k \otimes_{\mathbb{Q}} \mathbb{R})$ is the full ring of adèles. When k is a subfield of $\mathbb{C}$, k^{ab} and k^{al} denote respectively the largest abelian extension of k in $\mathbb{C}$ and the algebraic closure of k in $\mathbb{C}$. Complex conjugation is denoted by ι.

For a number field k, $\mathrm{rec}_k \colon \mathbb{A}_k^\times \to \mathrm{Gal}(k^{\mathrm{ab}}/k)$ is the usual reciprocity law and art_k is its reciprocal: a prime element corresponds to the inverse of the usual (arithmetic) Frobenius. In more detail, if $a \in \mathbb{A}_{f,k}^\times$ has v-component a prime element a_v in k_v and w-component $a_w = 1$ for $w \neq v$, then

$$\mathrm{art}_k(a)(x) \equiv x^{1/\mathbb{N}(v)} \mod \mathfrak{p}_v, \quad x \in \mathcal{O}_k.$$

When k is totally imaginary, art_k factors into $\mathbb{A}_k^\times \to \mathbb{A}_{f,k}^\times \xrightarrow{r_k} \mathrm{Gal}(k^{\mathrm{ab}}/k)$; we usually write art_k for r_k. The cyclotomic character $\chi = \chi_{\mathrm{cyc}} \colon \mathrm{Aut}(\mathbb{C}) \to \widehat{\mathbb{Z}}^\times \subset \mathbb{A}_f^\times$ is the homomorphism such that $\sigma\zeta = \zeta^{\chi(\sigma)}$ for every root of 1 in $\mathbb{C}$. The composite

$$\mathrm{art}_k \circ \chi_{\mathrm{cyc}} = \mathrm{Ver}_{k/\mathbb{Q}}, \tag{80}$$

the Verlagerung map $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})^{\mathrm{ab}} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/k)^{\mathrm{ab}}$.

Statement of the Theorem

Let A be an abelian variety over $\mathbb{C}$, and let E be a subfield of $\mathrm{End}(A) \otimes \mathbb{Q}$ of degree $2 \dim A$ over $\mathbb{Q}$. The representation of E on the tangent space to A at zero is of the form $\oplus_{\varphi \in \Phi} \varphi$ with Φ a subset of $\mathrm{Hom}(E, \mathbb{C})$. A ***Riemann form*** for A is a $\mathbb{Q}$-bilinear skew-symmetric form ψ on $H_1(A, \mathbb{Q})$ such that

$$(x, y) \mapsto \psi(x, iy) \colon H_1(A, \mathbb{R}) \times H_1(A, \mathbb{R}) \to \mathbb{R}$$

is symmetric and positive definite. We assume that there exists a Riemann form ψ compatible with the action of E in the sense that, for some involution ι_E of E,

$$\psi(ax, y) = \psi(x, (\iota_E a)y), \quad a \in E, \quad x, y \in H_1(A, \mathbb{Q}).$$

Then E is a CM-field, and Φ is a CM-type on E, i.e., $\mathrm{Hom}(E, \mathbb{C}) = \Phi \cup \iota\Phi$ (disjoint union). The pair $(A, E \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q})$ is said to be of ***CM-type*** (E, Φ). For simplicity, we assume that $E \cap \mathrm{End}(A) = \mathcal{O}_E$, the full ring of integers in E.

Let $\mathbb{C}^\Phi$ be the set of complex-valued functions on Φ, and embed E into $\mathbb{C}^\Phi$ through the natural map $a \mapsto (\varphi(a))_{\varphi \in \Phi}$. There then exist a $\mathbb{Z}$-lattice $\mathfrak{a}$ in E stable under $\mathcal{O}_E$,

an element $t \in E^\times$, and an $\mathcal{O}_E$-linear analytic isomorphism $\theta\colon \mathbb{C}^\Phi/\Phi(\mathfrak{a}) \to A$ such that $\psi(x, y) = \mathrm{Tr}_{E/\mathbb{Q}}(tx \cdot \iota_E y)$ where, in the last equation, we have used θ to identify $H_1(A, \mathbb{Q})$ with $\mathfrak{a} \otimes \mathbb{Q} = E$. The variety is said to be of ***type*** $(E, \Phi; \mathfrak{a}, t)$ relative to θ. The type determines the triple $(A, E \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}, \psi)$ up to isomorphism. Conversely, the triple determines the type up to a change of the following form: if θ is replaced by $\theta \circ a^{-1}$, $a \in E^\times$, then the type becomes $(E, \Phi; a\mathfrak{a}, \frac{t}{a \cdot \iota a})$ (see 3.17).

Let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Then $E \hookrightarrow \mathrm{End}^0(A)$ induces a map $E \hookrightarrow \mathrm{End}^0(\sigma A)$, so that σA also has complex multiplication by E. The form ψ is associated with a divisor D on A, and we let $\sigma\psi$ be the Riemann form for σA associated with σD. It has the following characterization: after multiplying ψ with a nonzero rational number, we can assume that it takes integral values on $H_1(A, \mathbb{Z})$; define ψ_m to be the pairing $A_m \times A_m \to \mu_m$, $(x, y) \mapsto \exp(\frac{2\pi i \cdot \psi(x,y)}{m})$; then $(\sigma\psi)_m(\sigma x, \sigma y) = \sigma(\psi_m(x, y))$ for all m.

In the next section we shall define for each CM-type (E, Φ) a map $f_\Phi\colon \mathrm{Aut}(\mathbb{C}) \to \mathbb{A}_{f,E}^\times/E^\times$ such that

$$f_\Phi(\sigma) \cdot \iota f_\Phi(\sigma) = \chi_{\mathrm{cyc}}(\sigma)E^\times, \quad \text{all } \sigma \in \mathrm{Aut}(\mathbb{C}).$$

We can now state the fundamental theorem of complex multiplication.

THEOREM 10.1 (SHIMURA, TANIYAMA, WEIL LANGLANDS, DELIGNE, TATE, ET AL) *Suppose A has type $(E, \Phi; \mathfrak{a}, t)$ relative to the uniformization $\theta\colon \mathbb{C}^\Phi/\mathfrak{a} \to A$. Let $\sigma \in \mathrm{Aut}(\mathbb{C})$, and let $f \in \mathbb{A}_{f,E}^\times$ lie in $f_\Phi(\sigma)$.*

(a) *The variety σA has type*

$$(E, \sigma\Phi; f\mathfrak{a}, \frac{t\,\chi_{\mathrm{cyc}}(\sigma)}{f \cdot \iota f})$$

relative to θ' say.

(b) *It is possible to choose θ' so that*

$$\begin{array}{ccccc} \mathbb{A}_{f,E} & \twoheadrightarrow & \mathbb{A}_{f,E}/\mathfrak{a} \otimes \widehat{\mathbb{Z}} \simeq E/\mathfrak{a} & \xrightarrow{\theta} & A_{tors} \\ \downarrow f & & & & \downarrow \sigma \\ \mathbb{A}_{f,E} & \twoheadrightarrow & \mathbb{A}_{f,E}/(f\mathfrak{a} \otimes \widehat{\mathbb{Z}}) \simeq E/f\mathfrak{a} & \xrightarrow{\theta'} & \sigma A_{tors} \end{array}$$

commutes, where A_{tors} denotes the torsion subgroup of A (and then θ' is uniquely determined),

We now restate the theorem in more invariant form. Let

$$TA \overset{\text{def}}{=} \varprojlim A_m(\mathbb{C}) \simeq \varprojlim(\tfrac{1}{m}H_1(A, \mathbb{Z})/H_1(A, \mathbb{Z})) \simeq H_1(A, \widehat{\mathbb{Z}})$$

(limit over all positive integers m), and let

$$V_f A \overset{\text{def}}{=} TA \otimes_{\mathbb{Z}} \mathbb{Q} \simeq H_1(A, \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{A}_f.$$

Then ψ gives rise to a pairing

$$\psi_f = \varprojlim \psi_m\colon V_f A \times V_f A \to \mathbb{A}_f(1)$$

where $\mathbb{A}_f(1) = (\varprojlim \mu_m(\mathbb{C})) \otimes \mathbb{Q}$.

THEOREM 10.2 *Let A have type (E,Φ); let $\sigma\in\mathrm{Aut}(\mathbb{C})$, and let $f\in f_{\Phi}(\sigma)$.*

(a) *σA is of type $(E,\sigma\Phi)$;*

(b) *there is an E-linear isomorphism $\alpha\colon H_1(A,\mathbb{Q})\to H_1(\sigma A,\mathbb{Q})$ such that*

i) $\psi(\frac{\chi_{\mathrm{cyc}}(\sigma)}{f\cdot\iota f}x,y)=(\sigma\psi)(\alpha x,\alpha y),\quad x,y\in H_1(A,\mathbb{Q})$;

ii) *the*[33] *diagram*

$$\begin{array}{ccc} V_f(A) & \xrightarrow{f} & V_f(A) \\ & \searrow^{\sigma} & \downarrow{\scriptstyle \alpha\otimes 1} \\ & & V_f(\sigma A) \end{array}$$

commutes.

LEMMA 10.3 *The statements (10.1) and (10.2) are equivalent.*

PROOF. Let θ and θ' be as in (10.1), and let $\theta_1\colon E\xrightarrow{\approx} H_1(A,\mathbb{Q})$ and $\theta_1'\colon E\xrightarrow{\approx} H_1(\sigma A,\mathbb{Q})$ be the E-linear isomorphisms induced by θ and θ'. Let $\chi=\chi_{\mathrm{cyc}}(\sigma)/f\cdot\iota f$ — it is an element of $E^\times$. Then

$$\begin{aligned}\psi(\theta_1(x),\theta_1(y)) &= \mathrm{Tr}_{E/\mathbb{Q}}(tx\cdot\iota y)\\ (\sigma\psi)(\theta_1'(x),\theta_1'(y)) &= \mathrm{Tr}_{E/\mathbb{Q}}(t\chi x\cdot\iota y)\end{aligned}$$

and

$$\begin{array}{ccc} \mathbb{A}_{f,E} & \xrightarrow{\theta_1} & V_f(A) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \sigma} \\ \mathbb{A}_{f,E} & \xrightarrow{\theta_1'} & V_f(\sigma A) \end{array}$$

commutes. Let $\alpha=\theta_1'\circ\theta_1^{-1}$; then

$$(\sigma\psi)(\alpha x,\alpha y)=\mathrm{Tr}_{E/\mathbb{Q}}(t\chi\theta_1^{-1}(x)\cdot\iota\theta_1^{-1}(y))=\psi(\chi x,y)$$

and (on $V_f(A)$),

$$\sigma=\theta_1'\circ f\circ\theta_1^{-1}=\theta_1'\circ\theta_1^{-1}\circ f=\alpha\circ f.$$

Conversely, let α be as in (10.2) and choose θ_1' so that $\alpha=\theta_1'\circ\theta_1^{-1}$. The argument can be reversed to deduce (10.1). □

Definition of $f_{\Phi}(\sigma)$

Let (E,Φ) be a CM-pair with E a field. In (9.9) we saw that N_{Φ} gives a well-defined homomorphism $\mathrm{Aut}(\mathbb{C}/E^*)\to\mathbb{A}_{f,E}^\times/E^\times$. In this subsection, we extend this to a homomorphism on the whole of $\mathrm{Aut}(\mathbb{C})$.

Choose an embedding $E\hookrightarrow\mathbb{C}$, and extend it to an embedding $i\colon E^{\mathrm{ab}}\hookrightarrow\mathbb{C}$. Choose elements $w_\rho\in\mathrm{Aut}(\mathbb{C})$, one for each $\rho\in\mathrm{Hom}(E,\mathbb{C})$, such that

$$w_\rho\circ i|E=\rho,\quad w_{\iota\rho}=\iota w_\rho.$$

[33] *Note that both $f\in\mathbb{A}_{f,E}^\times$ and the E-linear isomorphism α are uniquely determined up to multiplication by an element of $E^\times$. Changing the choice of one changes that of the other by the same factor.*

For example, choose w_ρ for $\rho \in \Phi$ (or any other CM-type) to satisfy the first equation, and then define w_ρ for the remaining ρ by the second equation. For any $\sigma \in \mathrm{Aut}(\mathbb{C})$, $w_{\sigma\rho}^{-1}\sigma w_\rho \circ i|E = w_{\sigma\rho}^{-1} \circ \sigma\rho|E = i$. Thus $i^{-1} \circ w_{\sigma\rho}^{-1}\sigma w_\rho \circ i \in \mathrm{Gal}(E^{\mathrm{ab}}/E)$, and we can define $F_\Phi : \mathrm{Aut}(\mathbb{C}) \to \mathrm{Gal}(E^{\mathrm{ab}}/E)$ by

$$F_\Phi(\sigma) = \prod_{\varphi\in\Phi} i^{-1} \circ w_{\sigma\varphi}^{-1}\sigma w_\varphi \circ i.$$

LEMMA 10.4 *The element F_Φ is independent of the choice of $\{w_\rho\}$.*

PROOF. Any other choice is of the form $w'_\rho = w_\rho h_\rho$, $h_\rho \in \mathrm{Aut}(\mathbb{C}/iE)$. Thus $F_\Phi(\sigma)$ is changed by $i^{-1} \circ (\prod_{\varphi\in\Phi} h_{\sigma\varphi}^{-1}h_\varphi) \circ i$. The conditions on w and w' imply that $h_{\iota\rho} = h_\rho$, and it follows that the inside product is 1 because σ permutes the unordered pairs $\{\varphi, \iota\varphi\}$ and so $\prod_{\varphi\in\Phi} h_\varphi = \prod_{\varphi\in\Phi} h_{\sigma\varphi}$. □

LEMMA 10.5 *The element F_Φ is independent of the choice of i (and $E \hookrightarrow \mathbb{C}$).*

PROOF. Any other choice is of the form $i' = \sigma \circ i$, $\sigma \in \mathrm{Aut}(\mathbb{C})$. Take $w'_\rho = w_\rho \circ \sigma^{-1}$, and then

$$F'_\Phi(\tau) = \prod i'^{-1} \circ (\sigma w_{\tau\varphi}^{-1}\tau w_\varphi\sigma^{-1}) \circ i' = F_\Phi(\tau).$$

□

Thus we can suppose $E \subset \mathbb{C}$ and ignore i; then

$$F_\Phi(\sigma) = \prod_{\varphi\in\Phi} w_{\sigma\varphi}^{-1}\sigma w_\varphi \mod \mathrm{Aut}(\mathbb{C}/E^{\mathrm{ab}})$$

where the w_ρ are elements of $\mathrm{Aut}(\mathbb{C})$ such that

$$w_\rho|E = \rho, \quad w_{\iota\rho} = \iota w_\rho.$$

PROPOSITION 10.6 *For any $\sigma \in \mathrm{Aut}(\mathbb{C})$, there is a unique $f_\Phi(\sigma) \in \mathbb{A}_{f,E}^\times/E^\times$ such that*

(a) $\mathrm{art}_E(f_\Phi(\sigma)) = F_\Phi(\sigma)$;

(b) $f_\Phi(\sigma) \cdot \iota f_\Phi(\sigma) = \chi(\sigma)E^\times$, $\chi = \chi_{cyc}$.

PROOF. Since art_E is surjective, there is an $f \in \mathbb{A}_{f,E}^\times/E^\times$ such that $\mathrm{art}_E(f) = F_\Phi(\sigma)$. We have

$$\begin{aligned}\mathrm{art}_E(f \cdot \iota f) &= \mathrm{art}_E(f) \cdot \mathrm{art}_E(\iota f)\\ &= \mathrm{art}_E(f) \cdot \iota\mathrm{art}_E(f)\iota^{-1}\\ &= F_\Phi(\sigma) \cdot F_{\iota\Phi}(\sigma)\\ &= \mathrm{Ver}_{E/\mathbb{Q}}(\sigma),\end{aligned}$$

where $\mathrm{Ver}_{E/\mathbb{Q}}\colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})^{\mathrm{ab}} \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/E)^{\mathrm{ab}}$ is the transfer (Verlagerung) map. As $\mathrm{Ver}_{E/\mathbb{Q}} = \mathrm{art}_E \circ \chi$, it follows that $f \cdot \iota f = \chi(\sigma)E^\times$ modulo $\mathrm{Ker}(\mathrm{art}_E)$. Lemma 9.6 shows that $1 + \iota$ acts bijectively on $\mathrm{Ker}(\mathrm{art}_E)$, and so there is a unique $a \in \mathrm{Ker}(\mathrm{art}_E)$ such that $a \cdot \iota a = (f \cdot \iota f/\chi(\sigma))E^\times$; we must take $f_\Phi(\sigma) = f/a$. □

REMARK 10.7 The above definition of $f_\Phi(\sigma)$ is due to Tate. The original definition, due to Langlands, was more direct but used the Weil group (see my notes *Abelian Varieties with Complex Multiplication (for Pedestrians)*, 7.2).

PROPOSITION 10.8 *The maps* $f_\Phi\colon \mathrm{Aut}(\mathbb{C}) \to \mathbb{A}_{f,E}^\times/E^\times$ *have the following properties:*
(a) $f_\Phi(\sigma\tau) = f_{\tau\Phi}(\sigma)\cdot f_\Phi(\tau)$;
(b) $f_{\Phi(\tau^{-1}|E)}(\sigma) = \tau f_\Phi(\sigma)$ *if* $\tau E = E$;
(c) $f_\Phi(\iota) = 1$.

PROOF. Let $f = f_{\tau\Phi}(\sigma)\cdot f_\Phi(\tau)$. Then

$$\mathrm{art}_E(f) = F_{\tau\Phi}(\sigma)\cdot F_\Phi(\tau) = \prod_{\varphi\in\Phi} w_{\sigma\tau\varphi}^{-1}\cdot \sigma w_{\tau\varphi}\cdot w_{\tau\varphi}^{-1}\cdot \tau w_\varphi = F_\Phi(\sigma\tau)$$

and $f\cdot \iota f = \chi(\sigma)\chi(\tau)E^\times = \chi(\sigma\tau)E^\times$. Thus f satisfies the conditions that determine $f_\Phi(\sigma\tau)$. This proves (a), and (b) and (c) can be proved similarly. □

Let E^* be the reflex field for (E,Φ), so that $\mathrm{Aut}(\mathbb{C}/E^*) = \{\sigma\in\mathrm{Aut}(\mathbb{C}) \mid \sigma\Phi = \Phi\}$. Then $\Phi\,\mathrm{Aut}(\mathbb{C}/E) \overset{\text{def}}{=} \bigcup_{\varphi\in\Phi}\varphi\cdot\mathrm{Aut}(\mathbb{C}/E)$ is stable under the left action of $\mathrm{Aut}(\mathbb{C}/E^*)$, and we write

$$\mathrm{Aut}(\mathbb{C}/E)\Phi^{-1} = \bigcup \psi\cdot\mathrm{Aut}(\mathbb{C}/E^*) \qquad \text{(disjoint union)}.$$

The set $\Psi = \{\psi|E^*\}$ is a CM-type for E^*, and (E^*,Ψ) is the reflex of (E,Φ). The map $a\mapsto\prod_{\psi\in\Psi}\psi(a)\colon E^*\to\mathbb{C}$ factors through E and defines a morphism of algebraic tori $N_\Phi\colon T^{E^*}\to T^E$. The fundamental theorem of complex multiplication over the reflex field states the following: let $\sigma\in\mathrm{Aut}(\mathbb{C}/E^*)$, and let $a\in\mathbb{A}_{f,E^*}^\times/E^{*\times}$ be such that $\mathrm{art}_{E^*}(a) = \sigma$; then (10.1) is true after f has been replaced by $N_\Phi(a)$ (see Theorem 9.10; also Shimura 1971, Theorem 5.15; the sign differences result from different conventions for the reciprocity law and the actions of Galois groups). The next result shows that this is in agreement with (10.1).

PROPOSITION 10.9 *For any* $\sigma\in\mathrm{Aut}(\mathbb{C}/E^*)$ *and* $a\in\mathbb{A}_{f,E^*}^\times/E^{*\times}$ *such that* $\mathrm{art}_{E^*}(a) = \sigma|E^{*\mathrm{ab}}$, $N_\Phi(a)\in f_\Phi(\sigma)$.

PROOF. Partition Φ into orbits, $\Phi = \cup_j\Phi_j$, for the left action of $\mathrm{Aut}(\mathbb{C}/E^*)$. Then $\mathrm{Aut}(\mathbb{C}/E)\Phi^{-1} = \bigcup_j \mathrm{Aut}(\mathbb{C}/E)\Phi_j^{-1}$, and

$$\mathrm{Aut}(\mathbb{C}/E)\Phi_j^{-1} = \mathrm{Aut}(\mathbb{C}/E)(\sigma_j^{-1}\,\mathrm{Aut}(\mathbb{C}/E^*)) = (\mathrm{Hom}_E(L_j,\mathbb{C})\circ\sigma_j^{-1})\,\mathrm{Aut}(\mathbb{C}/E^*)$$

where σ_j is any element of $\mathrm{Aut}(\mathbb{C})$ such that $\sigma_j|E\in\Phi_j$ and $L_j = (\sigma_j^{-1}E^*)E$. Thus $N_\Phi(a) = \prod b_j$, with $b_j = \mathrm{Nm}_{L_j/E}(\sigma_j^{-1}(a))$. Let

$$F_j(\sigma) = \prod_{\varphi\in\Phi_j} w_{\sigma\varphi}^{-1}\sigma w_\varphi \pmod{\mathrm{Aut}(\mathbb{C}/E^{\mathrm{ab}})}.$$

We begin by showing that $F_j(\sigma) = \mathrm{art}_E(b_j)$. The basic properties of Artin's reciprocity law show that

$$\begin{array}{ccccccc}
\mathbb{A}_{f,E}^\times & \xrightarrow{\text{injective}} & \mathbb{A}_{f,\sigma L_j}^\times & \xrightarrow{\sigma_j^{-1}} & \mathbb{A}_{f,L_j}^\times & \xrightarrow{\mathrm{Nm}_{L_j/K}} & \mathbb{A}_{f,K}^\times \\
\downarrow{\scriptstyle \mathrm{art}_E} & & \downarrow{\scriptstyle \mathrm{art}_{\sigma L_j}} & & \downarrow{\scriptstyle \mathrm{art}_{L_j}} & & {\scriptstyle \mathrm{art}_K}\downarrow \\
\mathrm{Gal}(E^{\mathrm{ab}}/E) & \xrightarrow{V_{\sigma_j L_j/E}} & \sigma_j\,\mathrm{Gal}(L_j^{\mathrm{ab}}/L_j)\sigma_j^{-1} & \xrightarrow{\mathrm{ad}\sigma_j^{-1}} & \mathrm{Gal}(L_j^{\mathrm{ab}}/L_j) & \xrightarrow{\text{restriction}} & \mathrm{Gal}(K^{\mathrm{ab}}/K)
\end{array}$$

commutes. Therefore $\mathrm{art}_E(b_j)$ is the image of $\mathrm{art}_{E^*}(a)$ by the three maps in the bottom row of the diagram. Consider $\{t_\varphi \mid t_\varphi = w_\varphi \sigma_j^{-1}, \quad \varphi \in \Phi_j\}$; this is a set of coset representatives for $\sigma_j \operatorname{Aut}(\mathbb{C}/L_j)\sigma_j^{-1}$ in $\operatorname{Aut}(\mathbb{C}/E^*)$, and so $F_j(\sigma) = \prod_{\varphi\in\Phi_j} \sigma_j^{-1} t_{\sigma\varphi}^{-1} \sigma t_\varphi \sigma_j = \sigma_j^{-1} V(\sigma) \sigma_j \mod \operatorname{Aut}(\mathbb{C}/E^{\mathrm{ab}})$.

Thus $\mathrm{art}_E(N_\Phi(a)) = \prod \mathrm{art}_E(b_j) = \prod F_j(\sigma) = F_\Phi(\sigma)$. As $N_\Phi(a) \cdot \iota N_\Phi(a) \in \chi_{\mathrm{cyc}}(\sigma) E^\times$ (see 9.7), this shows that $N_\Phi(a) \in f_\Phi(\sigma)$. □

Proof of Theorem 10.2 up to an element of order 2

The variety σA has type $(E, \sigma\Phi)$ because $\sigma\Phi$ describes the action of E on the tangent space to σA at zero. Choose any E-linear isomorphism $\alpha\colon H_1(A,\mathbb{Q}) \to H_1(\sigma A, \mathbb{Q})$. Then

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

is an $\mathbb{A}_{f,E}$-linear isomorphism, and hence is multiplication by some $g \in \mathbb{A}_{f,E}^\times$; thus

$$(\alpha \otimes 1) \circ g = \sigma.$$

LEMMA 10.10 *For this g, we have*

$$(\alpha\psi)(\frac{\chi(\sigma)}{g\cdot\iota g}x, y) = (\sigma\psi)(x,y), \quad \textit{all } x, y \in V_f(\sigma A).$$

PROOF. By definition,

$$\begin{aligned}(\sigma\psi)(\sigma x, \sigma y) &= \sigma(\psi(x,y)) \qquad x, y \in V_f(A)\\ (\alpha\psi)(\alpha x, \alpha y) &= \psi(x,y) \qquad x, y \in V_f(A).\end{aligned}$$

On replacing x and y by gx and gy in the second inequality, we find that

$$(\alpha\psi)(\sigma x, \sigma y) = \psi(gx, gy) = \psi((g\cdot\iota g)x, y).$$

As $\sigma(\psi(x,y)) = \chi(\sigma)\psi(x,y) = \psi(\chi(\sigma)x, y)$, the lemma is now obvious. □

REMARK 10.11 (a) On replacing x and y with αx and αy in (10.10), we obtain the formula

$$\psi(\frac{\chi(\sigma)}{g\cdot\iota g}x, y) = (\sigma\psi)(\alpha x, \alpha y).$$

(b) On taking $x, y \in H_1(A,\mathbb{Q})$ in (10.10), we can deduce that $\chi_{\mathrm{cyc}}(\sigma)/g\cdot\iota g \in E^\times$; therefore $g\cdot\iota g \equiv \chi_{\mathrm{cyc}}(\sigma)$ modulo $E^\times$.

The only choice involved in the definition of g is that of α, and α is determined up to multiplication by an element of $E^\times$. Thus the class of g in $\mathbb{A}_{f,E}^\times/E^\times$ depends only on A and σ. In fact, it depends only on (E,Φ) and σ, because any other abelian variety of type (E,Φ) is isogenous to A and leads to the same class $gE^\times$. We define $g_\Phi(\sigma) = gE^\times \in \mathbb{A}_{f,E}^\times/E^\times$.

PROPOSITION 10.12 *The maps $g_\Phi : \operatorname{Aut}(\mathbb{C}) \to \mathbb{A}_{f,E}^\times/E^\times$ have the following properties:*

(a) $g_\Phi(\sigma\tau) = g_{\tau\Phi}(\sigma)\cdot g_\Phi(\tau)$;

(b) $g_{\Phi(\tau^{-1}|E)}(\sigma) = \tau g_\Phi(\sigma)$ *if* $\tau E = E$;

(c) $g_\Phi(\iota) = 1$;
(d) $g_\Phi(\sigma) \cdot \iota g_\Phi(\sigma) = \chi_{\text{cyc}}(\sigma)E^\times$.

PROOF. (a) Choose E-linear isomorphisms $\alpha\colon H_1(A,\mathbb{Q}) \to H_1(\tau A,\mathbb{Q})$ and $\beta\colon H_1(\tau A,\mathbb{Q}) \to H_1(\sigma\tau A,\mathbb{Q})$, and let $g = (\alpha\otimes 1)^{-1}\circ\tau$ and $g_\tau = (\beta\otimes 1)^{-1}\circ\sigma$ so that g and g_σ represent $g_\Phi(\tau)$ and $g_{\tau\Phi}(\sigma)$ respectively. Then

$$(\beta\alpha)\otimes 1 \circ (g_\tau g) = (\beta\otimes 1)\circ g_\tau \circ (\alpha\otimes 1)\circ g = \sigma\tau,$$

which shows that $g_\tau g$ represents $g_\Phi(\sigma\tau)$.

(b) If $(A, E \hookrightarrow \text{End}(A)\otimes\mathbb{Q})$ has type (E,Φ), then $(A, E \xrightarrow{\tau^{-1}} E \to \text{End}(A)\otimes\mathbb{Q})$ has type $(E,\Phi\tau^{-1})$. The formula in (b) can be proved by transport of structure.

(c) Complex conjugation $\iota\colon A \to \iota A$ is a homeomorphism (relative to the complex topology) and so induces an E-linear isomorphism $\iota_1\colon H_1(A,\mathbb{Q}) \to H_1(A,\mathbb{Q})$. The map $\iota_1\otimes 1\colon V_f(A) \to V_f(\iota A)$ is ι again, and so on taking $\alpha = \iota_1$, we find that $g = 1$.

(d) This was proved in (10.11d). □

Theorem (10.2) (hence also 10.1) becomes true if f_Φ is replaced by g_Φ. Our task is to show that $f_\Phi = g_\Phi$. To this end we set

$$e_\Phi(\sigma) = g_\Phi(\sigma)/f_\Phi(\sigma) \in \mathbb{A}_{f,E}^\times/E^\times. \tag{81}$$

PROPOSITION 10.13 *The maps $e_\Phi : \text{Aut}(\mathbb{C}) \to \mathbb{A}_{f,E}^\times/E^\times$ have the following properties:*
(a) $e_\Phi(\sigma\tau) = e_{\tau\Phi}(\sigma)\cdot e_\Phi(\tau)$;
(b) $e_{\Phi(\tau^{-1}|E)}(\sigma) = \tau e_\Phi(\sigma)$ *if* $\tau E = E$;
(c) $e_\Phi(\iota) = 1$;
(d) $e_\Phi(\sigma)\cdot \iota_E e_\Phi(\sigma) = 1$;
(e) $e_\Phi(\sigma) = 1$ *if* $\sigma\Phi = \Phi$.

PROOF. Statements (a), (b), and (c) follow from (a), (b), and (c) of (10.8) and (10.12), and (d) follows from (10.6b) and (10.12d). The condition $\sigma\Phi = \Phi$ in (e) means that σ fixes the reflex field of (E,Φ) and, as we observed in the preceding subsection, the fundamental theorem is known to hold in that case, which means that $f_\Phi(\sigma) = g_\Phi(\sigma)$. □

PROPOSITION 10.14 *Let F be the largest totally real subfield of E; then $e_\Phi(\sigma) \in \mathbb{A}_{f,F}^\times/F^\times$ and $e_\Phi(\sigma)^2 = 1$; moreover, $e_\Phi(\sigma)$ depends only on the effect of σ on E^*, and is 1 if $\sigma|E^* = \text{id}$.*

PROOF. Recall (1.16) that σ fixes E^* if and only if $\sigma\Phi = \Phi$, in which case (10.13e) shows that $e_\Phi(\sigma) = 1$. Replacing τ by $\sigma^{-1}\tau$ in (a), we find that $e_\Phi(\tau) = e_\Phi(\sigma)$ if $\tau\Phi = \sigma\Phi$, i.e., $e_\Phi(\sigma)$ depends only on the restriction of σ to the reflex field of (E,Φ). From (b) with $\tau = \iota$, we find using $\iota\Phi = \Phi\iota_E$ that $e_{\iota\Phi}(\sigma) = \iota e_\Phi(\sigma)$. Putting $\tau = \iota$ in (a) and using (c) we find that $e_\Phi(\sigma\iota) = \iota e_\Phi(\sigma)$; putting $\sigma = \iota$ in (a) and using (c) we find that $e_\Phi(\iota\sigma) = e_\Phi(\sigma)$. Since $\iota\sigma$ and $\sigma\iota$ have the same effect on E^*, we conclude $e_\Phi(\sigma) = \iota e_\Phi(\sigma)$. Thus $e_\Phi(\sigma) \in (\mathbb{A}_{f,E}^\times/E^\times)^{\langle\iota_E\rangle}$, which equals $\mathbb{A}_{f,F}^\times/F^\times$ by Hilbert's Theorem 90.[34] Finally, (d) shows that $e_\Phi(\sigma)^2 = 1$. □

[34]The cohomology sequence of the sequence of $\text{Gal}(E/F)$-modules

$$1 \to E^\times \to \mathbb{A}_{f,E}^\times \to \mathbb{A}_{f,E}^\times/E^\times \to 1$$

is

$$1 \to F^\times \to \mathbb{A}_{f,F}^\times \to (\mathbb{A}_{f,E}^\times/E^\times)^{\text{Gal}(E/F)} \to H^1(\text{Gal}(E/F), E^\times) \overset{\text{(FT 5.22)}}{=} 0$$

COROLLARY 10.15 *Part (a) of (10.1) is true; part (b) of (10.1) becomes true when f is replaced by ef with $e \in \mathbb{A}_{f,F}^\times$, $e^2 = 1$.*

PROOF. Let $e \in e_\Phi(\sigma)$. Then $e^2 \in F^\times$ and, since an element of $F^\times$ that is a square locally at all finite primes is a square (CFT VIII 1.1), we can correct e to achieve $e^2 = 1$. Now (10.1) is true with f replaced by ef, but e (being a unit) does not affect part (a) of (10.1).□

It remains to show that:

$$\text{for all CM-fields } E \text{ and CM-types } \Phi \text{ on } E,\ e_\Phi = 1. \tag{82}$$

Completion of the proof (following Deligne)

As above, let (E, Φ) be a CM pair, and let $e_\Phi(\sigma) = g_\Phi(\sigma)/f_\Phi(\sigma)$ be the associated element of $\mathbb{A}_{f,E}^\times/E^\times$. Then, as in (10.14, 10.15),

$$e_\Phi(\sigma) \in \mu_2(\mathbb{A}_{f,F})/\mu_2(F), \quad \sigma \in \mathrm{Aut}(\mathbb{C}).$$

Let

$$e \in \mu_2(\mathbb{A}_{f,F}),\ e = (e_v)_v,\ e_v = \pm 1,\ v \text{ a finite prime of } F$$

be a representative for $e_\Phi(\sigma)$. We have to show that the e_v's are all -1 or all $+1$. For this, it suffices, to show that for, for any prime numbers ℓ_1 and ℓ_2, the image of $e_\Phi(\sigma)$ in $\mu_2(F_{\ell_1} \times F_{\ell_2})/\mu_2(F)$ is trivial. Here $F_\ell = F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

In addition to the properties (a–e) of (10.13), we need:

(f) let E' be a CM-field containing E, and let Φ' be the extension of Φ to E'; then for any $\sigma \in \mathrm{Aut}(\mathbb{C})$,

$$e_\Phi(\sigma) = e_{\Phi'}(\sigma) \quad (\text{in } \mathbb{A}_{f,E'}^\times/E'^\times). \tag{83}$$

To prove this, one notes that the same formula holds for each of f_Φ and g_Φ: if A is of type (E, Φ) then $A' \overset{\text{def}}{=} A \otimes_E E'$ is of type (E', Φ'). Here $A' = A^M$ with $M = \mathrm{Hom}_{E\text{-linear}}(E', E)$ (cf. 7.31).

Note that (f) shows that $e_{\Phi'} = 1 \implies e_\Phi = 1$, and so it suffices (82) for E Galois over $\mathbb{Q}$ (and contained in $\mathbb{C}$).

We also need:

(g) denote by $[\Phi]$ the characteristic function of $\Phi \subset \mathrm{Hom}(E, \mathbb{C})$; then

$$\textstyle\sum_i n_i[\Phi_i] = 0 \implies \prod_i e_{\Phi_i}(\sigma)^{n_i} = 1 \text{ for all } \sigma \in \mathrm{Aut}(\mathbb{C}).$$

This is a consequence of Deligne's theorem that all Hodge classes on abelian varieties are absolutely Hodge, which tells us that the results on abelian varieties with complex multiplication proved above extend to CM-motives. The CM-motives are classified by infinity types rather than CM-types, and (g) just says that the e attached to the trivial CM-motive is 1. This will be explained in the next chapter.

We make (d) (of 10.13) and (g) more explicit. Recall that an infinity type on E is a function $\rho\colon \mathrm{Hom}(E, \mathbb{C}) \to \mathbb{Z}$ that can be written as a finite sum of CM-types (see §4). Now (g) allows us to define e_ρ by linearity for ρ an infinity type on E. Moreover,

$$e_{2\rho} = e_\rho^2 = 0,$$

so that e_ρ depends only on the reduction modulo 2 of ρ, which can be regarded as a function

$$\overline{\rho}\colon \mathrm{Hom}(E,\mathbb{C}) \to \mathbb{Z}/2\mathbb{Z},$$

such that either (weight 0)

$$\overline{\rho}(\varphi) + \overline{\rho}(\iota\varphi) = 0 \text{ for all } \varphi \tag{84}$$

or (weight 1)

$$\overline{\rho}(\varphi) + \overline{\rho}(\iota\varphi) = 1 \text{ for all } \varphi.$$

We now prove that $e_{\overline{\rho}} = 1$ if $\overline{\rho}$ is of weight 0. The condition (84) means that $\overline{\rho}(\varphi) = \overline{\rho}(\iota\varphi)$, and so $\overline{\rho}$ arises from a function $q\colon \mathrm{Hom}(F,\mathbb{C}) \to \mathbb{Z}/2\mathbb{Z}$:

$$\overline{\rho}(\varphi) = q(\varphi|F).$$

We write $e_q = e_{\overline{\rho}}$. When E is a subfield of $\mathbb{C}$ Galois over $\mathbb{Q}$, (b) implies that there exists an $e(\sigma) \in \mu_2(\mathbb{A}_{f,F})/\mu_2(F)$ such that[35]

$$e_q(\sigma) = \prod\nolimits_{\varphi:F\to\mathbb{C}} \varphi^{-1}(e(\sigma))^{q(\varphi)},\ \sigma \in \mathrm{Aut}(\mathbb{C}).$$

Write $e(\sigma) = e^F(\sigma)$ to denote the dependence of e on F. It follows from (f), that for any totally real field F' containing F,

$$e^F(\sigma) = \mathrm{Nm}_{F'/F}\, e^{F'}(\sigma).$$

There exists a totally real field F', quadratic over F, and such that all primes of F dividing ℓ_1 or ℓ_2 remain prime in F'. The norm maps $\mu_2(F_{2,\ell}) \to \mu_2(F_{1,\ell})$ are zero for $\ell = \ell_1, \ell_2$, and so $e^F(\sigma)$ projects to zero in $\mu_2(F_{\ell_1}) \times \mu_2(F_{\ell_2})/\mu_2(F)$. Therefore $e_q(\sigma)$ projects to zero in $\mu_2(F_{\ell_1} \times F_{\ell_2})/\mu_2(F)$. This being true for every pair (ℓ_1, ℓ_2), we have $e_q = 1$.

We now complete the proof of (82). We know that $e_{\overline{\rho}}$ depends only on the weight of $\overline{\rho}$, and so, for Φ a CM-type, $e_\Phi(\sigma)$ depends only on σ. In calculating $e_\Phi(\sigma)$, we may take $E = \mathbb{Q}(\sqrt{-1})$ and Φ to be one of the two CM-types on $\mathbb{Q}[\sqrt{-1}]$. We know (see 10.14) that $e_\Phi(\sigma)$ depends only on $\sigma|E^* = \mathbb{Q}[\sqrt{-1}]$. But $e_\Phi(1) = 1 = e_\Phi(\iota)$ by (10.13c).

ASIDE 10.16 Throughout, should allow E to be a CM-algebra. Should restate Theorem 10.2 with $\mathbb{C}$ replaced by $\mathbb{Q}^{\mathrm{al}}$; then replace $\mathbb{C}$ with $\mathbb{Q}^{\mathrm{al}}$ throughout the proof (so σ is an automorphism of $\mathbb{Q}^{\mathrm{al}}$ rather than $\mathbb{C}$).

[35] For each $\varphi\colon F \to \mathbb{C}$, choose an extension (also denoted φ) of φ to E. Then

$$\overline{\rho} = \sum\nolimits_{\varphi':E\to\mathbb{C}} \overline{\rho}(\varphi')\varphi' = \sum\nolimits_{\varphi:F\to\mathbb{C}} q(\varphi)(\varphi + \iota\varphi)$$

and so

$$e_q(\sigma) \overset{\text{def}}{=} e_{\overline{\rho}}(\sigma) = \prod\nolimits_\varphi e_{(1+\iota)\varphi}(\sigma)^{q(\varphi)} = \prod\nolimits_\varphi \varphi^{-1}(e_{1+\iota}(\sigma))^{q(\varphi)}$$

— we can take $e(\sigma) = e_{1+\iota}(\sigma)$.

Chapter III

CM-motives

- ◇ Explain and prove Deligne's theorem that Hodge classes on abelian varieties are absolutely Hodge (at least in the CM-case).
- ◇ Construct the category of abelian motives (with complex multiplication) over any field of characteristic zero. Observe that over $\mathbb{C}$, the category coincides that defined in Chapter I.
- ◇ Construct the Taniyama group (Langlands/Tate) and observe that the fundamental theorem shows that it is the Tannaka group for the category of CM-motives over $\mathbb{Q}$ (with additional structure).
- ◇ Re-interprete the earlier results more motivically.

Chapter IV

Applications

- ◇ Abelian varieties over finite fields.
- ◇ Zeta function of abelian varieties of CM-type (even over $\mathbb{Q}$, using the Taniyama group).
- ◇ Hilbert's 12th problem.
- ◇ Periods, including the period torsor.
- ◇ Algebraic Hecke characters ("...the connection between [algebraic Hecke characters] and abelian varieties with complex multiplication appears to be so close that it can hardly be accidental; and any future arithmetical interpretation of the [algebraic Hecke characters], corresponding to the interpretation given by class field theory for the characters of finite order of the idèle class group, ought to take complex multiplication into account" Weil (Weil (1956a)1956a, p18).)
- ◇ Summary of applications to modular functions and forms.
- ◇ And so on (AVCM (for pedestrians), Blasius 1986, Colmez 1993, Schappacher 1988, Shimura 1998, Yoshida 2003, ...).

Appendix A

Additional notes; solutions to the exercises

EXERCISE 1.11

Let E_1^* be a Galois closure of E^* over $\mathbb{Q}$ with Galois group G, and extend Φ to a CM-type Φ_1 on E_1^*. Note that $E_1^* = F_1[\alpha]$ and that $\Phi_1 = \{\varphi \mid \Im(\varphi(\alpha)) > 0\}$. Let

$$H = \{\sigma \in G \mid \Phi_1\sigma = \Phi_1\}.$$

Then H is the set of $\sigma \in G$ such that $\sigma\alpha/\alpha$ is totally positive, and so it is the subgroup of G fixing E^* if and only the conditions (a) and (b) in the exercise hold. Now apply Corollary 1.10.

EXERCISE 2.9

Because E^* is a product of separable field extensions, the trace pairing

$$(x, y) \mapsto \mathrm{Tr}_{E^*/\mathbb{Q}}(xy)\colon E^* \times E^* \to \mathbb{Q}$$

is nondegenerate. For any $\mathbb{Q}$-bilinear form $\psi\colon E^*\times E^* \to \mathbb{Q}$, the map $x \mapsto \psi(x, 1)\colon E^* \to \mathbb{Q}$ is $\mathbb{Q}$-linear, and so

$$\psi(x, 1) = \mathrm{Tr}_{E^*/\mathbb{Q}}(\alpha x)$$

for a unique $\alpha \in E^*$, which lies in $E^{*\times}$ if ψ is nondegenerate. If ψ satisfies (a) (of 2.9), then

$$\psi(x, y) = \psi(\overline{y}x, 1) = \mathrm{Tr}_{E^*/\mathbb{Q}}(\alpha x\overline{y}).$$

Conversely, for any $\alpha \in E^{*\times}$, $(x, y) \mapsto \mathrm{Tr}_{E^*/\mathbb{Q}}(\alpha x\overline{y})$ is a nondegenerate $\mathbb{Q}$-bilinear form satisfying (a) .

Now let

$$\psi(x, y) = \mathrm{Tr}_{E^*/\mathbb{Q}}(\alpha x\overline{y}) \tag{85}$$

for some $\alpha \in E^{*\times}$. We have

$$\psi(y, x) = \mathrm{Tr}_{E^*/\mathbb{Q}}(\alpha y\overline{x}) = \mathrm{Tr}_{E^*/\mathbb{Q}}(\overline{\alpha y}x) \text{ (as } \mathrm{Tr}_{E^*/\mathbb{Q}}(\overline{x}) = \mathrm{Tr}_{E^*/\mathbb{Q}}(x)\text{), and so}$$
$$-\psi(y, x) = \mathrm{Tr}_{E^*/\mathbb{Q}}((-\overline{\alpha})x\overline{y}).$$

On comparing this with (85), we see that (b) holds for ψ if and only if $\alpha = -\overline{\alpha}$.

Under the isomorphism

$$E^* \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{a\otimes r \mapsto (\dots, r\cdot\varphi(a),\dots)} \mathbb{C}^{\Phi},$$

multiplication by J_Φ corresponds to multiplication by $i = \sqrt{-1}$ (this is how we defined J_Φ), and ψ corresponds to $\sum_{\varphi\in\Phi} \psi_\varphi$ where

$$\psi_\varphi(x, y) = \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\alpha_\varphi x\overline{y}), \quad \alpha_\varphi \stackrel{\text{def}}{=} \varphi(\alpha).$$

Now

$$\psi_\varphi(ix, iy) = \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\alpha_\varphi \cdot ix \cdot \overline{iy}) = \psi_\varphi(x, y),$$

and so (c) holds automatically. Finally, because α_φ is totally imaginary,

$$\psi_\varphi(x, y) = \alpha_\varphi(x\overline{y} - \overline{x}y),$$

and so

$$\psi_\varphi(x, ix) = -(i\alpha_\varphi)(2x\overline{x}).$$

This is > 0 for all nonzero x if and only if $\Im(\alpha_\varphi) > 0$.

EXERCISE 3.10

Appendix B

Summary

1 Let A be an abelian variety over a field k. Then $\mathrm{End}^0(A) \stackrel{\text{def}}{=} \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a semi-simple $\mathbb{Q}$-algebra of reduced degree $\leq 2 \dim A$. When equality holds, we say that A has complex multiplication over k (or be a CM abelian variety over k, or an abelian variety of CM-type over k).

2 When A has complex multiplication over k, all maximal étale $\mathbb{Q}$-subalgebras of $\mathrm{End}^0(A)$ have degree $2 \dim A$ over $\mathbb{Q}$. We say that A has complex multiplication by E over k when E is an étale subalgebra of $\mathrm{End}^0(A)$ of degree $2 \dim A$. When, in addition, $\mathrm{End}(A) \cap E = \mathcal{O}_E$, the ring of integers in E, we say that A has complex multiplication by $\mathcal{O}_E$ over k.

3 Let A have complex multiplication by E over a field k of characteristic zero, and assume that k contains all conjugates of E. Then

$$\mathrm{Tgt}_0(A) \simeq \bigoplus\nolimits_{\varphi \in \Phi} k_\varphi \quad (\text{as } E \otimes_{\mathbb{Q}} k\text{-modules})$$

where k_φ is a one-dimensional k-vector space on which E acts through φ, and Φ is a subset of $\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(E, k)$ such that

$$\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(E, k) = \Phi \sqcup \iota\Phi \text{ for all complex conjugations } \iota \text{ on } k. \tag{86}$$

Conversely, when k is algebraically closed, every pair (E, Φ) satisfying (86) arises from an abelian variety (unique up to an E-isogeny).

4 Let $k \subset K$ be algebraically closed fields of characteristic zero. The functor $A \mapsto A_K$ from abelian varieties over k to abelian varieties over K is fully faithful, and it is an equivalence on the subcategories of CM abelian varieties.

5 A number field is a CM-field if it admits a unique nontrivial complex conjugation, and a CM-algebra is a finite product of CM-fields. A CM-type on E is a subset Φ of $\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(E, \overline{\mathbb{Q}})$ satisfying

$$\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(E, k) = \Phi \sqcup \Phi\iota_E. \tag{87}$$

Here $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. A CM-pair (E, Φ) is a CM-algebra together with a CM-type. Let L be an étale $\mathbb{Q}$-algebra and Φ subset of $\mathrm{Hom}_{\mathbb{Q}\text{-alg}}(L, \overline{\mathbb{Q}})$; then Φ satisfies (86) if and only if there exists a CM-pair (E, Φ_0) with $E \subset L$ such that

$$\Phi = \{\varphi \mid \varphi | E \in \Phi_0\}.$$

6 The reflex field of a CM-pair (E, Φ) is the smallest subfield E^* of $\overline{\mathbb{Q}}$ for which there exists an $E \otimes_{\mathbb{Q}} E^*$-module V such that

$$V \otimes_{E^*} \overline{\mathbb{Q}} \simeq \bigoplus\nolimits_{\varphi \in \Phi} \overline{\mathbb{Q}}_\varphi \quad \text{(as } E \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}\text{-modules)}$$

where $\overline{\mathbb{Q}}_\varphi$ is a one-dimensional $\overline{\mathbb{Q}}$-vector space on which E acts through φ. The $E \otimes_{\mathbb{Q}} E^*$-module V is unique up to a nonunique isomorphism. Let T^E and T^{E^*} be the algebraic tori over $\mathbb{Q}$ with $\mathbb{Q}$-points $E^\times$ and $E^{*\times}$ respectively. The reflex norm is the homomorphism $N_\Phi \colon T^{E^*} \to T^E$ such that, for any $\mathbb{Q}$-algebra R and $a \in (E^* \otimes_{\mathbb{Q}} R)^\times$,

$$N_\Phi(a) = \det_{E \otimes_{\mathbb{Q}} R}(a | V \otimes_{\mathbb{Q}} R)$$

(determinant of $x \mapsto ax \colon V \otimes_{\mathbb{Q}} R \to V \otimes_{\mathbb{Q}} R$ regarded as an $E \otimes_{\mathbb{Q}} R$-module). For any number field $k \subset \overline{\mathbb{Q}}$ containing all conjugates of E and element (or ideal, ...) a of k,

$$N_\Phi(\mathrm{Nm}_{k/E^*} a) = \prod\nolimits_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{k/\varphi E} a).$$

7 (SHIMURA-TANIYAMA FORMULA) Let A be an abelian variety with complex multiplication by $\mathcal{O}_E$ over a number field k containing the conjugates of E. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_k$ at which A has good reduction. Then

(a) there exists an element $\pi \in \mathcal{O}_E$ inducing the Frobenius endomorphism[1] on the reduction A_0 of A, and
(b) the ideal generated by π factors as

$$\pi \mathcal{O}_E = \prod\nolimits_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{k/\varphi E} \mathfrak{p})$$

where $\Phi \subset \mathrm{Hom}(E, k)$ is the CM-type of A.

8 Let A have complex multiplication by $\mathcal{O}_E$ over k. For any ideal $\mathfrak{a}$ in $\mathcal{O}_E$, there is a "smallest quotient" $\alpha^{\mathfrak{a}} \colon A \to A^{\mathfrak{a}}$, unique up to unique isomorphism, such that $a \colon A \to A$ factors through $\alpha^{\mathfrak{a}}$ for all $a \in \mathfrak{a}$;[2] it is any isogeny, and there is an $\mathcal{O}_E$-structure on $A^{\mathfrak{a}}$ for which $\alpha^{\mathfrak{a}}$ is an $\mathcal{O}_E$-isogeny. Any such $\mathcal{O}_E$-isogeny is called an $\mathfrak{a}$-multiplication.

9 Let A be an abelian variety with complex multiplication by $\mathcal{O}_E$ over a sufficiently large number field k Galois over E^*. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_k$ at which A has good reduction. Assume $(p) \overset{\text{def}}{=} \mathfrak{P} \cap \mathbb{Z}$ is unramified in E and that $\mathfrak{P}$ is unramified over E^*. Let $\mathfrak{p} = \mathfrak{P} \cap E^*$, and let $\sigma = (\mathfrak{P}, k/E^*)$ (the Frobenius automorphism at $\mathfrak{P}$); then

(a) there exists an $\mathfrak{a}$-multiplication $\alpha \colon A \to \sigma A$ whose reduction $\alpha_0 \colon A_0 \to A_0^{(q)}$ is the q-power Frobenius map, $q = (\mathcal{O}_{E^*} \colon \mathfrak{p})$;
(b) moreover, $\mathfrak{a} = N_\Phi(\mathfrak{p})$.

10 (FUNDAMENTAL THEOREM OVER THE REFLEX FIELD: IDEAL VERSION) Let A be an abelian variety with complex multiplication by $\mathcal{O}_E$ over $\overline{\mathbb{Q}}$, and fix an integer $m > 0$. Then, there exists a modulus $\mathfrak{m}$ for E^* such that the following hold:

[1] Let $q = (\mathcal{O}_k \colon \mathfrak{p})$ be the order of the residue field. By the Frobenius endomorphism of A_0 we mean the q-power Frobenius map $\pi_0 \colon A_0 \to A_0$.

[2] In scheme-theoretic terms, it is the quotient of A by

$$\mathrm{Ker}(\alpha^{\mathfrak{a}}) \overset{\text{def}}{=} \bigcap \mathrm{Ker}(a \colon A \to A).$$

(a) for each fractional ideal $\mathfrak{a}^*$ of E^* prime to $\mathfrak{m}$, there exists an ideal $\mathfrak{a}$ of $\mathcal{O}_E$ and an $\mathfrak{a}$-multiplication $\alpha: A \to \sigma A$, where $\sigma = (\mathfrak{a}^*, E^*_{\mathfrak{m}}/E^*)$, such that

$$\alpha(x) = \sigma x, \quad \text{for all } x \in A_m;$$

(b) the ideal $\mathfrak{a}$ is determine by $\mathfrak{a}^*$ up to a principal ideal in $i(E_{m,1})$, and

$$\mathfrak{a} \equiv N_{\Phi}(\mathfrak{a}^*) \mod i(E_{m,1}).$$

11 (FUNDAMENTAL THEOREM OVER THE REFLEX FIELD: IDÈLE VERSION) Let A be an abelian variety with complex multiplication by E over $\overline{\mathbb{Q}}$, and let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/E^*)$. For any $s \in \mathbb{A}_{f,E}^{\times}$ with $\mathrm{art}(s) = \sigma|E^{*\mathrm{ab}}$, there is a unique E-isogeny $\alpha: A \to \sigma A$ such that

$$\alpha(N_{\Phi}(s) \cdot x) = \sigma x \text{ for all } x \in V_f A.$$

If s is replaced with as, $a \in E^{*\times}$, then α must be replaced by αa^{-1}.

12 (FUNDAMENTAL THEOREM OVER THE REFLEX FIELD: UNIFORMIZATION VERSION) Let $(A, i: E \hookrightarrow \mathrm{End}^0(A))$ be an abelian variety with complex multiplication over $\mathbb{C}$, and let λ be a polarization of (A, i). Recall (3.11, 3.17) that the choice of a basis element e_0 for $H_0(A, \mathbb{Q})$ determines a uniformization $\theta: \mathbb{C}^{\Phi} \to A(\mathbb{C})$, and hence a quadruple $(E, \Phi; \mathfrak{a}, t)$, called the type of (A, i, λ) relative to θ. Let σ be an automorphism of $\mathbb{C}$ fixing E^*. For any $s \in \mathbb{A}_{f,E^*}^{\times}$ such that $\mathrm{art}_{E^*}(s) = \sigma|E^{*\mathrm{ab}}$, there is a unique uniformization $\theta': \mathbb{C}^{\Phi'} \to (\sigma A)(\mathbb{C})$ of σA such that

THEOREM 0.17 (a) *$\sigma(A, i, \psi)$ has type $(E, \Phi; f\mathfrak{a}, t \cdot \chi_{\mathrm{cyc}}(\sigma)/f\overline{f})$ where $f = N_{\Phi}(s) \in \mathbb{A}_{f,E}^{\times}$;*

(b) *the diagram*

$$\begin{array}{ccc} E/\mathfrak{a} & \xrightarrow{\theta_0} & A(\mathbb{C}) \\ \downarrow f & & \downarrow \sigma \\ E/f\mathfrak{a} & \xrightarrow{\theta_0'} & \sigma A(\mathbb{C}) \end{array}$$

commutes, where $\theta_0(x) = \theta((\varphi x)_{\varphi \in \Phi})$ and $\theta_0'(x) = \theta'((\varphi x)_{\varphi \in \Phi'})$.

13 (FUNDAMENTAL THEOREM OVER THE REFLEX FIELD: MODULI VERSION) See Theorem 9.19

14 (FUNDAMENTAL THEOREM OVER $\mathbb{Q}$: IDÈLE VERSION) See Theorem 10.2.

15 (FUNDAMENTAL THEOREM OVER $\mathbb{Q}$: UNIFORMIZATION VERSION) See Theorem 10.1.

Bibliography

ARTIN, M. 1986. Néron models, pp. 213–230. *In* Arithmetic geometry (Storrs, Conn., 1984). Springer, New York.

BIRKENHAKE, C. AND LANGE, H. 2004. Complex abelian varieties, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin.

BLASIUS, D. 1986. On the critical values of Hecke L-series. *Ann. of Math. (2)* 124:23–63.

BOSCH, S., LÜTKEBOHMERT, W., AND RAYNAUD, M. 1990. Néron models, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin.

BOURBAKI, N. 1958. Éléments de mathématique. I: Les structures fondamentales de l'analyse. Fascicule VII. Livre II: Algèbre. Chapitre 3: Algèbre multilinéaire. Nouvelle édition. Actualités Scientifiques et Industrielles, No. 1044. Hermann, Paris.

CHAI, C.-L. AND FALTINGS, G. 1990. Degeneration of abelian varieties, volume 22 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin.

COLMEZ, P. 1993. Périodes des variétés abéliennes à multiplication complexe. *Ann. of Math. (2)* 138:625–683.

DEBARRE, O. 1999. Tores et variétés abéliennes complexes, volume 6 of *Cours Spécialisés*. Société Mathématique de France, Paris.

DELIGNE, P. 1979. Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques, pp. 247–289. *In* Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., XXXIII. Amer. Math. Soc., Providence, R.I.

DELIGNE, P. 1981. Letter to Tate, dated October 8, 1981.

DELIGNE, P. nd. Théorie de Shimura-Taniyama et cristaux. Handwritten notes, 7pp, c1968.

DELIGNE, P. AND MILNE, J. S. 1982. Tannakian categories, pp. 101–228. *In* Hodge cycles, motives, and Shimura varieties, Lecture Notes in Mathematics. Springer-Verlag, Berlin.

GIRAUD, J. 1968. Remarque sur une formule de Shimura-Taniyama. *Invent. Math.* 5:231–236.

GREENBERG, M. J. 1967. Lectures on algebraic topology. W. A. Benjamin, Inc., New York-Amsterdam.

HARTSHORNE, R. 1977. Algebraic geometry. Springer-Verlag, New York.

HATCHER, A. 2002. Algebraic topology. Cambridge University Press, Cambridge. Available at http://www.math.cornell.edu/ hatcher/.

HEWITT, E. AND ROSS, K. A. 1963. Abstract harmonic analysis. Vol. I: Structure of topological groups. Integration theory, group representations. Die Grundlehren der mathematischen Wissenschaften, Bd. 115. Academic Press Inc., Publishers, New York.

HONDA, T. 1968. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan* 20:83–95.

MILNE, J. S. 1986. Abelian varieties, pp. 103–150. *In* Arithmetic geometry (Storrs, Conn., 1984). Springer, New York.

MILNE, J. S. 1994. Shimura varieties and motives, pp. 447–523. *In* Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math. Amer. Math. Soc., Providence, RI.

MILNE, J. S. 2005. Introduction to Shimura varieties, pp. 265–378. *In* Harmonic analysis, the trace formula, and Shimura varieties, volume 4 of *Clay Math. Proc.* Amer. Math. Soc., Providence, RI.

MUMFORD, D. 1970. Abelian varieties. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay.

MUMFORD, D. 1999. The red book of varieties and schemes, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin.

NÉRON, A. 1964. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Inst. Hautes Études Sci. Publ.Math. No.* 21:128.

OORT, F. 1973. The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field. *J. Pure Appl. Algebra* 3:399–408.

SCHAPPACHER, N. 1988. Periods of Hecke characters, volume 1301 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin.

SERRE, J.-P. 1967. Complex multiplication, pp. 292–296. *In* Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965). Thompson, Washington, D.C.

SERRE, J.-P. 1968. Abelian l-adic representations and elliptic curves. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam.

SERRE, J.-P. AND TATE, J. 1968. Good reduction of abelian varieties. *Ann. of Math. (2)* 88:492–517.

SHAFAREVICH, I. R. 1994. Basic algebraic geometry. 1,2. Springer-Verlag, Berlin.

SHIMURA, G. 1971. Introduction to the arithmetic theory of automorphic functions. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo.

SHIMURA, G. 1998. Abelian varieties with complex multiplication and modular functions, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ.

SHIMURA, G. AND TANIYAMA, Y. 1961. Complex multiplication of abelian varieties and its applications to number theory, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo. Note: Shimura 1998 is an expanded version of this work, and retains most of the same numbering.

SILVERMAN, J. H. 1986. The arithmetic of elliptic curves, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

SILVERMAN, J. H. 1994. Advanced topics in the arithmetic of elliptic curves, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

TANIYAMA, Y. 1956. Jacobian varieties and number fields. *In* Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, pp. 31–45, Tokyo. Science Council of Japan.

TATE, J. 1966. Endomorphisms of abelian varieties over finite fields. *Invent. Math.* 2:134–144.

TATE, J. 1968. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda). Séminaire Bourbaki: Vol. 1968/69, Expose 352.

TATE, J. T. 1981. On conjugation of abelian varieties of CM-type. Handwritten manuscript, 8pp, April 1981.

VLĂDUŢ, S. G. 1991. Kronecker's Jugendtraum and modular functions, volume 2 of *Studies in the Development of Modern Mathematics*. Gordon and Breach Science Publishers, New York.

WATERHOUSE, W. C. 1969. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)* 2:521–560.

WATERHOUSE, W. C. 1979. Introduction to affine group schemes, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York.

WEIL, A. 1956a. On a certain type of characters of the idèle-class group of an algebraic number-field. *In* Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, pp. 1–7, Tokyo. Science Council of Japan.

WEIL, A. 1956b. On the theory of complex multiplication. *In* Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, pp. 9–22, Tokyo. Science Council of Japan.

YOSHIDA, H. 2003. Absolute CM-periods, volume 106 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI.

YU, C.-F. 2004. The isomorphism classes of abelian varieties of CM-type. *J. Pure Appl. Algebra* 187:305–319.

If you don't find it in the index, look very carefully through the entire catalogue.

Sears & Roebuck catalogue for 1897.

Index of definitions