The Fundamental Theorem of Complex Multiplication *

J.S. Milne

May 23, 2007

Abstract

The goal of this expository article is to present a proof that is as direct and elementary as possible of the fundamental theorem of complex multiplication (Shimura, Taniyama, Langlands, Tate, Deligne et al.).

The article is a revision of part of my manuscript Milne 2006.

Contents

Introduction

A simple abelian variety A over $\mathbb{C}$ is said to have complex multiplication if its endomorphism algebra is a field of degree $2\dim A$ over $\mathbb{Q}$, and a general abelian variety over $\mathbb{C}$ is said to have complex multiplication if each of its simple isogeny factors does. Abelian varieties with complex multiplication correspond to special points in the moduli space of abelian varieties, and their arithmetic is intimately related to that of the values of modular functions and modular forms at those points. The fundamental theorem of complex multiplication describes how an automorphism of $\mathbb{C}$ (as an abstract field) acts on the abelian varieties with complex multiplication and their torsion points.

The basic theory of complex multiplication was extended from elliptic curves to abelian varieties in the 1950s by Shimura, Taniyama, and Weil.[1] The first result in the direction of the fundamental theorem is the formula of Taniyama for the prime-ideal decomposition of an endomorphism of an abelian variety that becomes the Frobenius map modulo p.[2] In their book Shimura and Taniyama 1961, and in various other works, Shimura and Taniyama proved the fundamental theorem for automorphisms of $\mathbb{C}$ fixing the reflex field of the abelian variety. Except for the result of Shih 1976,

[1]See the articles by Shimura, Taniyama, and Weil in: Proceedings of the International Symposium on Algebraic Number Theory, Tokyo & Nikko, September, 1955. Science Council of Japan, Tokyo, 1956.

[2]Ibid. p21 (article of Weil).

no progress was made on the problem of extending the theorem to all automorphisms of $\mathbb{C}$ until the article Langlands 1979. In that work, Langlands attempted to understand how the automorphisms of $\mathbb{C}$ act on Shimura varieties and their special points, and in doing so he was led to define a cocycle that conjecturally describes how the automorphisms of $\mathbb{C}$ act on abelian varieties with complex multiplication and their torsion points. Langlands's cocycle enables one to give a precise conjectural statement of the fundamental theorem *over* $\mathbb{Q}$. Tate (1981) gave a more elementary construction of Langlands's cocycle and he proved that it did indeed describe the action of $\mathrm{Aut}(\mathbb{C})$ on abelian varieties of CM-type and their torsion points up to a sequence of signs indexed by the primes of $\mathbb{Q}$. Finally, Deligne 1982 showed that there exists at most one cocycle describing this action of $\mathrm{Aut}(\mathbb{C})$ that is consistent with the results of Shimura and Taniyama, and so completed the proof of the fundamental theorem over $\mathbb{Q}$.

The goal of this article is to present a proof of the fundamental theorem of complex multiplication that is as direct and elementary as possible.

I assume that the reader is familiar with some of the more elementary parts of the theory of complex multiplication. See Milne 2006 for more background.

Notations.

"Field" means "commutative field", and "number field" means "field of finite degree over $\mathbb{Q}$" (not necessarily contained in $\mathbb{C}$). The ring of integers in a number field k is denoted by $\mathcal{O}_k$, and k^{al} denotes an algebraic closure of a field k. By $\mathbb{C}$, I mean an algebraic closure of $\mathbb{R}$, and $\mathbb{Q}^{\mathrm{al}}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Complex conjugation on $\mathbb{C}$ (or a subfield) is denoted by ι.

For an abelian group X and integer m, $X_m = \{x \in X \mid mx = 0\}$.

An étale algebra over a field is a finite product of finite separable field extensions of the field. When E is an étale $\mathbb{Q}$-algebra and k is a field of characteristic zero, I say that k ***contains all conjugates of*** E when every $\mathbb{Q}$-algebra homomorphism $E \to k^{\mathrm{al}}$ maps into k. This means that there are exactly $[E\colon\mathbb{Q}]$ distinct $\mathbb{Q}$-algebra homomorphisms $E \to k$.

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

Following Bourbaki TG, I §9.1, I require compact topological spaces to be separated.

1 Preliminaries

CM-algebras; CM-types; reflex norms

A number field E is said to be a ***CM-field*** if there exists an automorphism $\iota_E \neq 1$ of E such that $\rho \circ \iota_E = \iota \circ \rho$ for every embedding ρ of E into $\mathbb{C}$. Equivalently, $E = F[\sqrt{a}]$ with F a totally real number field and a a totally negative element of F. A ***CM-algebra*** is a finite product of CM-fields.

For a CM-algebra E the homomorphisms $E \to \mathbb{C}$ occur in complex conjugate pairs $\{\varphi, \iota \circ \varphi\}$. A ***CM-type*** on E is a choice of one element from each pair. More formally, it is a subset Φ of $\mathrm{Hom}(E, \mathbb{C})$ such that

$$\mathrm{Hom}(E, \mathbb{C}) = \Phi \sqcup \iota\Phi \qquad \text{(disjoint union).}$$

A ***CM-pair*** is a CM-algebra together with a CM-type.

Let (E, Φ) be a CM-pair, and for $a \in E$, let $\mathrm{Tr}_\Phi(a) = \sum_{\varphi \in \Phi} \varphi(a) \in \mathbb{C}$. The ***reflex field*** E^* of (E, Φ) is the subfield of $\mathbb{C}$ generated by the elements $\mathrm{Tr}_\Phi(a)$, $a \in E$. It can also be described as the fixed field of $\{\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q}) \mid \sigma\Phi = \Phi\}$.

Let (E,Φ) be a CM-pair, and let k be a subfield of $\mathbb{C}$. There exists a finitely generated $E\otimes_{\mathbb{Q}}k$-module V such that[3]

$$\mathrm{Tr}_k(a|V)=\mathrm{Tr}_\Phi(a)\quad\text{for all } a\in E \tag{1}$$

if and only if $k\supset E^*$, in which case V is uniquely determined up to an $E\otimes_{\mathbb{Q}}k$-isomorphism. For example, if k contains all conjugates of E, then V must be $\bigoplus_{\varphi\in\Phi}k_\varphi$ where k_φ is a one-dimensional k-space on which E acts through φ.

Now assume that k has finite degree over $\mathbb{Q}$, and let V_Φ be an $E\otimes_{\mathbb{Q}}k$-module satisfying (1). An element a of k defines an E-linear map $v\mapsto av\colon V\to V$ 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 $a\in(k\otimes_{\mathbb{Q}}R)^\times$, we obtain an element

$$\det_{E\otimes_{\mathbb{Q}}R}(a|V_\Phi\otimes_{\mathbb{Q}}R)\in(E\otimes_{\mathbb{Q}}R)^\times,$$

and hence a homomorphism

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

natural in R and independent of the choice of V_Φ. It is called the ***reflex norm***. When $k=E^*$, we drop it from the notation. The following formulas are easy to check (Milne 2006, §1):

$$N_{k,\Phi}=N_\Phi\circ\mathrm{Nm}_{k/E^*}, \tag{2}$$

($k\subset\mathbb{C}$ is a finite extension of E^*);

$$N_\Phi(a)\cdot\iota_E N_\Phi(a)=\mathrm{Nm}_{k\otimes_{\mathbb{Q}}R/R}(a),\text{ all } a\in(k\otimes_{\mathbb{Q}}R)^\times, \tag{3}$$

(R is a $\mathbb{Q}$-algebra);

$$N_{k,\Phi}(a)=\prod\nolimits_{\varphi\in\Phi}\varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\,a),\quad a\in k^\times, \tag{4}$$

($k\subset\mathbb{C}$ is a finite extension of E^* containing all conjugates of E).

From (4), we see that $N_{k,\Phi}$ maps units in $\mathcal{O}_k$ to units in $\mathcal{O}_E$ when k contains all conjugates of E. Now (2) shows that this remains true without the condition on k. Therefore, $N_{k,\Phi}$ is well-defined on principal ideals, and one sees easily that it has a unique extension to all fractional ideals: if $\mathfrak{a}^h=(a)$, then $N_{k,\Phi}(\mathfrak{a})=N_{k,\Phi}(a)^{1/h}$. The formulas (2,3,4) hold for ideals. If $\mathfrak{a}$ is a fractional ideal of E^* and k is a number field containing all conjugates of E, then (4) applied to the extension $\mathfrak{a}'$ of $\mathfrak{a}$ to a fractional ideal of k gives

$$N_\Phi(\mathfrak{a})^{[k:E^*]}=\prod\nolimits_{\varphi\in\Phi}\varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\,\mathfrak{a}'). \tag{5}$$

Riemann pairs; Riemann forms

A ***Riemann pair*** (Λ,J) is a free $\mathbb{Z}$-module Λ of finite rank 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 ***rational Riemann form*** for a Riemann pair is an alternating $\mathbb{Q}$-bilinear form $\psi\colon\Lambda_{\mathbb{Q}}\times\Lambda_{\mathbb{Q}}\to\mathbb{Q}$ such that

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

[3] To give an $E\otimes_{\mathbb{Q}}k$-module structure on a $\mathbb{Q}$-vector space V is the same as to give commuting actions of E and k. An element a of E defines a k-linear map $v\mapsto av\colon V\to V$ whose trace we denote by $\mathrm{Tr}_k(a|V)$.

is symmetric and positive definite.

Let (E, Φ) be a CM-pair, and let Λ be a lattice in E. Then Φ defines an isomorphism

$$e \otimes r \mapsto (\varphi(e)r)_{\varphi\in\Phi} \colon E \otimes_{\mathbb{Q}} \mathbb{R} \to \mathbb{C}^{\Phi},$$

and so

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

from which $\Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ acquires a complex structure J_{Φ}. An $\alpha \in E^{\times}$ defines a $\mathbb{Q}$-bilinear form

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

which is a rational Riemann form if and only if

$$\iota_E \alpha = -\alpha \text{ and } \Im(\varphi(\alpha)) > 0 \text{ for all } \varphi \in \Phi; \tag{6}$$

every rational Riemann form is of this form for a unique α.

Let F be the product of the largest totally real subfields of the factors of E. Then $E = F[\alpha]$ with $\alpha^2 \in F$, which implies that $\iota_E \alpha = -\alpha$. The weak approximation theorem shows that α can be chosen so that $\Im(\varphi\alpha) > 0$ for all $\varphi \in \Phi$. Thus, there certainly exist αs satisfying (6), and so (Λ, J_{Φ}) admits a Riemann form.

Let α be one element of $E^{\times}$ satisfying (6). Then the other such elements are exactly those of the form $a\alpha$ with a a totally positive element of $F^{\times}$. In other words, if ψ is one rational Riemann form, then the other rational Riemann forms are exactly those of the form $a\psi$ with a a totally positive element of $F^{\times}$.

Abelian varieties with complex multiplication

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

$$[E \colon \mathbb{Q}] \leq 2 \dim A. \tag{7}$$

In general, for $\ell \neq \mathrm{char}\, k$, $\mathrm{End}^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}$ acts faithfully on $V_{\ell} A$, which again implies (7). When equality holds we say that A has ***complex multiplication by*** E ***over*** k. 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 an étale $\mathbb{Q}$-algebra E of degree $2 \dim A$ into $\mathrm{End}^0(A)$ (recall that this requires that $i(1)$ acts as id_A; see Notations).

Classification up to isogeny

1.1 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

$$H_1(A, \mathbb{R}) \simeq \mathrm{Tgt}_0(A) \oplus \overline{\mathrm{Tgt}_0(A)} \tag{8}$$

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 ***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. (8))

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

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

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

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

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

$$\begin{array}{ccc} \mathrm{Tgt}_0(A)/\Lambda & \longrightarrow & A \\ \downarrow & & \downarrow \\ \mathbb{C}^\Phi/\Phi(\mathfrak{a}) & = & A_\Phi. \end{array} \tag{9}$$

PROPOSITION 1.2 *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.*

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 (1.1) that e determines an isomorphism

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

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

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

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 $(A,i,\leftarrow)$ 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 $H_1(A,\mathbb{Q})$. Then (see p4), there exists a unique element $t\in E^\times$ such that $\psi(xe,ye) = \mathrm{Tr}_{E/\mathbb{Q}}(tx\bar{y})$. The triple $(A,i,\leftarrow)$ is said to be of ***type*** $(E,\Phi;\mathfrak{a},t)$ relative to θ (cf. Shimura 1971, Section 5.5 B).

PROPOSITION 1.3 *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 $(E,\Phi;a\mathfrak{a},t/a\bar{a})$. 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. □

Commutants

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

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

Then R is an ***order*** in E, i.e., it is simultaneously a subring and a lattice in E.

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 $R_\ell \overset{\text{def}}{=} R \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ on $T_\ell A$ and of $E_\ell \overset{\text{def}}{=} \mathbb{Q}_\ell \otimes_{\mathbb{Q}} E$ on $V_\ell A$.

PROPOSITION 1.4 *(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.

(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 1.5 *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 (1.4a).

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 $[E{:}\mathbb{Q}] \leq [C{:}\mathbb{Q}]$, and $C \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is contained in the commutant E_ℓ of E in $\mathrm{End}(V_\ell A)$, so $[E{:}\mathbb{Q}] \geq [C{:}\mathbb{Q}]$. 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 1.6 *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 1.7 If ℓ does not divide $(\mathcal{O}_E{:}\, R)$, then R_ℓ is a product of discrete valuation rings, and $T_\ell A$ is a free R_ℓ-module of rank 1, but in general this need not be true (Serre and Tate 1968, p502). Similarly, $T_m A \overset{\text{def}}{=} \prod_{\ell | m} T_\ell A$ is a free $R_m \overset{\text{def}}{=} \prod_{\ell | m} R_\ell$-module of rank 1 if m is relatively prime to $(\mathcal{O}_E{:}\, R)$.

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 $\varphi(a)$. For any complex conjugation[4] ι on k,

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

[4]A ***complex conjugation*** on a field k is the involution induced by complex conjugation on $\mathbb{C}$ through some embedding of k into $\mathbb{C}$.

A subset Φ of $\mathrm{Hom}(E,k)$ with this property will be called a CM-type on E with values in k. If $k \subset \mathbb{C}$, then it can also be regarded as a CM-type on E with values in $\mathbb{C}$.

Extension of the base field

Let k be an algebraically closed subfield of $\mathbb{C}$. For abelian varieties A, B over k, $\mathrm{Hom}(A,B) \simeq \mathrm{Hom}(A_{\mathbb{C}}, B_{\mathbb{C}})$, i.e., the functor from abelian varieties over k to abelian varieties over $\mathbb{C}$ is fully faithful. It is even essentially surjective (hence an equivalence) on abelian varieties with complex multiplication. See, for example, Milne 2006, Proposition 7.8.

Good reduction

Let R be a discrete valuation ring with field of fractions K and residue field k. An abelian variety A over K is said to have ***good reduction*** if it is the generic fibre of an abelian scheme $\mathcal{A}$ over R. Then the special fibre A_0 of $\mathcal{A}$ is an abelian variety, and $\mathrm{Tgt}_0(\mathcal{A})$ is a free R-module such that

$$\begin{aligned}\mathrm{Tgt}_0(\mathcal{A}) \otimes_R K &\simeq \mathrm{Tgt}_0(A)\\ \mathrm{Tgt}_0(\mathcal{A}) \otimes_R k &\simeq \mathrm{Tgt}_0(A_0).\end{aligned}$$

The map

$$\mathrm{End}(\mathcal{A}) \to \mathrm{End}(A)$$

is an isomorphism, and there is a reduction map

$$\mathrm{End}(A) \simeq \mathrm{End}(\mathcal{A}) \to \mathrm{End}(A_0). \tag{10}$$

This is an injective homomorphism. See, for example, Milne 2006, II, §6.

It is a fairly immediate consequence of Néron's theorem on the existence of minimal models that an abelian variety with complex multiplication over a number field k acquires good reduction at all finite primes after finite extension of k (Serre and Tate 1968, Theorem 6; Milne 2006, 7.12).[5]

The degrees of isogenies

An isogeny $\alpha\colon A \to B$ defines a homomorphism $\alpha^*\colon k(B) \to k(A)$ of the fields of rational functions, and the ***degree*** of α is defined to be $[k(A)\colon \alpha^* k(B)]$.

PROPOSITION 1.8 *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 $d \cdot \mathrm{char}(k)$. 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 $\mathrm{Nm}_{E_\ell/\mathbb{Q}_\ell}(\alpha)$, which equals $\mathrm{Nm}_{E/\mathbb{Q}}(\alpha)$. But R is a lattice in E, and so this norm equals $(R\colon \alpha R)$.[6] □

[5] Néron's theorem was, of course, not available to Shimura and Taniyama, who proved their results "for almost all $\mathfrak{p}$". Néron's theorem allowed later mathematicians to claim to have sharpened the results of Shimura and Taniyama without actually having done anything.

[6] In more detail: let $e_1, \ldots, e_n$ be a basis for R as a $\mathbb{Z}$-module, and let $\alpha e_j = \sum_i a_{ij} e_i$. For some $\varepsilon \in V_\ell A$, $e_1\varepsilon, \ldots, e_n\varepsilon$ 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).

PROPOSITION 1.9 (SHIMURA AND TANIYAMA 1961, I 2.8, THM 1) *Let k be an algebraically closed field of characteristic $p > 0$, and let $\alpha: A \to B$ 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 $\mathrm{Tgt}_0(\alpha): \mathrm{Tgt}_0(A) \to \mathrm{Tgt}_0(B)$; then*

$$\deg(\alpha) \le q^d.$$

We offer two proofs, according to the taste and knowledge of the reader.

Proof of (1.9) in terms of varieties and differentials

LEMMA 1.10 *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. We use that $\mathrm{Hom}_{K\text{-linear}}(\Omega^1_{L/K}, K)$ is isomorphic to the space of K-derivations $L \to K$. Let $x_1, \ldots, x_n$ 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, L is a purely inseparable extension of $K(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ 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 1.9) In the lemma, take $L = k(A)$ and $K = \alpha^*(k(B))$. Then $\deg(\alpha) = [L\colon K]$ and $\dim \Omega^1_{L/K} = \dim \mathrm{Ker}(\mathrm{Tgt}_0(\alpha))$, and so the proposition follows. □

Proof of (1.9) in terms of finite group schemes

The ***order*** of a finite group scheme $N = \mathrm{Spec}\, R$ over a field k is $\dim_k R$.

LEMMA 1.11 *The kernel of an isogeny of abelian varieties is a finite group scheme of order equal to the degree of the isogeny.*

PROOF. Let $\alpha: A \to B$ 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 $\mathrm{Ker}(\alpha)$, 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 $r = [k(A)\colon \alpha^*k(B)] = \deg(\alpha)$. □

PROOF (OF 1.9) The condition on α implies that $\mathrm{Ker}(\alpha)$ is connected, and therefore its affine ring is of the form $k[T_1, \ldots, T_s]/(T_1^{p^{r_1}}, \ldots, T_s^{p^{r_s}})$ 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,

$$\deg(\alpha) = \prod\nolimits_{i=1}^{s} p^{r_i} \le p^{ms} = q^d.$$ □

$\mathfrak{a}$-multiplications: first approach

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,[7] 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 $\lambda^{\mathfrak{a}}: A \to A^{\mathfrak{a}}$ with certain properties. The shortest definition is to take $A^{\mathfrak{a}}$ to be the quotient of A by the finite group scheme

$$\mathrm{Ker}(\mathfrak{a}) = \bigcap\nolimits_{a \in \mathfrak{a}} \mathrm{Ker}(a).$$

However, the formation of quotients by finite group schemes in characteristic p is subtle (Mumford 1970, p109-123)[8], and was certainly not available to Shimura and Taniyama. In this subsection, we give an elementary construction.

DEFINITION 1.12 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 $\lambda^{\mathfrak{a}}: A \to A^{\mathfrak{a}}$ is an $\mathfrak{a}$-***multiplication*** if every homomorphism $a: A \to A$ 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 $\lambda': A \to A'$ with the same property, there is a homomorphism $\alpha: A' \to A^{\mathfrak{a}}$, necessarily unique, such that $\alpha \circ \lambda' = \lambda^{\mathfrak{a}}$:

$$\begin{tikzcd}
 & A^{\mathfrak{a}} \arrow[d, dotted, "\exists!"'] \\
A \arrow[ur, two heads, "\lambda^{\mathfrak{a}}"] \arrow[r, "a"] \arrow[dr, two heads, "\lambda'"'] & A \\
 & A'. \arrow[u, dotted, "\exists!"] \arrow[uu, bend right, "\exists!\alpha"']
\end{tikzcd}$$

An abelian variety B for which there exists an $\mathfrak{a}$-multiplication $A \to B$ is called an $\mathfrak{a}$-***transform*** of A.

EXAMPLE 1.13 (a) If $\mathfrak{a}$ is principal, say, $\mathfrak{a} = (a)$, then $a: A \to A$ is an $\mathfrak{a}$-multiplication (obvious from the definition) — this explains the name "$\mathfrak{a}$-multiplication". More generally, if $\lambda: A \to A'$ is an $\mathfrak{a}$-multiplication, then

$$A \xrightarrow{a} A \xrightarrow{\lambda} A'$$

is an $\mathfrak{a}a$-multiplication for any $a \in E$ such that $\mathfrak{a}a \subset R$ (obvious from the construction in 1.15 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 $R \stackrel{\text{def}}{=} \mathrm{End}(A) \cap E$,

$$\begin{aligned}
\mathrm{Ker}(\mathfrak{a}) &= \{z + \Phi(\Lambda) \mid az \in \Phi(\Lambda) \text{ all } a \in \mathfrak{a}\} \\
&= \Phi(\mathfrak{a}^{-1}\Lambda)/\Phi(\Lambda)
\end{aligned}$$

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.

[7] 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.

[8] Compare the proof of (1.15) with that of Mumford 1970, III, Theorem 1, p111.

REMARK 1.14 (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, $R \subset \mathrm{End}(A^{\mathfrak{a}}) \cap E$, but the inclusion may be strict unless $R = \mathcal{O}_E$.[9]

(d) If $\lambda\colon A \to B$ is an $\mathfrak{a}$-multiplication, then so also is $\lambda_{k'}\colon A_{k'} \to B_{k'}$ for any $k' \supset k$. This follows from the construction in (1.15) below.

PROPOSITION 1.15 *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

$$x \mapsto (a_1 x, \ldots)\colon A \to A^n. \tag{11}$$

For any $a = \sum_i r_i a_i \in \mathfrak{a}$, the diagram

$$\begin{tikzcd} A \arrow[r, "\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}"] \arrow[rr, bend right, "a"'] & A^n \arrow[r, "(r_1, \cdots, r_n)"] & A \end{tikzcd}$$

shows that $a\colon A \to A$ factors through $\lambda^{\mathfrak{a}}$.

Let $\lambda'\colon A \to A'$ be a quotient map such that each a_i factors through λ', say, $\alpha_i \circ \lambda' = a_i$. Then the composite of

$$\begin{tikzcd} A \arrow[r, "\lambda'"] & A' \arrow[r, "\alpha = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}"] & A^n \end{tikzcd} \tag{12}$$

is $x \mapsto (a_1 x, \ldots)\colon A \to A^n$, which shows that $\alpha \circ \lambda' = \lambda^{\mathfrak{a}}$. □

REMARK 1.16 A surjective homomorphism $\lambda\colon A \to B$ is an $\mathfrak{a}$-multiplication if and only if every homomorphism $a\colon A \to A$ 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 $\lambda\colon A \to B$ 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).

PROPOSITION 1.17 *Let A be an abelian variety with complex multiplication by E over k, and assume that $E \cap \mathrm{End}(A) = \mathcal{O}_E$. Let $\lambda\colon A \to B$ and $\lambda'\colon A \to B'$ be $\mathfrak{a}$ and $\mathfrak{a}'$-multiplications respectively. 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 quotient 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 (1.22) below. □

COROLLARY 1.18 *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 $\mathfrak{a} = \mathfrak{a}'$.*

[9] Over $\mathbb{C}$, A is E-isogenous to an abelian variety with $\mathrm{End}(A) \cap E = \mathcal{O}_E$, but every such isogeny is an $\mathfrak{a}$-multiplication for some $\mathfrak{a}$ (see below).

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 1.19 *Let $a \in \operatorname{End}(A) \cap E$. 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 1.20 Let $\lambda\colon A \to B$ be an $\mathfrak{a}$-multiplication. Let $a_1, \ldots, a_n$ be a basis for $\mathfrak{a}$, and let $a_i = \alpha_i \circ \lambda$. In the diagram

$$\begin{tikzcd} A \arrow[r, "\lambda"] \arrow[rr, bend right, "a"'] & B \arrow[r, "\alpha"] & A^n \end{tikzcd} \qquad \alpha = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

α maps B isomorphically onto the image of a. For any prime ℓ different from the characteristic of k, we get a diagram

$$\begin{tikzcd} T_\ell A \arrow[r, "T_\ell\lambda"] \arrow[rr, bend right, "T_\ell a"'] & T_\ell B \arrow[r, "T_\ell\alpha"] & T_\ell A^n \end{tikzcd}$$

in which $T_\ell\alpha$ maps $T_\ell B$ isomorphically onto the image of $T_\ell a$.

PROPOSITION 1.21 *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 $\mathfrak{a}'\mathfrak{a} = (\ldots, a_i' a_j, \ldots)$, and one can show that A'' is isomorphic to the image of A under $x \mapsto (\ldots, a_i' a_j x, \ldots)$ (alternatively, use (1.31) and (13)). □

PROPOSITION 1.22 *For any $\mathfrak{a}$-multiplication λ, $\deg(\lambda) = (\mathcal{O}_E \colon \mathfrak{a})$ provided $\mathfrak{a}$ is invertible (locally free of rank 1).*

PROOF. For simplicity, we assume that $\mathcal{O}_E = \operatorname{End}(A) \cap E$. 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.[10] 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 $\deg(\lambda^{\mathfrak{b}}) = (\mathcal{O} \colon \mathfrak{b})$. □

COROLLARY 1.23 *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 (1.12), 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. □

[10] 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 $(\mathcal{O}_E \colon \mathfrak{a})$.

PROPOSITION 1.24 *Let E be a CM-algebra, and let A and B be abelian varieties with complex multiplication by E over $\mathbb{C}$. If A and B are E-isogenous, then there exists a lattice ideal $\mathfrak{a}$ and an $\mathfrak{a}$-multiplication $A \to B$.*

PROOF. 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

$$\mathbb{C}^\Phi/\Phi(\mathfrak{a}) \to A(\mathbb{C}), \quad \mathbb{C}^\Phi/\Phi(\mathfrak{b}) \to B(\mathbb{C}).$$

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 1.25 *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 $a_1, \ldots, a_n$ be a basis for $\mathfrak{a}$, and let $a_i = \alpha_i \circ \lambda$. In the diagram

$$\begin{tikzcd} A \arrow[r, "\lambda"] \arrow[rr, bend right, "a"'] & B \arrow[r, "\alpha"] & A^n \end{tikzcd} \qquad \alpha = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix},$$

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 (10)), and reduces to a similar diagram over k_0, which proves the proposition. (For an alternative proof, see 1.27.) □

$\mathfrak{a}$-multiplications: second approach

In this subsection, R is a commutative ring.

PROPOSITION 1.26 *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*

$$\underline{A}^M(T) = \mathrm{Hom}_R(M, A(T)) \qquad (T \text{ a } k\text{-scheme})$$

is represented by a commutative algebraic group A^M over k with an action of R. Moreover,

$$A^{M\otimes_R N} \simeq (A^M)^N. \tag{13}$$

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

$$\mathrm{Hom}_R(N, \mathrm{Hom}_R(M, A(T))) \simeq \mathrm{Hom}_R(M \otimes_R N, A(T)).$$

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 $\bar{k}$ of k and a prime $\ell \neq \operatorname{char} k$,

$$\begin{aligned} A^M(\bar{k})_\ell &= \mathrm{Hom}_R(M, A(\bar{k})_\ell) \\ &\simeq \mathrm{Hom}_{R_\ell}(M_\ell, A(\bar{k})_\ell), \quad R_\ell \stackrel{\text{def}}{=} \mathbb{Z}_\ell \otimes R, \quad M_\ell \stackrel{\text{def}}{=} \mathbb{Z}_\ell \otimes_{\mathbb{Z}} M. \end{aligned}$$

But M_ℓ is free of rank r over R_ℓ (because R is semi-local), and so the order of $A^M(\bar{k})_\ell$ is $l^{2r \dim A}$. Thus A^M has dimension $r \dim A$. □

REMARK 1.27 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 1.28 *Let R act on an abelian variety A over a field k. For any finitely presented R-module M and $\ell \neq \operatorname{char} k$,*

$$T_\ell(A^M) \simeq \mathrm{Hom}_{R_\ell}(M_\ell, T_\ell A), \quad R_\ell \stackrel{\text{def}}{=} \mathbb{Z}_\ell \otimes R, \quad M_\ell \stackrel{\text{def}}{=} \mathbb{Z}_\ell \otimes_{\mathbb{Z}} M.$$

PROOF. As in the proof of (1.26),

$$A^M(\bar{k})_{\ell^n} \simeq \mathrm{Hom}_{R_\ell}(M_\ell, A(\bar{k})_{\ell^n}).$$

Now pass to the inverse limit over n. □

Let $R = \mathrm{End}_R(A)$. For any R-linear map $\alpha\colon M \to R$ and $a \in A(T)$, we get an element

$$x \mapsto \alpha(x) \cdot a\colon M \to A(T)$$

of $\underline{A}^M(T)$. In this way, we get a map $\mathrm{Hom}_R(M, R) \to \mathrm{Hom}_R(A, A^M)$.

PROPOSITION 1.29 *If M is projective, then* $\mathrm{Hom}_R(M, R) \simeq \mathrm{Hom}_R(A, A^M)$.

PROOF. When $M = R$, the map is simply $R \simeq \mathrm{End}_R(A)$. 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

$$\begin{array}{ccc} \mathrm{Hom}_R(M, R) \oplus \mathrm{Hom}_R(N, R) & \longrightarrow & \mathrm{Hom}_R(A, A^M) \oplus \mathrm{Hom}_R(A, A^N) \\ \wr\| & & \wr\| \\ \mathrm{Hom}_R(R^n, R) & \xrightarrow{\simeq} & \mathrm{Hom}_R(A, A^n). \end{array}$$

□

PROPOSITION 1.30 *Let A be an abelian variety over a field k, and let R be a commutative subring of* $\mathrm{End}(A)$ *such that $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a product of fields and* $[R\colon\mathbb{Z}] = 2\dim A$. *For any invertible ideal $\mathfrak{a}$ in R, the map $\lambda^{\mathfrak{a}}\colon A \to A^{\mathfrak{a}}$ corresponding to the inclusion $\mathfrak{a} \hookrightarrow A$ is an isogeny with kernel* $A_{\mathfrak{a}} \stackrel{\text{def}}{=} \bigcap_{a \in \mathfrak{a}} \mathrm{Ker}(a)$.

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, from which this follows. □

COROLLARY 1.31 *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 1.15). □

REMARK 1.32 Corollary 1.31 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 $A^{\mathfrak{a}}/(A^{\mathfrak{a}})^\circ \simeq \mathrm{Ext}^1_R(R/\mathfrak{a}, A)$ (see Waterhouse 1969, Appendix).

$\mathfrak{a}$-multiplications: complements

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 $\lambda \circ a \in \mathrm{Hom}(A, B)$ (rather than $\mathrm{Hom}^0(A, B)$). To see this, choose a basis for $a_1, \ldots, a_n$ for $\mathfrak{a}$, and note that the composite of the 'homomorphisms'

$$A \xrightarrow{a} A \xrightarrow{x \mapsto (\ldots, a_i x, \ldots)} A^n$$

is a homomorphism into $A^{\mathfrak{a}} \subset A^n$.

PROPOSITION 1.33 *Let A have complex multiplication by E over k.*

(a) Let $\lambda\colon A \to B$ be an $\mathfrak{a}$-multiplication. Then the map

$$a \mapsto \lambda^{\mathfrak{a}} \circ a\colon \mathfrak{a}^{-1} \to \mathrm{Hom}_R(A, B)$$

is an isomorphism. In particular, every R-isogeny $A \to B$ is a $\mathfrak{b}$-multiplication for some ideal $\mathfrak{b}$.

(b) Assume $\mathcal{O}_E = \mathrm{End}(A) \cap E$. For any lattice ideals $\mathfrak{a} \subset \mathfrak{b}$ in $\mathcal{O}_E$,

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

PROOF. (a) In view of (1.31), the first statement is a special case of (1.29). For the second, recall (1.13) 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 1.21), and so this follows from (a). $\square$

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 1.34 *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 (1.33) 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. $\square$

PROPOSITION 1.35 *Let A and B be abelian varieties with complex 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 becomes an $\mathfrak{a}$-multiplication over a finite extension of k.*

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 (1.24) (after a finite extension of k). According to Proposition 1.25, $\lambda_0\colon A_0 \to B_0$ 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 (1.33). Therefore, μ lifts to an isogeny $\lambda'\colon A \to B$, which is a $\mathfrak{b}$-multiplication (see 1.33). $\square$

2 The Shimura-Taniyama formula

The ***numerical norm*** of a nonzero integral ideal $\mathfrak{a}$ in a number field K is $\mathbb{N}\mathfrak{a} = (\mathcal{O}_K : \mathfrak{a})$. For a prime ideal $\mathfrak{p}$ lying over p, $\mathbb{N}\mathfrak{p} = p^{f(\mathfrak{p}/p)}$. The map $\mathbb{N}$ is multiplicative: $\mathbb{N}\mathfrak{a} \cdot \mathbb{N}\mathfrak{b} = \mathbb{N}(\mathfrak{a}\mathfrak{b})$.

Let k be a field of characteristic p, let q be a power of p, and let σ be the homomorphism $a \mapsto a^q : k \to k$. For a variety V over k, we let $V^{(q)} = \sigma V$. For example, if V is defined by polynomials $\sum a_{i_1 \ldots} X_1^{i_1} \cdots$, then $V^{(q)}$ is defined by polynomials $\sum a_{i_1 \ldots}^q X_1^{i_1} \cdots$. The q-***power Frobenius map*** is the regular map $V \to \sigma V$ that acts by raising the coordinates of a k^{al}-point of V to the qth power.

When $k = \mathbb{F}_q$, $V^{(q)} = V$ and the q-power Frobenius map is a regular map $\pi : V \to V$. When V is an abelian variety, the Frobenius maps are homomorphisms.

THEOREM 2.1 *Let A be an abelian variety with complex multiplication by a CM-algebra E over a number field k. Assume that k contains all conjugates of E and let $\mathfrak{P}$ be prime ideal of $\mathcal{O}_k$ at which A has good reduction. Assume (i) that $(p) \overset{\text{def}}{=} \mathfrak{P} \cap \mathbb{Z}$ 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*

$$(\pi) = \prod\nolimits_{\varphi \in \Phi} \varphi^{-1}(\mathrm{Nm}_{k/\varphi E}\, \mathfrak{P}) \tag{14}$$

where $\Phi \subset \mathrm{Hom}(E, k)$ is the CM-type of A.

PROOF. Let A_0 be the reduction of A to $k_0 \overset{\text{def}}{=} \mathcal{O}_k/\mathfrak{P}$, and let

$$q = |k_0| = (\mathcal{O}_k : \mathfrak{P}) = p^{f(\mathfrak{P}/p)}.$$

(a) Recall that the reduction map $\mathrm{End}(A) \to \mathrm{End}(A_0)$ is injective. As $\mathrm{End}(A) \cap E$ is the maximal order $\mathcal{O}_E$ in E, $\mathrm{End}(A_0) \cap E$ must be also. The (q-power) Frobenius endomorphism π of A_0 commutes with all endomorphisms of A_0, and so it lies in $\mathcal{O}_E$ by (1.5).

(b) Let $\mathcal{A}$ be the abelian scheme over over $\mathcal{O}_k$ with fibres A and A_0. Then $\mathcal{T} \overset{\text{def}}{=} \mathrm{Tgt}_0(\mathcal{A})$ is a free $\mathcal{O}_k$-module of rank $\dim A$ such that $\mathcal{T} \otimes_{\mathcal{O}_k} k \simeq \mathrm{Tgt}_0(A)$ and $\mathcal{T}/\mathfrak{P}\mathcal{T} \simeq \mathrm{Tgt}_0(A_0) \overset{\text{def}}{=} T_0$.

Because p is unramified in E, the isomorphism $E \otimes_{\mathbb{Q}} k \simeq \prod_{\sigma : E \to k} k_\sigma$ induces an isomorphism $\mathcal{O}_E \otimes_{\mathbb{Z}} \mathcal{O}_k \simeq \prod_{\sigma : E \to k} \mathcal{O}_\sigma$ where $\mathcal{O}_\sigma$ denotes $\mathcal{O}_k$ with the $\mathcal{O}_E$-algebra structure provided by σ. Similarly, the isomorphism $T \simeq \bigoplus_{\varphi \in \Phi} k_\varphi$ induces an isomorphism $\mathcal{T} \simeq \bigoplus_{\varphi \in \Phi} \mathcal{O}_\varphi$ where $\mathcal{O}_\varphi$ is the submodule of $\mathcal{T}$ on which $\mathcal{O}_k$ acts through φ. In other words, there exists an $\mathcal{O}_k$-basis $(e_\varphi)_{\varphi \in \Phi}$ for $\mathcal{T}$ such that $ae_\varphi = \varphi(a)e_\varphi$ for $a \in \mathcal{O}_E$.

Because $\pi\bar{\pi} = q$, the ideal (π) is divisible only by prime ideals dividing p, say,

$$(\pi) = \prod\nolimits_{v|p} \mathfrak{p}_v^{m_v}, \quad m_v \geq 0.$$

For h the class number of E, let

$$\mathfrak{p}_v^{m_v h} = (\gamma_v), \quad \gamma_v \in \mathcal{O}_E, \tag{15}$$

and let

$$\Phi_v = \{\varphi \in \Phi \mid \varphi^{-1}(\mathfrak{P}) = \mathfrak{p}_v\},$$
$$d_v = |\Phi_v|.$$

The kernel of $T_0 \xrightarrow{\gamma_v} T_0$ is the span of the e_φ for which $\varphi(\gamma_v) \in \mathfrak{P}$, but $\varphi^{-1}(\mathfrak{P})$ is a prime ideal of $\mathcal{O}_E$ and $\mathfrak{p}_v$ is the only prime ideal of $\mathcal{O}_E$ containing γ_v, and so $\varphi(\gamma_v) \in \mathfrak{P}$ if and only if $\varphi^{-1}(\mathfrak{P}) = \mathfrak{p}_v$:

$$\operatorname{Ker}(T_0 \xrightarrow{\gamma_v} T_0) = \langle e_\varphi \mid \varphi \in \Phi_v \rangle.$$

Since $\pi^h \colon A_0 \to A_0$ 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 1.9 shows that

$$\deg(A_0 \xrightarrow{\gamma_v} A_0) \le q^{h d_v}.$$

As

$$\deg(A_0 \xrightarrow{\gamma_v} A_0) \overset{(1.8)}{=} \mathbb{N}(\gamma_v) \overset{(15)}{=} \mathbb{N}(\mathfrak{p}_v^{h m_v})$$

we deduce that

$$\mathbb{N}(\mathfrak{p}_v^{m_v}) \le q^{d_v}. \tag{16}$$

On taking the product over v, we find that

$$\operatorname{Nm}_{E/\mathbb{Q}}(\pi) \le q^{\sum_{v|p} d_v} = q^g.$$

But

$$\operatorname{Nm}_{E/\mathbb{Q}}(\pi) \overset{(1.8)}{=} \deg(A_0 \xrightarrow{\pi} A_0) = q^g,$$

and so the inequalities are all equalities.

Equality in (16) implies that

$$\operatorname{Nm}_{E/\mathbb{Q}}(\mathfrak{p}_v^{m_v}) = \left(\operatorname{Nm}_{k/\mathbb{Q}} \mathfrak{P}\right)^{d_v}$$

which equals,

$$\begin{aligned}\prod\nolimits_{\varphi \in \Phi_v} \operatorname{Nm}_{k/\mathbb{Q}} \mathfrak{P} &= \prod\nolimits_{\varphi \in \Phi_v} \left(\operatorname{Nm}_{E/\mathbb{Q}}(\varphi^{-1}(\operatorname{Nm}_{k/\varphi E} \mathfrak{P}))\right) \\ &= \operatorname{Nm}_{E/\mathbb{Q}} \left(\prod\nolimits_{\varphi \in \Phi_v} \varphi^{-1}(\operatorname{Nm}_{k/\varphi E} \mathfrak{P})\right).\end{aligned}$$

From the definition of Φ_v, we see that $\prod_{\varphi \in \Phi_v} \varphi^{-1}(\operatorname{Nm}_{k/\varphi E} \mathfrak{P})$ is a power of $\mathfrak{p}_v$, and so this shows that

$$\mathfrak{p}_v^{m_v} = \prod\nolimits_{\varphi \in \Phi_v} \varphi^{-1}(\operatorname{Nm}_{k/\varphi E} \mathfrak{P}). \tag{17}$$

On taking the product over v, we obtain the required formula. □

COROLLARY 2.2 *With the hypotheses of the theorem, for all primes $\mathfrak{p}$ of E dividing p,*

$$\operatorname{ord}_{\mathfrak{p}}(\pi) = \sum\nolimits_{\varphi \in \Phi,\, \varphi^{-1}(\mathfrak{P}) = \mathfrak{p}} f(\mathfrak{P}/\varphi\mathfrak{p}). \tag{18}$$

Here $\varphi\mathfrak{p}$ is the image of $\mathfrak{p}$ in $\varphi\mathcal{O}_E \subset \varphi E \subset k$.

PROOF. Let $\mathfrak{p}$ be a p-adic prime ideal of $\mathcal{O}_E$, and let φ be a homomorphism $E \to k$. If $\mathfrak{p} = \varphi^{-1}(\mathfrak{P})$, then

$$\operatorname{ord}_{\mathfrak{p}}(\varphi^{-1}(\operatorname{Nm}_{k/\varphi E} \mathfrak{P})) = \operatorname{ord}_{\varphi\mathfrak{p}} \operatorname{Nm}_{k/\varphi E} \mathfrak{P} = f(\mathfrak{P}/\varphi\mathfrak{p}),$$

and otherwise it is zero. Thus, (18) is nothing more than a restatement of (15). □

COROLLARY 2.3 *With the hypotheses of the theorem, for all primes v of E dividing p,*

$$\frac{\operatorname{ord}_v(\pi)}{\operatorname{ord}_v(q)} = \frac{|\Phi \cap H_v|}{|H_v|} \tag{19}$$

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. We show that (18) implies (19) (and conversely) without assuming p to be unramified in E. Note that

$$\operatorname{ord}_v(q) = f(\mathfrak{P}/p) \cdot \operatorname{ord}_v(p) = f(\mathfrak{P}/p) \cdot e(\mathfrak{p}_v/p),$$

and that

$$|H_v| = e(\mathfrak{p}_v/p) \cdot f(\mathfrak{p}_v/p).$$

Therefore, the equality

$$\operatorname{ord}_v(\pi) = \sum\nolimits_{\varphi \in \Phi \cap H_v} f(\mathfrak{P}/\varphi\mathfrak{p}_v),$$

implies that

$$\frac{\operatorname{ord}_v(\pi)}{\operatorname{ord}_v(q)} = \sum\nolimits_{\varphi \in \Phi \cap H_v} \frac{1}{e(\mathfrak{p}_v/p) \cdot f(\mathfrak{p}_v/p)} = |\Phi \cap H_v| \cdot \frac{1}{|H_v|}$$

(and conversely). □

REMARK 2.4 (a) In the statement of Theorem 2.1, k can be replaced by a finite extension of $\mathbb{Q}_p$.

(b) The conditions in the statement are unnecessarily strong. For example, the formula holds without the assumption that p be unramified in E. See Theorem 3.2 below.

(c) When E is a subfield of k, Theorem 2.1 can be stated in terms of the reflex CM-type cf. Shimura and Taniyama 1961, §13.

APPLICATION 2.5 Let A be an abelian variety with complex multiplication by a CM-algebra E over a number field k, and let $\Phi \subset \operatorname{Hom}(E, k)$ be the type of A. Because $\operatorname{Tgt}_0(A)$ is an $E \otimes_{\mathbb{Q}} k$-module satisfying (1), k contains the reflex field E^* of (E, Φ) and we assume k is Galois over E^*. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_k$ at which A has good reduction, and let $\mathfrak{P} \cap \mathcal{O}_{E^*} = \mathfrak{p}$ and $\mathfrak{p} \cap \mathbb{Z} = (p)$. Assume

- ◇ that p is unramified in E,
- ◇ that $\mathfrak{p}$ is unramified in k, and
- ◇ that $\operatorname{End}(A) \cap E = \mathcal{O}_E$.

Let σ be the Frobenius element $(\mathfrak{P}, k/E^*)$ in $\operatorname{Gal}(k/E^*)$.[11] As σ fixes E^*, A and σA have the same CM-type and so they become isogenous over a finite extension of k. According to (1.35), there exists an $\mathfrak{a}$-multiplication $\lambda \colon A \to \sigma A$ over a finite extension of k whose reduction $\lambda_0 \colon A_0 \to A_0^{(p^{f(\mathfrak{p}/p)})}$ is the $p^{f(\mathfrak{p}/p)}$-power Frobenius map. Moreover,

$$\sigma^{f(\mathfrak{P}/\mathfrak{p})-1}\lambda \circ \cdots \circ \sigma\lambda \circ \lambda = \pi$$

where π is as in the statement of the theorem. Therefore, Theorem 2.1 shows that

$$\mathfrak{a}^{f(\mathfrak{P}/\mathfrak{p})} = N_\Phi(\operatorname{Nm}_{k/E^*}\mathfrak{P}) = N_\Phi(\mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}) = N_\Phi(\mathfrak{p})^{f(\mathfrak{P}/\mathfrak{p})},$$

and so

$$\mathfrak{a} = N_\Phi(\mathfrak{p}). \tag{20}$$

Notice that, for any m prime to p and such that $A_m(k) = A_m(\mathbb{C})$, the homomorphism λ agrees with σ on $A_m(k)$ (because it does on $A_{0,m}$).

NOTES The proof Theorem 2.1 in this section is essentially the original proof.

[11] So $\sigma(\mathfrak{P}) = \mathfrak{P}$ and $\sigma a \equiv a^{p^{f(\mathfrak{P}/\mathfrak{p})}} \mod \mathfrak{P}$ for all $a \in \mathcal{O}_k$.

3 The fundamental theorem over the reflex field.

Preliminaries from algebraic number theory

We review some class field theory (see, for example, Milne CFT, V). 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 for k is just an ideal in $\mathcal{O}_k$. For such a modulus $\mathfrak{m}$, $S(\mathfrak{m})$ denotes the set of finite primes v dividing $\mathfrak{m}$, and $k_{\mathfrak{m},1}$ 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 $\mathcal{O}_v/\mathfrak{p}_v^{\mathrm{ord}_v(\mathfrak{m})} = \mathcal{O}_v/\mathfrak{m}$. The ray class group modulo $\mathfrak{m}$ is

$$C_{\mathfrak{m}}(k) = I^{S(\mathfrak{m})}/i(k_{\mathfrak{m},1})$$

where i is the map sending an element to its principal ideal. The reciprocity map is an isomorphism

$$\mathfrak{a} \mapsto (\mathfrak{a}, L_{\mathfrak{m}}/k) \colon C_{\mathfrak{m}}(k) \to \mathrm{Gal}(L_{\mathfrak{m}}/k)$$

where $L_{\mathfrak{m}}$ is the ray class field of $\mathfrak{m}$.

LEMMA 3.1 *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

$$\mathrm{ord}_v(a) + \mathrm{ord}_v(\mathfrak{a}) \geq 0 \tag{21}$$

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 $\mathrm{ord}_v(\mathfrak{a}) < 0$, 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. □

The fundamental theorem in terms of ideals

THEOREM 3.2 *Let A be an abelian variety over $\mathbb{C}$ with complex multiplication by a CM-algebra E, and let $\Phi \subset \mathrm{Hom}(E, \mathbb{C})$ be the type of A. Assume that $\mathrm{End}(A) \cap E = \mathcal{O}_E$. Fix an integer $m > 0$, and let σ be an automorphism of $\mathbb{C}$ fixing E^*.*

(a) *There exists an ideal $\mathfrak{a}(\sigma)$ in E and an $\mathfrak{a}(\sigma)$-multiplication $\lambda \colon A \to \sigma A$ such that $\lambda(x) = \sigma x$ for all $x \in A_m$; moreover, the class $[\mathfrak{a}(\sigma)]$ of $\mathfrak{a}(\sigma)$ in $C_m(E)$ is uniquely determined.*

(b) *For any sufficiently divisible modulus $\mathfrak{m}$ for E^*, the ideal class $[\mathfrak{a}(\sigma)]$ depends only on the restriction of σ to the ray class field $L_{\mathfrak{m}}$ of $\mathfrak{m}$, and*

$$[\mathfrak{a}(\sigma)] = [N_\Phi(\mathfrak{b})] \text{ if } \sigma|L_{\mathfrak{m}} = (\mathfrak{b}, L_{\mathfrak{m}}/E^*). \tag{22}$$

PROOF. Because σ fixes E^*, the varieties A and σA have the same CM-types and so are E-isogenous. Therefore, there exists an $\mathfrak{a}$-multiplication $\lambda \colon A \to \sigma A$ for some ideal $\mathfrak{a} \subset \mathcal{O}_E$ (see

1.24). Recall (1.22) that λ has degree $(\mathcal{O}_E\colon\mathfrak{a})$. After possibly replacing λ with $\lambda\circ a$ for some $a\in\mathfrak{a}^{-1}$, it will have degree prime to m (apply 3.1). Then λ maps A_m isomorphically onto σA_m.

Let $\mathbb{Z}_m=\prod_{\ell|m}\mathbb{Z}_\ell$ and $\mathcal{O}_m=\mathcal{O}_E\otimes\mathbb{Z}_m$. Then $T_mA\overset{\text{def}}{=}\prod_{\ell|m}T_\ell A$ is a free $\mathcal{O}_m$-module of rank 1 (see 1.7). The maps

$$\begin{matrix} x\mapsto\sigma x \\ x\mapsto\lambda x\end{matrix}\colon T_mA\to T_m(\sigma A)$$

are both $\mathcal{O}_m$-linear isomorphisms, and so they differ by a homothety by an element α of $\mathcal{O}_m^\times$:

$$\lambda(\alpha x)=\sigma x,\quad \text{all } x\in T_mA.$$

For any $a\in\mathcal{O}_E$ sufficiently close to α, $\lambda\circ a$ will agree with σ on A_m. Thus, after replacing λ with $\lambda\circ a$, we will have

$$\lambda(x)\equiv\sigma x\mod m,\quad \text{all } x\in T_mA.$$

Now λ is an $\mathfrak{a}$-multiplication for an ideal $\mathfrak{a}=\mathfrak{a}(\sigma)$ that is well-defined up to an element of $i(E_{m,1})$.

Let σ' be a second element of $\mathrm{Gal}(\mathbb{C}/E^*)$, and let $\lambda'\colon A\to\sigma'A$ be an $\mathfrak{a}'$-multiplication acting as σ' on A_m (which implies that it has degree prime to m). Then $\sigma\lambda'$ is again an $\mathfrak{a}'$-multiplication (obvious from the definition 1.12), and so $\sigma\lambda'\circ\lambda$ is an $\mathfrak{a}\mathfrak{a}'$-multiplication $A\to\sigma'\sigma A$ (see 1.21) acting as $\sigma'\sigma$ on A_m. Therefore, the map $\sigma\mapsto\mathfrak{a}(\sigma)\colon\mathrm{Gal}(\mathbb{C}/E^*)\to C_m(E)$ is a homomorphism, and so it factors through $\mathrm{Gal}(k/E^*)$ for some finite abelian extension k of E^*, which we may take to be the ray class field $L_\mathfrak{m}$. Thus, we obtain a well-defined homomorphism

$$I^{S(\mathfrak{m})}(E^*)\to C_\mathfrak{m}(E^*)\to C_m(E)$$

sending an ideal $\mathfrak{a}^*$ in $I^{S(\mathfrak{m})}(E^*)$ to $[\mathfrak{a}(\sigma)]$ where $\sigma=(\mathfrak{a}^*,L_\mathfrak{m}/E^*)$. If $\mathfrak{m}$ is sufficiently divisible, then N_Φ also defines a homomorphism $I^{S(\mathfrak{m})}(E^*)\to C_\mathfrak{m}(E^*)\to C_m(E)$, and it remains to show that the two homomorphisms coincide.

According to §1, there exists a field $k\subset\mathbb{C}$ containing the ray class field $L_\mathfrak{m}$ and finite and Galois over E^* such that A has a model A_1 over k with the following properties:

- ◇ A_1 has complex multiplication by E over k and $\mathcal{O}_E=\mathrm{End}(A_1)\cap E$,
- ◇ A has good reduction at all the prime ideals of $\mathcal{O}_k$. and
- ◇ $A_m(k)=A_m(\mathbb{C})$.

Now (2.5) shows that the two homomorphisms agree on the prime ideals $\mathfrak{p}$ of $\mathcal{O}_{E^*}$ such $\mathfrak{p}$ is unramified in k and $\mathfrak{p}\cap\mathbb{Z}$ is unramified in E. This excludes only finitely many prime ideals of $\mathcal{O}_{E^*}$, and according to Dirichlet's theorem on primes in arithmetic progressions (e.g., Milne CFT V 2.5), the classes of these primes exhaust $C_\mathfrak{m}$. □

ASIDE 3.3 Throughout this subsection and the next, $\mathbb{C}$ can be replaced by an algebraic closure of $\mathbb{Q}$.

More preliminaries from algebraic number theory

We let $\hat{\mathbb{Z}}=\varprojlim\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{A}_f=\hat{\mathbb{Z}}\otimes\mathbb{Q}$. 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. For any adèle a, a_∞ and a_f denote its infinite and finite components. 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 $\mathbb{C}$. As usual, 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 Frobenius element. 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, $\mathrm{art}_k(a_\infty a_f)$ depends only on a_f, and we often regard art_k as a map $\mathbb{A}_{f,k}^\times \to \mathrm{Gal}(k^{\mathrm{ab}}/k)$. 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 $\mathbb{A}_{f,k}^\times$.

The cyclotomic character is the homomorphism $\chi_{\mathrm{cyc}}\colon \mathrm{Aut}(\mathbb{C}) \to \hat{\mathbb{Z}}^\times \subset \mathbb{A}_f^\times$ such that $\sigma\zeta = \zeta^{\chi_{\mathrm{cyc}}(\sigma)}$ for every root ζ of 1 in $\mathbb{C}$.

LEMMA 3.4 *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 (or see Milne 2005 §11 (50)). □

LEMMA 3.5 *Let E be a CM-field. For any $s \in \mathbb{A}_{f,E}^\times$ and automorphism σ of $\mathbb{C}$ such that* $\mathrm{art}_E(s) = \sigma|E^{\mathrm{ab}}$,

$$\mathrm{Nm}_{E/\mathbb{Q}}(s) \in \chi_{\mathrm{cyc}}(\text{œ}) \cdot \mathbb{Q}_{>0}.$$

PROOF. By class field theory,

$$\mathrm{art}_{\mathbb{Q}}(\mathrm{Nm}_{E/\mathbb{Q}}(s)) = \sigma|\mathbb{Q}^{\mathrm{ab}},$$

which equals $\mathrm{art}_{\mathbb{Q}}(\chi_{\mathrm{cyc}}(\sigma))$. Therefore $\mathrm{Nm}_{E/\mathbb{Q}}(s)$ and $\chi_{\mathrm{cyc}}(\text{œ})$ differ by an element of the kernel of $\mathrm{art}_{\mathbb{Q}}\colon \mathbb{A}_f^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$, which equals $\mathbb{A}_f^\times \cap (\mathbb{Q}^\times \cdot \mathbb{R}_{>0}) = \mathbb{Q}_{>0}$ (embedded diagonally). □

LEMMA 3.6 *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 $\bar{U}/U$ for any subgroup U of $\mathcal{O}_E^\times$ of finite index. A theorem of Chevalley (see Serre 1964, 3.5, or Artin and Tate 1961, Chap. 9, §1) 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 $\bar{U}/U$ is fixed by ι_E and, being isomorphic to $(\hat{\mathbb{Z}}/\mathbb{Z})^{[E:\mathbb{Q}]/2-1}$, it is uniquely divisible. □

LEMMA 3.7 *Let E be a CM-field and let Φ be a CM-type on E. For any $s \in \mathbb{A}_{f,E}^\times$ and automorphism σ of $\mathbb{C}$ such that* $\mathrm{art}_E(s) = \sigma|E^{\mathrm{ab}}$,

$$N_\Phi(s) \cdot \iota_E N_\Phi(s) \in \chi_{\mathrm{cyc}}(\sigma) \cdot \mathbb{Q}_{>0}.$$

PROOF. According to (3), p3,

$$N_\Phi(s) \cdot \iota_E N_\Phi(s) = \mathrm{Nm}_{E/\mathbb{Q}}(s),$$

and so we can apply (3.5). □

LEMMA 3.8 *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 3.9 *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 σ be an automorphism of $\mathbb{C}$ such that

$$\mathrm{art}_{E^*}(s) = \sigma|E^{*\mathrm{ab}} = \mathrm{art}_{E^*}(s').$$

Then (see 3.7),

$$N_\Phi(s)\cdot \iota_E N_\Phi(s) \in \chi_{\mathrm{cyc}}(\sigma)\cdot \mathbb{Q}_{>0} \ni N_\Phi(s')\cdot \iota_E N_\Phi(s').$$

Let $t = N_\Phi(s/s') \in \mathbb{A}_{f,E}^{\times}$. Then $t \in \mathrm{Ker}(\mathrm{art}_E)$ by (3.8) and $t\cdot\iota_E t \in \mathbb{Q}_{>0}$. Lemma 3.6 implies that the map $x \mapsto x\cdot\iota_E x$ is bijective on $\mathrm{Ker}(\mathrm{art}_E)/E^\times$; as $t\cdot\iota_E t \in E^\times$, so also does t. □

The fundamental theorem in terms of idèles

THEOREM 3.10 *Let A be an abelian variety over $\mathbb{C}$ with complex multiplication by a CM-algebra E, and let $\Phi \subset \mathrm{Hom}(E,\mathbb{C})$ be the type of A. Let σ be an automorphism of $\mathbb{C}$ fixing E^*. For any $s \in \mathbb{A}_{f,E^*}^{\times}$ with $\mathrm{art}_{E^*}(s) = \sigma|E^{*\mathrm{ab}}$, there exists a unique E-'isogeny' $\lambda\colon A \to \sigma A$ such that $\lambda(N_\Phi(s)\cdot x) = \sigma x$ for all $x \in V_f A$.*

REMARK 3.11 (a) It is obvious that λ is determined uniquely by the choice of an s such that $\mathrm{rec}(s) = \sigma|E^{*\mathrm{ab}}$. If s is replaced by s', then $N_\Phi(s') = a\cdot N_\Phi(s)$ with $a \in E^\times$ (see 3.9), and λ must be replaced by $\lambda\cdot a^{-1}$.

(b) The theorem is a statement about the E-'isogeny' class of A — if $\beta\colon A \to B$ is an E-'isogeny', and λ satisfies the conditions of the theorem for A, then $\sigma\beta\circ\lambda\circ\beta^{-1}$ satisfies the conditions for B. Therefore, in proving the theorem we may assume that $\mathrm{End}(A)\cap E = \mathcal{O}_E$.

(c) Let λ as in the theorem, let α 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. The condition on the Rosati involution means that

$$\psi(a\cdot x, y) = \psi(x, \iota_E a\cdot y), \quad x, y \in V_f A, \quad a \in \mathbb{A}_{f,E}. \tag{23}$$

Then, for $x, y \in V_f A$,

$$(\sigma\psi)(\sigma x, \sigma y) \stackrel{\mathrm{def}}{=} \sigma(\psi(x,y)) = \chi_{\mathrm{cyc}}(\sigma)\cdot\psi(x,y)$$

because $\psi(x,y) \in \mathbb{A}_f(1)$. Thus if λ is as in the theorem, then

$$\chi_{\mathrm{cyc}}(\sigma)\cdot\psi(x,y) = (\sigma\psi)(N_\Phi(s)\lambda(x), N_\Phi(s)\lambda(y)). \tag{24}$$

According to (3), p3, $N_\Phi(s)\cdot\iota_E N_\Phi(s) = N_{E^*/\mathbb{Q}}(s)$, and so, on combining (23) and (24), we find that

$$(c\psi)(x,y) = (\sigma\psi)(\lambda x, \lambda y),$$

with $c = \chi_{\mathrm{cyc}}(\sigma)/N_{E^*/\mathbb{Q}}(s) \in \mathbb{Q}_{>0}$ (see 3.5).

Let σ be an automorphism of $\mathbb{C}$ fixing E^*. Because σ fixes E^*, there exists an E-isogeny $\lambda\colon A \to \sigma A$. The maps

$$\begin{matrix} x \mapsto \sigma x \\ x \mapsto \lambda x \end{matrix} : V_f(A) \to V_f(\sigma A)$$

are both $\mathbb{A}_{f,E} \overset{\text{def}}{=} E \otimes \mathbb{A}_f$-linear isomorphisms. As $V_f(A)$ is free of rank one over $\mathbb{A}_{f,E}$,[12] they differ by a homothety by an element $\eta(\sigma)$ of $\mathbb{A}_{f,E}^\times$:

$$\lambda(\eta(\sigma)x) = \sigma x, \quad \text{all } x \in V_f(A). \tag{25}$$

When the choice of λ is changed, $\eta(\sigma)$ is changed only by an element of $E^\times$, and so we have a well-defined map

$$\mathrm{Aut}(\mathbb{C}/E^*) \to \mathbb{A}_{f,E}^\times/E^\times. \tag{26}$$

LEMMA 3.12 *For a suitable choice of λ, the quotient $t = \eta(\sigma)/N_\Phi(s)$ satisfies the equation $t\cdot\iota_E t = 1$ in $\mathbb{A}_{f,E}^\times$.*

PROOF. We know that

$$N_\Phi(s)\cdot\iota_E N_\Phi(s) \overset{(3)}{=} \mathrm{Nm}_{\mathbb{A}_{f,E^*}/\mathbb{A}_f}(s) \overset{(3.5)}{=} \chi_{\mathrm{cyc}}(\sigma)\cdot a$$

for some $a \in \mathbb{Q}_{>0}$.

A calculation as in (3.11c) shows that,

$$(c\psi)(x,y) = (\sigma\psi)(\lambda x, \lambda y), \text{ all } x, y \in \mathbb{A}_{f,E}^\times, \tag{27}$$

with $c = \chi_{\mathrm{cyc}}(\sigma)/\left(\eta(\sigma)\cdot\iota_E\eta(\sigma)\right)$. Now the discussion on p4 shows that c is a totally positive element of F. Thus

$$\eta(\sigma)\cdot\iota_E\eta(\sigma) = \chi_{\mathrm{cyc}}(\sigma)/c, \quad c \in F_{\gg 0}. \tag{28}$$

Let $t = \eta(\sigma)/N_\Phi(s)$. Then

$$t\cdot\iota_E t = 1/ac \in F_{\gg 0}. \tag{29}$$

Being a totally positive element of F, ac is a local norm from E at the infinite primes, and (29) shows that it is also a local norm at the finite primes. Therefore we can write $ac = e\cdot\iota_E e$ for some $e \in E^\times$. Then

$$te\cdot\iota_E(te) = 1.$$

□

The map $\eta\colon \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/E^*) \to \mathbb{A}_{f,E}^\times/E^\times$ is a homomorphism[13], and so it factors through $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/E^*)^{\mathrm{ab}}$. When combined with the Artin map, it gives a homomorphism $\eta'\colon \mathbb{A}_{f,E^*}^\times/E^{*\times} \to \mathbb{A}_{f,E}^\times/E^\times$.

---

[12] This is even true when $R \overset{\text{def}}{=} \mathrm{End}(A)\cap E$ is not the whole of $\mathcal{O}_E$ because, for all ℓ, $V_\ell A$ is free of rank one over $E_\ell \overset{\text{def}}{=} E\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$, and for all ℓ not dividing $(\mathcal{O}_E\colon R)$, $T_\ell A$ is free of rank one over $R_\ell \overset{\text{def}}{=} R\otimes_{\mathbb{Z}}\mathbb{Z}_\ell$ (see 1.7).

[13] Choose E-isogenies $\alpha\colon A \to \sigma A$ and $\alpha'\colon A \to \sigma' A'$, and let

$$\alpha(sx) = \sigma x$$
$$\alpha'(s'x) = \sigma' x.$$

Then $\sigma\alpha'\circ\alpha$ is an isogeny $A \to \sigma\sigma' A$, and

$$(\sigma\alpha'\circ\alpha)(ss'x) = (\sigma\alpha')(\alpha(ss'x)) = (\sigma\alpha')(\sigma(s'x)) = \sigma(\alpha'(s'x)) = \sigma\sigma' x.$$

Choose an integer $m > 0$. For some modulus $\mathfrak{m}$, there exist a commutative diagrams

$$\begin{array}{ccc} \mathbb{A}_{f,E^*}^{\times}/E^{*\times} & \longrightarrow & \mathbb{A}_{f,E}^{\times}/E^{\times} \\ \downarrow{\scriptstyle \text{onto}} & & \downarrow{\scriptstyle \text{onto}} \\ C_{\mathfrak{m}}(E^*) & \longrightarrow & C_m(E) \end{array}$$

with the top map either N_{Φ} or by η' and the vertical maps the obvious maps (Milne CFT, V 4.6). The bottom maps in the two diagrams agree by Theorem 3.2, which implies that $t \stackrel{\text{def}}{=} \eta(\sigma)/N_{\Phi}(s)$ lies in the common kernel of the maps $\mathbb{A}_{f,E}^{\times}/E^{\times} \to C_m(E)$ for $m > 0$. But this common kernel is equal to the kernel of the Artin map $\mathbb{A}_{f,E}^{\times}/E^{\times} \to \mathrm{Gal}(E^{\mathrm{ab}}/E)$. As $t \cdot \iota_E t = 1$ (see 3.12), $t = 1$ (see 3.6).

NOTES The proof in this subsection is that sketched in Milne 2005. Cf. Shimura 1970, 4.3, and Shimura 1971, pp117–121, p129.

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 α be a polarization of (A, i). Recall (1.1, 1.3) 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 3.13 *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 $\mathrm{art}_{E^*}(s) = \sigma|E^{*\mathrm{ab}}$, 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 $(E, \Phi; f\mathfrak{a}, t \cdot \chi_{\mathrm{cyc}}(\sigma)/f\bar{f})$ where $f = N_{\Phi}(s) \in \mathbb{A}_{f,E}^{\times}$;*

(b) *the diagram*

$$\begin{array}{ccc} E/\mathfrak{a} & \xrightarrow{\theta_0} & A(\mathbb{C}) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \sigma} \\ E/f\mathfrak{a} & \xrightarrow{\theta_0'} & \sigma A(\mathbb{C}) \end{array}$$

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 3.10, there exists an isogeny $\lambda\colon A \to \sigma A$ such that $\lambda(N_{\Phi}(s) \cdot x) = \sigma x$ for all $x \in V_f A$. Then $H_1(\lambda)$ 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 $H_1(\lambda)(e_0)$ for $H_1(\sigma A, \mathbb{Q})$. The statement now follows immediately from Theorem 3.10 and (3.11c). □

4 The fundamental theorem over $\mathbb{Q}$

The first three subsections follow Tate 1981 and the last subsection follows Deligne 1981.

We begin by reviewing some notations. We let $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{A}_f = \hat{\mathbb{Z}} \otimes \mathbb{Q}$. 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 $\mathbb{C}$. 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. When k is totally imaginary, we also write art_k for the map $\mathbb{A}_{f,k}^\times \to \mathrm{Gal}(k^{\mathrm{ab}}/k)$ that it defines. The cyclotomic character $\chi = \chi_{\mathrm{cyc}} \colon \mathrm{Aut}(\mathbb{C}) \to \hat{\mathbb{Z}}^\times \subset \mathbb{A}_f^\times$ is the homomorphism such that $\sigma\zeta = \zeta^{\chi(\sigma)}$ for every root of 1 in $\mathbb{C}$. The composite

$$\mathrm{art}_k \circ \chi_{\mathrm{cyc}} = \mathrm{Ver}_{k/\mathbb{Q}}, \tag{30}$$

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 $\bigoplus_{\varphi \in \Phi} \varphi$ 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 1.3).

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 4.1 *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 some uniformization θ'.

(b) *It is possible to choose θ' so that*

$$\begin{array}{ccccc}
\mathbb{A}_{f,E} & \longrightarrow & \mathbb{A}_{f,E}/\mathfrak{a}\otimes\hat{\mathbb{Z}}\simeq E/\mathfrak{a} & \xrightarrow{\theta} & A_{\mathrm{tors}}\\
\downarrow f & & & & \downarrow\sigma\\
\mathbb{A}_{f,E} & \longrightarrow & \mathbb{A}_{f,E}/(f\mathfrak{a}\otimes\hat{\mathbb{Z}})\simeq E/f\mathfrak{a} & \xrightarrow{\theta'} & \sigma A_{\mathrm{tors}}
\end{array}$$

commutes, where A_{tors} denotes the torsion subgroup of A (and then θ' is uniquely determined),

We now restate the theorem in a more canonical form. Let

$$TA\overset{\mathrm{def}}{=}\varprojlim A_m(\mathbb{C})\simeq\varprojlim(\tfrac{1}{m}H_1(A,\mathbb{Z})/H_1(A,\mathbb{Z}))\simeq H_1(A,\hat{\mathbb{Z}})$$

(limit over all positive integers m), and let

$$V_fA\overset{\mathrm{def}}{=}TA\otimes_{\mathbb{Z}}\mathbb{Q}\simeq H_1(A,\mathbb{Q})\otimes_{\mathbb{Q}}\mathbb{A}_f.$$

Then ψ gives rise to a pairing

$$\psi_f=\varprojlim\psi_m\colon V_fA\times V_fA\to\mathbb{A}_f(1)$$

where $\mathbb{A}_f(1)=(\varprojlim\mu_m(\mathbb{C}))\otimes\mathbb{Q}$.

THEOREM 4.2 *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[14] diagram*

$$\begin{tikzcd}
V_f(A) \arrow[r, "f"] \arrow[dr, "\sigma"'] & V_f(A) \arrow[d, "\alpha\otimes 1"] \\
& V_f(\sigma A)
\end{tikzcd}$$

commutes.

LEMMA 4.3 *The statements (4.1) and (4.2) are equivalent.*

[14] 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.

PROOF. Let θ and θ' be as in (4.1), 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 $\chi = \chi_{\text{cyc}}(\sigma)/f \cdot \iota f$ — it is an element of $E^\times$. Then

$$\psi(\theta_1(x),\theta_1(y)) = \mathrm{Tr}_{E/\mathbb{Q}}(tx\cdot\iota y)$$
$$(\sigma\psi)(\theta_1'(x),\theta_1'(y)) = \mathrm{Tr}_{E/\mathbb{Q}}(t\chi x\cdot\iota y)$$

and

$$\begin{array}{ccc}
\mathbb{A}_{f,E} & \xrightarrow{\theta_1} & V_f(A) \\
\downarrow f & & \downarrow \sigma \\
\mathbb{A}_{f,E} & \xrightarrow{\theta_1'} & V_f(\sigma A)
\end{array}$$

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 (4.2) and choose θ_1' so that $\alpha = \theta_1' \circ \theta_1^{-1}$. The argument can be reversed to deduce (4.1). □

Definition of $f_\Phi(\sigma)$

Let (E,Φ) be a CM-pair with E a field. In (3.9) 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 $i\colon E^{\text{ab}} \hookrightarrow \mathbb{C}$. Choose elements $w_\rho \in \mathrm{Aut}(\mathbb{C})$, one for each $\rho \in \mathrm{Hom}(E,\mathbb{C})$, such that

$$w_\rho \circ i|E = \rho, \quad w_{\iota\rho} = \iota w_\rho.$$

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 $i^{-1}\circ w_{\sigma\rho}^{-1}\sigma w_\rho \circ i \in \mathrm{Gal}(E^{\text{ab}}/E)$, and we can define $F_\Phi : \mathrm{Aut}(\mathbb{C}) \to \mathrm{Gal}(E^{\text{ab}}/E)$ by

$$F_\Phi(\sigma) = \prod_{\varphi\in\Phi} i^{-1}\circ w_{\sigma\varphi}^{-1}\sigma w_\varphi \circ i.$$

LEMMA 4.4 *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 4.5 *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

$$F_{\Phi}(\sigma) = \prod_{\varphi \in \Phi} w_{\sigma\varphi}^{-1} \sigma w_{\varphi} \mod \operatorname{Aut}(\mathbb{C}/E^{\mathrm{ab}})$$

where the w_ρ are elements of $\operatorname{Aut}(\mathbb{C})$ such that

$$w_\rho | E = \rho, \quad w_{\iota\rho} = \iota w_\rho.$$

PROPOSITION 4.6 *For any* $\sigma \in \operatorname{Aut}(\mathbb{C})$, *there is a unique* $f_\Phi(\sigma) \in \mathbb{A}_{f,E}^\times / E^\times$ *such that*

(a) $\operatorname{art}_E(f_\Phi(\sigma)) = F_\Phi(\sigma)$;

(b) $f_\Phi(\sigma) \cdot \iota f_\Phi(\sigma) = \chi(\sigma) E^\times$, $\chi = \chi_{\text{cyc}}$.

PROOF. Since art_E is surjective, there is an $f \in \mathbb{A}_{f,E}^\times / E^\times$ such that $\operatorname{art}_E(f) = F_\Phi(\sigma)$. We have

$$\begin{aligned} \operatorname{art}_E(f \cdot \iota f) &= \operatorname{art}_E(f) \cdot \operatorname{art}_E(\iota f) \\ &= \operatorname{art}_E(f) \cdot \iota \operatorname{art}_E(f) \iota^{-1} \\ &= F_\Phi(\sigma) \cdot F_{\iota\Phi}(\sigma) \\ &= \operatorname{Ver}_{E/\mathbb{Q}}(\sigma), \end{aligned}$$

where $\operatorname{Ver}_{E/\mathbb{Q}} \colon \operatorname{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})^{\mathrm{ab}} \to \operatorname{Gal}(\mathbb{Q}^{\mathrm{al}}/E)^{\mathrm{ab}}$ is the transfer (Verlagerung) map. As $\operatorname{Ver}_{E/\mathbb{Q}} = \operatorname{art}_E \circ \chi$, it follows that $f \cdot \iota f = \chi(\sigma) E^\times$ modulo $\operatorname{Ker}(\operatorname{art}_E)$. Lemma 3.6 shows that $1 + \iota$ acts bijectively on $\operatorname{Ker}(\operatorname{art}_E)$, and so there is a unique $a \in \operatorname{Ker}(\operatorname{art}_E)$ such that $a \cdot \iota a = (f \cdot \iota f / \chi(\sigma)) E^\times$; we must take $f_\Phi(\sigma) = f/a$. □

REMARK 4.7 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 (Langlands 1979, §5).

PROPOSITION 4.8 *The maps* $f_\Phi \colon \operatorname{Aut}(\mathbb{C}) \to \mathbb{A}_{f,E}^\times / E^\times$ *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

$$\operatorname{art}_E(f) = F_{\tau\Phi}(\sigma) \cdot F_\Phi(\tau) = \prod_{\varphi \in \Phi} w_{\sigma\tau\varphi}^{-1} \cdot \sigma w_{\tau\varphi} \cdot w_{\tau\varphi}^{-1} \cdot \tau w_\varphi = F_\Phi(\sigma\tau)$$

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 $\operatorname{Aut}(\mathbb{C}/E^*) = \{\sigma \in \operatorname{Aut}(\mathbb{C}) \mid \sigma\Phi = \Phi\}$. Then $\Phi \operatorname{Aut}(\mathbb{C}/E) \stackrel{\text{def}}{=} \bigcup_{\varphi \in \Phi} \varphi \cdot \operatorname{Aut}(\mathbb{C}/E)$ is stable under the left action of $\operatorname{Aut}(\mathbb{C}/E^*)$, and we write

$$\operatorname{Aut}(\mathbb{C}/E)\Phi^{-1} = \bigcup \psi \cdot \operatorname{Aut}(\mathbb{C}/E^*) \qquad \text{(disjoint union)}.$$

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 $\sigma \in \operatorname{Aut}(\mathbb{C}/E^*)$, and let $a \in \mathbb{A}_{f,E^*}^\times / E^{*\times}$ be such that $\operatorname{art}_{E^*}(a) = \sigma$; then (4.1) is true after f has been replaced by $N_\Phi(a)$ (see Theorem 3.10; 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 (4.1).

PROPOSITION 4.9 *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

$$F_j(\sigma) = \prod_{\varphi \in \Phi_j} w_{\sigma\varphi}^{-1}\sigma w_\varphi \quad (\mathrm{mod}\,\mathrm{Aut}(\mathbb{C}/E^{\mathrm{ab}})).$$

We begin by showing that $F_j(\sigma) = \mathrm{art}_E(b_j)$. The basic properties of Artin's reciprocity law show that

$$\begin{tikzcd}
\mathbb{A}_{f,E}^{\times} \arrow[r, "\text{injective}"] \arrow[d, "\mathrm{art}_E"] & \mathbb{A}_{f,\sigma L_j}^{\times} \arrow[r, "\sigma_j^{-1}"] \arrow[d, "\mathrm{art}_{\sigma L_j}"] & \mathbb{A}_{f,L_j}^{\times} \arrow[r, "\mathrm{Nm}_{L_j/K}"] \arrow[d, "\mathrm{art}_{L_j}"] & \mathbb{A}_{f,K}^{\times} \arrow[d, "\mathrm{art}_K"'] \\
\mathrm{Gal}(E^{\mathrm{ab}}/E) \arrow[r, "V_{\sigma_j L_j/E}"] & \sigma_j\,\mathrm{Gal}(L_j^{\mathrm{ab}}/L_j)\sigma_j^{-1} \arrow[r, "\mathrm{ad}\sigma_j^{-1}"] & \mathrm{Gal}(L_j^{\mathrm{ab}}/L_j) \arrow[r, "\text{restriction}"] & \mathrm{Gal}(K^{\mathrm{ab}}/K)
\end{tikzcd}$$

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 $\sigma_j\,\mathrm{Aut}(\mathbb{C}/L_j)\sigma_j^{-1}$ in $\mathrm{Aut}(\mathbb{C}/E^*)$, 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 $\mathrm{Aut}(\mathbb{C}/E^{\mathrm{ab}})$.

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 3.7), this shows that $N_\Phi(a) \in f_\Phi(\sigma)$. □

Proof of Theorem 4.2 up to a sequence of signs

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 4.10 *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,

$$(\sigma\psi)(\sigma x, \sigma y) = \sigma(\psi(x, y)) \qquad x, y \in V_f(A)$$
$$(\alpha\psi)(\alpha x, \alpha y) = \psi(x, y) \qquad x, y \in V_f(A).$$

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 4.11 (a) On replacing x and y with αx and αy in (4.10), 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 (4.10), 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 4.12 *The maps* $g_\Phi : \mathrm{Aut}(\mathbb{C}) \to \mathbb{A}_{f,E}^\times/E^\times$ *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) $g_\Phi(\sigma) \cdot \iota g_\Phi(\sigma) = \chi_{\mathrm{cyc}}(\sigma)E^\times$.

PROOF. (a) Choose E-linear isomorphisms $\alpha: H_1(A, \mathbb{Q}) \to H_1(\tau A, \mathbb{Q})$ and $\beta: H_1(\tau A, \mathbb{Q}) \to H_1(\sigma\tau A, \mathbb{Q})$, 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 $(A, E \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q})$ has type (E, Φ), then $(A, E \overset{\tau^{-1}}{\to} E \to \mathrm{End}(A) \otimes \mathbb{Q})$ has type $(E, \Phi\tau^{-1})$. The formula in (b) can be proved by transport of structure.

(c) Complex conjugation $\iota: A \to \iota A$ is a homeomorphism (relative to the complex topology) and so induces an E-linear isomorphism $\iota_1: H_1(A, \mathbb{Q}) \to H_1(A, \mathbb{Q})$. The map $\iota_1 \otimes 1: V_f(A) \to V_f(\iota A)$ is ι again, and so on taking $\alpha = \iota_1$, we find that $g = 1$.

(d) This was proved in (4.11d). □

Theorem (4.2) (hence also 4.1) 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

$$e_\Phi(\sigma) = g_\Phi(\sigma)/f_\Phi(\sigma) \in \mathbb{A}_{f,E}^\times/E^\times. \tag{31}$$

PROPOSITION 4.13 *The maps* $e_\Phi : \mathrm{Aut}(\mathbb{C}) \to \mathbb{A}_{f,E}^\times/E^\times$ *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 (4.8) and (4.12), and (d) follows from (4.6b) and (4.12d). 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 4.14 *Let F be the largest totally real subfield of E; then $e_\Phi(\sigma) \in \mathbb{A}^\times_{f,F}/F^\times$ and $e_\Phi(\sigma)^2 = 1$; moreover, $e_\Phi(\sigma)$ depends only on the effect of σ on E^*, and is 1 if $\sigma|E^* = \mathrm{id}$.*

PROOF. Recall that σ fixes E^* if and only if $\sigma\Phi = \Phi$, in which case (4.13e) 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 $e_\Phi(\sigma) \in (\mathbb{A}^\times_{f,E}/E^\times)^{\langle\iota_E\rangle}$, which equals $\mathbb{A}^\times_{f,F}/F^\times$ by Hilbert's Theorem 90.[15] Finally, (d) shows that $e_\Phi(\sigma)^2 = 1$. □

COROLLARY 4.15 *Part (a) of (4.1) is true; part (b) of (4.1) becomes true when f is replaced by ef with $e \in \mathbb{A}^\times_{f,F}$, $e^2 = 1$.*

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 (Milne CFT VIII 1.1), we can correct e to achieve $e^2 = 1$. Now (4.1) is true with f replaced by ef, but e (being a unit) does not affect part (a) of (4.1). □

It remains to show that:

$$\text{for all CM-fields } E \text{ and CM-types } \Phi \text{ on } E,\ e_\Phi = 1. \tag{32}$$

Completion of the proof

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 $\mathbb{A}^\times_{f,E}/E^\times$. Then, as in (4.14, 4.15),

$$e_\Phi(\sigma) \in \mu_2(\mathbb{A}_{f,F})/\mu_2(F), \quad \sigma \in \mathrm{Aut}(\mathbb{C}).$$

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 (4.13), we need:

(f) let E' be a CM-field containing E, and let Φ' be the extension of Φ to E'; then for any $\sigma \in \mathrm{Aut}(\mathbb{C})$,

$$e_\Phi(\sigma) = e_{\Phi'}(\sigma) \quad (\text{in } \mathbb{A}^\times_{f,E'}/E'^\times). \tag{33}$$

[15] The cohomology sequence of the sequence of $\mathrm{Gal}(E/F)$-modules

$$1 \to E^\times \to \mathbb{A}^\times_{f,E} \to \mathbb{A}^\times_{f,E}/E^\times \to 1$$

is

$$1 \to F^\times \to \mathbb{A}^\times_{f,F} \to (\mathbb{A}^\times_{f,E}/E^\times)^{\mathrm{Gal}(E/F)} \to H^1(\mathrm{Gal}(E/F), E^\times) = 0$$

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. 1.26).

Note that (f) shows that $e_{\Phi'} = 1 \implies e_\Phi = 1$, and so it suffices (32) 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

$$\sum\nolimits_i n_i[\Phi_i] = 0 \implies \prod\nolimits_i e_{\Phi_i}(\sigma)^{n_i} = 1 \text{ for all } \sigma \in \mathrm{Aut}(\mathbb{C}).$$

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 4.13) 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

$$\bar\rho\colon \mathrm{Hom}(E,\mathbb{C}) \to \mathbb{Z}/2\mathbb{Z},$$

such that either (weight 0)

$$\bar\rho(\varphi) + \bar\rho(\iota\varphi) = 0 \text{ for all } \varphi \tag{34}$$

or (weight 1)

$$\bar\rho(\varphi) + \bar\rho(\iota\varphi) = 1 \text{ for all } \varphi.$$

We now prove that $e_{\bar\rho} = 1$ if $\bar\rho$ is of weight 0. The condition (34) means that $\bar\rho(\varphi) = \bar\rho(\iota\varphi)$, and so $\bar\rho$ arises from a function $q\colon \mathrm{Hom}(F,\mathbb{C}) \to \mathbb{Z}/2\mathbb{Z}$:

$$\bar\rho(\varphi) = q(\varphi|F).$$

We write $e_q = e_{\bar\rho}$. 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[16]

$$e_q(\sigma) = \prod\nolimits_{\varphi\colon F\to\mathbb{C}} \varphi^{-1}(e(\sigma))^{q(\varphi)},\ \sigma \in \mathrm{Aut}(\mathbb{C}).$$

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,

$$e^F(\sigma) = \mathrm{Nm}_{F'/F}\, e^{F'}(\sigma).$$

[16]For each $\varphi\colon F \to \mathbb{C}$, choose an extension (also denoted φ) of φ to E. Then

$$\bar\rho = \sum\nolimits_{\varphi'\colon E\to\mathbb{C}} \bar\rho(\varphi')\varphi' = \sum\nolimits_{\varphi\colon F\to\mathbb{C}} q(\varphi)(\varphi + \iota\varphi)$$

and so

$$e_q(\sigma) \overset{\text{def}}{=} e_{\bar\rho}(\sigma) = \prod\nolimits_\varphi e_{(1+\iota)\varphi}(\sigma)^{q(\varphi)} = \prod\nolimits_\varphi \varphi^{-1}(e_{1+\iota}(\sigma))^{q(\varphi)}$$

— we can take $e(\sigma) = e_{1+\iota}(\sigma)$.

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 (32). We know that $e_{\bar{\rho}}$ depends only on the weight of $\bar{\rho}$, 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 4.14) that $e_\Phi(\sigma)$ depends only on $\sigma|E^* = \mathbb{Q}[\sqrt{-1}]$. But $e_\Phi(1) = 1 = e_\Phi(\iota)$ by (4.13c).

ASIDE 4.16 Throughout, should allow E to be a CM-algebra. Should restate Theorem 4.2 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 $\mathbb{C}$).

Bibliography

ARTIN, E. AND TATE, J. 1961. Class field theory. Harvard, Dept. of Mathematics. Reprinted by Benjamin, 1968, and by Addison-Wesley, 1990.

BOURBAKI, N. TG. Topologie Générale. Éléments de mathématique. Hermann, Paris. Chap. I, II, Hermann 1965 (4th edition); Chap. III, IV, Hermann 1960 (3rd edition) (English translation available from Springer).

DELIGNE, P. 1981. Letter to Tate, dated October 8, 1981. Not generally available.

DELIGNE, P. 1982. Motifs et groupes de Taniyama, pp. 261–279. *In* Hodge cycles, motives, and Shimura varieties, Lecture Notes in Mathematics. Springer-Verlag, Berlin. Available at www.jmilne.org/math/.

LANGLANDS, R. P. 1979. Automorphic representations, Shimura varieties, and motives. Ein Märchen, pp. 205–246. *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. Available online at the LANGLANDS ARCHIVE.

MILNE, J. S. 1986. Abelian varieties, pp. 103–150. *In* Arithmetic geometry (Storrs, Conn., 1984). Springer, New York.

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. Version with additional notes available at www.jmilne.org/math/.

MILNE, J. S. 2006. Complex multiplication. Preliminary version, April 7, 2006, available at www.jmilne.org/math/.

MILNE, J. S. CFT. Class field theory, v3.1, May 6, 1997. Available at www.jmilne.org/math/.

MUMFORD, D. 1970. Abelian varieties. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, by Oxford University Press.

SERRE, J.-P. 1964. Sur les groupes de congruence des variétés abéliennes. *Izv. Akad. Nauk SSSR Ser. Mat.* 28:3–20.

SERRE, J.-P. AND TATE, J. 1968. Good reduction of abelian varieties. *Ann. of Math. (2)* 88:492–517.

SHIH, K.-Y. 1976. Anti-holomorphic automorphisms of arithmetic automorphic function fields. *Ann. of Math. (2)* 103:81–102.

SHIMURA, G. 1970. On canonical models of arithmetic quotients of bounded symmetric domains. *Ann. of Math. (2)* 91:144–222.

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. 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. (Shimura, Abelian varieties with complex multiplication and modular functions, Princeton, 1998, is an expanded version of this work, and retains most of the same numbering.).

TATE, J. T. 1981. On conjugation of abelian varieties of CM-type. Handwritten manuscript, 8pp, April 1981. Not generally available.

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.