Complex multiplication of abelian varieties

Margaret Bilu

Contents

Introduction

The theory of complex multiplication takes its origins in the beginning of the twentieth century with the study of elliptic curves having an endomorphism ring strictly larger than $\mathbf{Z}$, by mathematicians like Kronecker, Deuring and Hasse, whom we now recognise as being among the founders of class field theory. The goal was primarily to get explicit class field constructions for some number fields, aiming at what became known as Kronecker's Jugendtraum: a partial answer to Hilbert's 12th problem, asking for a generalisation of the Kronecker-Weber theorem. Elliptic curves with complex multiplication indeed provide a complete solution to this problem for quadratic imaginary fields. After some serious breakthroughs in algebraic geometry, and in particular in the theory of abelian varieties, by Weil, Shimura and Taniyama, these results could be generalised to abelian varieties of higher dimensions ([3],[4]). This led to the construction of some explicit finite abelian extensions of a type of number fields called CM-fields. Though the answers it has given to Hilbert's 12th problem until now are far from being complete, complex multiplication has become a theory of its own, widely studied because of its important role in other fields of number theory like Shimura varieties.

In this essay, after giving an overview of the theory for elliptic curves to motivate the introduction of the additional technicalities that are needed for Shimura's theorem, we are going to focus on the theory of complex multiplication of abelian varieties, the main goal being the proof of the main theorem of complex multiplication over the reflex field. It describes how an abelian variety with complex multiplication behaves under the action of an automorphism σ of $\mathbf{C}$ fixing a field called the reflex field. Such an abelian variety together with some polarisation is indeed characterised up to isomorphism by a set of objects we will call its type, and the following theorem gives the type of A^σ in terms of it using a map called the reflex norm. Moreover, the second part of the theorem gives a reinterpretation of the action of σ on the torsion points of A.

Theorem 0.1 *Let (K,Φ) be a CM-type and $\mathcal{P}=(A,\iota,\mathcal{C})$ a polarised abelian variety of type $(K,\Phi,\mathfrak{a},\tau)$ with respect to an isomorphism $\xi:\mathbf{C}^n/u(a)\longrightarrow A$. Fix $\sigma\in Aut(\mathbf{C}/K')$ and choose $s\in\mathbf{A}_K^*$ such that $\sigma_{|K'^{ab}}=[s,K']$. Then there is a unique complex analytic isomorphism*

$$\xi':\mathbf{C}^n/u(N_\Phi(s)^{-1}\mathfrak{a})\longrightarrow A^\sigma$$

having the following properties:

(1) $\mathcal{P}^\sigma$ is of type $(K,\Phi,N_\Phi(s)^{-1}\mathfrak{a},N((s))\tau)$ with respect to ξ'.

(2) There is a commutative diagram

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{N_\Phi(s)^{-1}} & K/N_\Phi(s)^{-1}\mathfrak{a} \\ {\scriptstyle \xi\circ u}\downarrow & & \downarrow{\scriptstyle \xi'\circ u} \\ A & \xrightarrow{\sigma} & A^\sigma \end{array}$$

The field K' occurring in the statement is called the reflex field of K. This theorem describes the reciprocity map

$$\mathbf{A}_{K'}^*\longrightarrow \mathrm{Gal}(K'^{\mathrm{ab}}/K')$$

and we will be able to prove that the field of moduli of $(A,\iota,\mathcal{C})$ is an abelian extension of K' and to compute the corresponding subgroup of $\mathbf{A}_{K'}^*$. The second part of the theorem will be

important to show that other abelian extensions of K' are obtained using torsion points of A and to give the corresponding subgroups.

Outline of the essay: Section 1 is an introductory section, reviewing some results from the theory of complex multiplication of elliptic curves and motivating what follows. Section 2 is a recall of basic facts, mainly on abelian varieties and on class field theory. Section 3 is crucial for the understanding of Theorem 0.1, containing all important definitions and preliminary constructions leading to the statement and proof of it. Among other things, we are going to define CM-fields, the type of an abelian variety and the reflex norm, as well as classify abelian varieties with complex multiplication in terms of these notions. Section 4 contains the theorem itself, with a detailed sketch of the proof. Finally, Section 5 shows how the theorem can be used to construct class fields of CM-fields, relating them to fields of moduli of certain abelian varieties.

Sources: Most of the results and proofs in this essay come from Shimura's book *Abelian varieties with complex multiplication* ([3]). For the review of the elliptic curves case, I equally used Silverman's account in [5] and Shimura's in [4]. Some light modifications in the statements and proofs, as well as subsection 3.3 and the classifications in subsections 3.4 and 3.5 were inspired by Milne's *Complex multiplication* ([2]).

Acknowledgments: I thank Prof. A.J. Scholl for setting this essay, giving me useful advice and answering my questions.

Notations and conventions. Fields are always commutative. Rings are assumed to have a unit, and homomorphisms of rings are required to map units to units. For every $x \in \mathbf{C}$, the complex conjugate of x is denoted $\bar{x}$. The action of an algebraic automorphism σ is on the right: the image of x by σ is written x^σ, and $x^{\sigma_1\sigma_2} = (x^{\sigma_1})^{\sigma_2}$. This notation, though sometimes quite confusing, will help us to distinguish them from analytic actions and therefore will stress the importance of the link the main theorem of complex multiplications creates between them. For an algebraic variety V, V^σ denotes the variety obtained by applying σ to the coefficients of the equations defining V.

A number field is a finite extension of $\mathbf{Q}$. We write $N_{K/\mathbf{Q}}(x)$, $\mathrm{Tr}_{K/\mathbf{Q}}$ for the norm and trace of an element of K, and $N(\mathfrak{a})$ for the norm of an ideal $\mathfrak{a}$ of K. An étale algebra over a field k is a finite product of finite separable field extensions of k. In particular, an étale $\mathbf{Q}$-algebra is a finite product of number fields. If $W = K_1 \times \ldots \times \mathrm{K}_r$ is an étale $\mathbf{Q}$-algebra, we define its ring of integers to be $\mathcal{O}_W = \mathcal{O}_{K_1} \times \ldots \times \mathcal{O}_{K_r}$. For an element $x \in W$, we sometimes write $x = (x_1, \ldots, x_r)$ where $x_i \in K_i$ for all i. By a fractional ideal in W we will understand a product $\mathfrak{a}_1 \times \ldots \times \mathfrak{a}_r \subset W$ such that $\mathfrak{a}_i$ is a fractional ideal of K_i of all i. Equivalently, it is an additive subgroup $\mathfrak{a} \subset W$ such that $\mathcal{O}_W\mathfrak{a} \subset \mathfrak{a}$. We say that $\mathfrak{a}$ is an integral ideal if $\mathfrak{a}$ moreover is contained in $\mathcal{O}_W$. We define the norm of $\mathfrak{a}$, $N(\mathfrak{a})$, to be the product of the norms of the $\mathfrak{a}_i$. We define also for all $x = (x_1, \ldots, x_r) \in E$,

$$\mathrm{Tr}_{W/\mathbf{Q}}(x) = \mathrm{Tr}_{K_1/\mathbf{Q}}(x_1) + \ldots + \mathrm{Tr}_{K_r/\mathbf{Q}}(x_r).$$

1 A quick review of the elliptic curves case

This section is very sketchy as most of the results stated here will be proven later in the more general abelian varieties case. It is mainly meant to play an introductory role and to serve as a basis to explain what is needed for the generalisation. Let E be an elliptic curve over $\mathbf{C}$. Its equation can be chosen to be of the form $y^2 = x^3 + Ax + B$, and it is isomorphic to a complex torus $\mathbf{C}/\Lambda$ where Λ is a lattice in $\mathbf{C}$. The endomorphisms of E can through this isomorphism be seen as complex analytic endomorphisms of $\mathbf{C}/\Lambda$, which can be shown to be exactly the $\mathbf{C}$-linear maps $\alpha : \mathbf{C} \longrightarrow \mathbf{C}$ such that $\alpha(\Lambda) \subset \Lambda$, and every such map is given by multiplication by an element $a \in \mathbf{C}$ such that $a\Lambda \subset \Lambda$. Therefore,

$$\mathrm{End}(E) \cong \{a \in \mathbf{C} |\ a\Lambda \subset \Lambda\} \subset \mathbf{C}. \tag{1}$$

We know that $\mathbf{Z} \subset \mathrm{End}(E)$, as multiplication by n is a non-torsion element of $\mathrm{End}(E)$ for every integer n. A short computation using (1) shows that $\mathrm{End}(E)$, as well as Λ, are contained in a quadratic imaginary field K, so that in the case where $\mathrm{End}(E) \neq \mathbf{Z}$, $\mathrm{End}(E)$ is an order in K, namely the order of the lattice Λ. In particular, if $\mathrm{End}(E) = \mathcal{O}_K$, Λ is a fractional ideal in K. The torsion points in E correspond through the isomorphism $E \cong \mathbf{C}/\mathfrak{a}$ to the $\mathbf{Z}$-submodule $K/\mathfrak{a}$: more precisely, if $m > 0$ is an integer the m-torsion points of E correspond to the submodule $m^{-1}\mathfrak{a}/\mathfrak{a}$.

Referring to 4.1 for the definition of the multiplication by an idele map, we can state the main theorem of complex multiplication for elliptic curves:

Theorem 1.1 *(Main theorem of complex multiplication for elliptic curves) Fix the following objects:*

K a quadratic imaginary field

E an elliptic curve over $\mathbf{C}$ such that $End_{\mathbf{Q}}(E) \cong K$.

σ an automorphism of $\mathbf{C}$ over K

$s \in \mathbf{A}_K^*$ an idele of K satisfying $[s, K] = \sigma_{|K^{ab}}$.

Fix moreover an isomorphism $\xi : \mathbf{C}/\mathfrak{a} \longrightarrow E$ where $\mathfrak{a}$ is a lattice in K. Then there is a unique complex analytic isomorphism $\xi' : \mathbf{C}/s^{-1}\mathfrak{a} \longrightarrow E^\sigma$ making the following diagram commute:

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\ s^{-1}\ } & K/s^{-1}\mathfrak{a} \\ {\scriptstyle\xi}\downarrow & & \downarrow{\scriptstyle\xi'} \\ E & \xrightarrow{\ \sigma\ } & E^\sigma \end{array}$$

This theorem gives us information on the reciprocity map $\mathbf{A}_K^* \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$. To determine for example the class group corresponding to the field $K(j)$ where j is the $j-$invariant of E, take $\sigma \in \mathrm{Gal}(K^{\mathrm{ab}}/K(j))$. Then $E \cong E^\sigma$, so the lattices $\mathfrak{a}$ and $s^{-1}\mathfrak{a}$ need to be homothetic, that is, there exists $\alpha \in K$ such that $\mathfrak{a} = \alpha s^{-1}\mathfrak{a}$. The corresponding subgroup of $\mathbf{A}_K^*$ is therefore easily seen to be $\{s \in \mathbf{A}_K^* \mid \exists \alpha \in K \text{ such that } s\mathfrak{a} = \alpha\mathfrak{a}\}$. In the same manner we can determine the class groups corresponding to extensions containing j and some torsion point of the elliptic curve, as stated in the following proposition.

Proposition 1.2 *Let K, E, $\mathfrak{a}$, ξ as in Theorem 1.1, and let $h : E \longrightarrow E/Aut(E) \cong \mathbf{P}^1$ be a Weber function for E. Let moreover $w \in K/\mathfrak{a}$, so that $t = \xi(w)$ is a torsion point of E, and define*

$$T = \{s \in \mathbf{A}_K^* |\ s\mathfrak{a} = \mathfrak{a},\ sw = w\}.$$

Then the field $K(j, h(t))$ is the class field of K corresponding to the subgroup K^*T of $\mathbf{A}_K^*$.

The Weber function used in this statement is necessary, as it can be seen that $K(j,t)$ (meaning that we adjoin to $K(j)$ the x and y coordinates of the point t of the elliptic curve E) is not an abelian extension of $K(j)$. The Weber function enables us to eliminate some extra automorphisms that make it non-abelian. For most elliptic curves (that is, when $j \neq 0, 1728$) the automorphism group is $\{\pm 1\}$, and h can simply be taken to be the x-coordinate function, which eliminates the $(x, y) \mapsto (x, -y)$ automorphism of E.

Using the characterisation of the kernel of the reciprocity map, one even proves that adjoining the j-invariant and torsion points is the only way to get abelian extensions of K, that is, K^{ab} is generated over K by the j-invariant j and all $h(t)$ for all torsion points $t \in E$. Moreover, $K(j)$ is always Galois and $\text{Gal}(K(j)/K)$ is isomorphic to the group of classes of $\mathcal{O}$-ideals. In particular, in the case where $\text{End}(E) \cong \mathcal{O}_K$, it is isomorphic to the ideal class group:

Theorem 1.3 *Let K be a quadratic imaginary field, and let E be an elliptic curve such that $End(E) \cong \mathcal{O}_K$, j its j-invariant. Then $K(j)$ is the Hilbert class field of K.*

In the same way, the case where $\text{End}(E) = \mathcal{O}_K$ also gives us a complete description of all ray class fields of K: for $\mathfrak{c}$ an integral ideal in K, denote by $E[\mathfrak{c}]$ the $\mathfrak{c}$-torsion points of E, that is,

$$E[\mathfrak{c}] = \{t \in E \mid ct = 0 \text{ for all } c \in \mathfrak{c}\},$$

where ct denotes of course the image of t by the endomorphism of E associated to c through $\text{End}(E) \cong \mathcal{O}_K$.

Theorem 1.4 *Let K be a quadratic imaginary field, E an elliptic curve such that $End(E) \cong \mathcal{O}_K$, j its j-invariant, $\mathfrak{c}$ an integral ideal in K. Fix a Weber function h for E. Then $K(j, h(E[\mathfrak{c}]))$ is the ray class field of K modulo $\mathfrak{c}$.*

As a conclusion, the main theorem of complex multiplication for elliptic curves is a powerful tool for constructing class fields of a quadratic imaginary field. When used with an elliptic curve whose endomorphism ring is the ring of integers $\mathcal{O}_K$, it even yields a description of the ray class fields of K, obtained with the j-invariant and torsion points of this elliptic curve.

Changes that need to be made to generalise this to abelian varieties. The overall approach stays the same: to a special kind of field K, we associate a geometric object A, and generate class fields thanks to fields of moduli coming from this object, as well as torsion points on this object. Let us state the major differences that nevertheless appear, as well as some helpful similarities:

1. As in the elliptic curves case, the fields for which we will get results are sufficiently large fields that can be embedded into $\text{End}_{\mathbf{Q}}(A)$ for A an abelian variety. It turns out that such fields are totally imaginary quadratic extensions of totally real number fields. They will be called CM-fields.

2. Now, the way a CM-field K is embedded into $\mathrm{End}_{\mathbf{Q}}(A)$ also has its importance. For a quadratic imaginary field there are two possible embeddings that are complex conjugate to each other, and one of them is chosen canonically using differential forms. Here there will be $2n$ embeddings, and a particular choice $\Phi = \{\phi_1, \ldots, \phi_n\}$ of n of them such that no two of them are equal or conjugate to each other will be called a CM-type. The obtained results will depend on the chosen Φ.

3. Given a quadratic imaginary field K, it was sufficient to consider an elliptic curve with complex multiplication by K. Now, there will be two fields involved: consider a CM-field K and an abelian variety A with complex multiplication by K. Looking as in the main theorem for elliptic curves at the action $A \longrightarrow A^\sigma$ of an automorphism of $\mathbf{C}$ on A, we will see that for A and A^σ to be isogenous, we will need σ to preserve the CM-type. An essential difficulty lies then in the fact that at this condition σ doesn't necessarily fix K as in the elliptic curves case: it permutes the elements of Φ, so fixes a field generated by all symmetric algebraic expressions involving values of the ϕ_i's. This field will be called the reflex field K', and will be the one for which we will be able to construct class fields. Of course, $K' = K$ for a quadratic imaginary field K.

4. For a quadratic imaginary field K, choosing a principal elliptic curve E with complex multiplication by K (i.e. such that $\mathrm{End}(E) \cong \mathcal{O}_K$), unramified extensions of K are obtained as subfields of $K(j_E)$. This is the field of moduli of (E, ι), where $\iota : K \longrightarrow \mathrm{End}_{\mathbf{Q}}(E)$ is the complex multiplication embedding. For a CM-field K, considering just a principal abelian variety with complex multiplication by K won't be sufficient, since an abelian variety alone doesn't define a field of moduli, having too many automorphisms. Therefore, we will be always working with polarised abelian varieties $(A, \mathcal{C})$, and the unramified extension of K' we will get will be $k_{A,\iota,\mathcal{C}}$, the field of moduli of the system $(A, \iota, \mathcal{C})$ with $\iota : K \longrightarrow \mathrm{End}_{\mathbf{Q}}(A)$.

5. Ramified extensions of conductor dividing some integral ideal $\mathfrak{c} \subset K'$ will then be obtained, as in the quadratic imaginary case, by adding the images of $\mathfrak{c}$-torsion points of a principal variety by a generalisation of the Weber function: again, the fact of having a finite number of automorphisms, and so the polarisation, is important.

6. For a quadratic imaginary K we get a complete classification of all finite abelian extensions of K. This is not the case for a general CM-field K: we will obtain some class fields thanks to different choices of the CM-type Φ, but we won't get all extensions.

7. Though all the above explanations are in terms of CM-fields for simplicity, as we will see in subsection 3.3, the biggest commutative object that can be contained in $\mathrm{End}_{\mathbf{Q}}(A)$ for A with complex multiplication is in general not necessarily a CM-field, but a CM-algebra, that is, a finite product of CM-fields. Therefore, to be completely general, we will work with CM-algebras and not only CM-fields. Everything will generalise quite easily by replacing K by a CM-algebra W: we will basically just need to take products everywhere to extend our results.

The following comparative table is an attempt to sum these differences up:

Initial data	Quadratic imaginary field K	CM-algebra W with CM-type Φ, inducing reflex type (K', Φ')
Associated geometric object	Elliptic curve E such that $\mathrm{End}_{\mathbf{Q}}(E) \cong K$	polarised abelian variety $(A, \mathcal{C})$ with $\iota : W \hookrightarrow \mathrm{End}_{\mathbf{Q}}(A)$
Reciprocity map described by main theorem	$\mathbf{A}_K^* \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$	$\mathbf{A}_{K'}^* \longrightarrow \mathrm{Gal}(K'^{\mathrm{ab}}/K')$
Obtained unramified class fields for principal object	$H = K(j_E)$ field of moduli of (E, ι)	Field of moduli of $(A, \iota, \mathcal{C})$
Obtained ramified class fields for principal object	$K(j, h(E[\mathfrak{c}]))$, h Weber function	$k_{A,\iota,\mathcal{C}}(h(A[\mathfrak{c}]))$, h Kummer variety quotient map

2 Preliminary definitions and properties

2.1 Some facts about abelian varieties

In this subsection we will recall without proof all the facts about abelian varieties that will be used in this essay. By an abelian variety over a field k we will here mean a projective group variety over k. The group law of an abelian variety is always commutative, and therefore written additively. A fundamental fact for our purpose is the fact that a complex abelian variety is isomorphic to a complex torus:

Fact 2.1 *If A is an abelian variety of dimension n over $\mathbf{C}$, it can be seen as a complex manifold, and there is a complex analytic group isomorphism $\theta : A \longrightarrow \mathbf{C}^n/\Lambda$ where $\Lambda \subset \mathbf{C}^n$ is a lattice.*

Recall that a free $\mathbf{Z}$-module $\Lambda \in \mathbf{C}^n$ of rank $2n$ is called a lattice if $\Lambda \otimes \mathbf{R} = \mathbf{C}^n$, or equivalently, if $\Lambda \otimes \mathbf{Q}$ is dense in $\mathbf{C}^n$.

Remark When $n = 1$, this corresponds to the classical Uniformisation Theorem for elliptic curves, the converse of which is also true: any complex torus of dimension one is isomorphic to an elliptic curve. We will see below in the paragraph on polarisations that this is false for higher-dimensional abelian varieties.

Homomorphisms and endomorphisms

Definition 2.2 *Let A and B be abelian varieties. A homomorphism of A into B is a rational map $\lambda : A \longrightarrow B$ that is also a group homomorphism. If $A = B$, it is called an endomorphism. If A and B have same dimension, λ is called an isogeny.*

We will denote $\mathrm{End}(A)$ the ring of endomorphisms of the abelian variety A, and $\mathrm{End}_{\mathbf{Q}}(A) = \mathrm{End}(A) \otimes \mathbf{Q}$. If A and B have same dimension and if there is an isogeny from A into B, there is also an isogeny from B into A, and A and B are then called isogenous. An isogeny, being a rational map between varieties of same dimension, has finite kernel.

We can also consider homomorphisms from one abelian variety into the other from the complex torus point of view. If $\lambda : A \longrightarrow B$ is an isogeny, it induces a homomorphism

$\mathbf{C}^n/\Lambda_1 \longrightarrow \mathbf{C}^n/\Lambda_2$ of complex tori, which in turn induces a linear map $\lambda : \mathbf{C}^n \longrightarrow \mathbf{C}^n$ sending the first lattice into the second, i.e. such that $\lambda(\Lambda_1) \subset \Lambda_2$. The evoked correspondences are exact and can be summed up by saying there is a ring isomorphism:

$$\mathrm{Hom}(A, B) \cong \{M \in \mathcal{M}_n(\mathbf{C}) |\ M\Lambda_1 \subset \Lambda_2\}.$$

In the same way, denoting by $\mathbf{Q}\Lambda$ the $\mathbf{Q}$-vector space $\Lambda \otimes \mathbf{Q}$, there is a $\mathbf{Q}$-algebra isomorphism

$$\mathrm{Hom}_{\mathbf{Q}}(A, B) \cong \{M \in \mathcal{M}_n(\mathbf{C}) |\ M\mathbf{Q}\Lambda_1 \subset \mathbf{Q}\Lambda_2\}. \tag{2}$$

The corresponding $\mathbf{Q}$-algebra homomorphism $\mathrm{End}_{\mathbf{Q}}(A) \longrightarrow \mathcal{M}_n(\mathbf{C})$ is sometimes (for example in Shimura's works [3],[4]) called the analytic representation of $\mathrm{End}_{\mathbf{Q}}(A)$.

Polarisations A complex torus $\mathbf{C}^n/\Lambda$ of dimension $n > 1$ is not always a projective variety. It does have a projective embedding if there exists an ample divisor on $\mathbf{C}^n/\Lambda$, or, equivalently, a Riemann form:

Definition 2.3 *Let Λ be a lattice in $\mathbf{C}^n$. An $\mathbf{R}$-bilinear form $E : \mathbf{C}^n \times \mathbf{C}^n \longrightarrow \mathbf{R}$ is called a Riemann form on $\mathbf{C}^n/\Lambda$ if it satisfies the following conditions:*

(i) $E(\Lambda \times \Lambda) \subset \mathbf{Z}$;

(ii) *E is alternating, i.e. $E(z, w) = -E(w, z)$ for all $z, w \in \mathbf{C}^n$.*

(iii) *The bilinear form $(z, w) \mapsto E(z, \sqrt{-1}w)$ is a symmetric positive definite form.*

We say the complex torus $\mathbf{C}^n/\Lambda$ is polarised if there is a Riemann form on $\mathbf{C}^n/\Lambda$. For an abstract abelian variety without fixing any isomorphism with a complex torus, we can define a polarisation in the following way:

Definition 2.4 *A polarisation of A is a set $\mathcal{C}$ of divisors of A satisfying the following three conditions:*

(i) *$\mathcal{C}$ contains an ample divisor;*

(ii) *If X and Y are elements of $\mathcal{C}$, there are positive integers m, n such that mX is algebraically equivalent to nY.*

(iii) *$\mathcal{C}$ is maximal under the conditions (i) and (ii).*

A polarised abelian variety is then a couple $(A, \mathcal{C})$ where $\mathcal{C}$ is a polarisation of the abelian variety A.

Remark: Let us stress that, under the definitions we have given, it is equivalent for an abelian variety to be polarised or to have a Riemann form, but choosing a Riemann form on it is not equivalent to choosing a polarisation.

A homomorphism $\lambda : (A_1, \mathcal{C}_1) \longrightarrow (A_2, \mathcal{C}_2)$ of polarised abelian varieties is a homomorphism $\lambda : A_1 \longrightarrow A_2$ such that $\lambda^{-1}\mathcal{C}_2 = \mathcal{C}_1$. There is a divisor $X_0 \in \mathcal{C}$ such that every $X \in \mathbf{C}$ is algebraically equivalent to mX_0 for some positive integer m. X_0 is called the *basic polar divisor* of $\mathcal{C}$.

Let us go back now to the case where A is defined over $\mathbf{C}$, and choose an isomorphism $\xi : \mathbf{C}^n/\Lambda \longrightarrow A$, through which every divisor X on A defines a divisor $\xi^{-1}(X)$ on the complex

torus. Then condition (i) of the previous definition is equivalent to the fact that every divisor $X \in \mathcal{C}$ determines a Riemann form. We mean by this that every such divisor X gives a divisor $\xi^{-1}(X)$ on the torus, that is the divisor of some theta-function, which in turn gives a Riemann form.

A polarisation $\mathcal{C}$ of the abelian variety A defines an involution (that is, an antiautomorphism of order 1 or 2) on $\mathrm{End}_{\mathbf{Q}}(A)$ in the following way: choose any Riemann form E determined by a divisor in $\mathcal{C}$. Then, identifying for simplicity $\mathrm{End}_{\mathbf{Q}}(A)$ with a subalgebra of $\mathcal{M}_n(\mathbf{C})$, E gives an involution γ of $\mathrm{End}_{\mathbf{Q}}(A)$ by

$$E(\lambda x, y) = E(x, \lambda^{\gamma} y)$$

for every $\lambda \in \mathrm{End}_{\mathbf{Q}}(A)$. It can be proven that this involution is independent of the choice of E, of the torus $\mathbf{C}^n/\Lambda$ and of the isomorphism ξ. It is therefore called the involution of $\mathrm{End}_{\mathbf{Q}}(A)$ determined by $\mathcal{C}$.

2.2 Idelic formulation of class field theory

Let F be an algebraic number field and $\mathcal{M}_F$ the set of places of F. Denote

$$\mathbf{A}_F^* = \left\{ (x_v)_v \in \prod_{v \in \mathcal{M}_F} F_v^* \mid x_v \in \mathcal{O}_{F,v}^* \text{ for almost all } v \right\}$$

the idele group of F. Choose a normalised valuation $v_{\mathfrak{p}}$ on every $F_{\mathfrak{p}}$. For an idele $s \in \mathbf{A}_F^*$, define

$$(s) = \prod_{\mathfrak{p} \text{ prime of } F} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}} s_{\mathfrak{p}}}$$

the ideal associated to s. Class field theory states that there exists a surjective homomorphism

$$\begin{array}{ccc} \mathbf{A}_F^* & \longrightarrow & \mathrm{Gal}(F^{\mathrm{ab}}/F) \\ s & \mapsto & [s, F] \end{array}$$

called the reciprocity map, such that for every finite abelian extension L/F of conductor $\mathfrak{c}_{L/F}$ and for every idele s whose ideal (s) is divisible only by primes unramified in L,

$$[s, F]_{|L} = ((s), L/F),$$

where $(\,\cdot\,, L/F) : I_F(\mathfrak{c}_{L/F}) \longrightarrow \mathrm{Gal}(L/F)$ is the Artin map for the extension L/F. In particular, let $\mathfrak{p}$ be a prime of F, L an abelian extension of F unramified at $\mathfrak{p}$, and $\varpi = (\ldots, 1, \varpi_{\mathfrak{p}}, 1, \ldots)$ an idele such that $\varpi_{\mathfrak{p}}$ is a uniformiser in $F_{\mathfrak{p}}$, and that $\varpi_{\mathfrak{q}} = 1$ for $\mathfrak{q} \neq \mathfrak{p}$. Then $(\varpi) = \mathfrak{p}$, and therefore $[\varpi, F]_{|L} = (\mathfrak{p}, L/F)$ is the Frobenius element for L/F at $\mathfrak{p}$.
For any integral ideal $\mathfrak{c}$ in F, put

$$U(\mathfrak{c}) = \left\{ s \in \mathbf{A}_F^* |\ s_{\mathfrak{p}} \in\ \mathcal{O}_{F,\mathfrak{p}}^* \text{ and } s_{\mathfrak{p}} \equiv 1 \pmod{\mathfrak{c}\mathcal{O}_{F,\mathfrak{p}}} \text{ for all primes } \mathfrak{p} \text{ in } F \right\}.$$

When several fields are involved, we will write $U_F(\mathfrak{c})$. Moreover, if $\mathfrak{c} = (c)$ is a principal ideal, we will write $U(c)$ instead of $U((c))$. The results of class field theory are essential to us mostly for the sake of the following result, which states that $F^* U(\mathfrak{c})$ is exactly the class group corresponding to the ray class field $F_{\mathfrak{c}}$ of F modulo $\mathfrak{c}$ and therefore enables us to perform a crucial decomposition in the proof of the main theorem of complex multiplication.

Fact 2.5 *(Idelic characterisation of ray class fields) There is an isomorphism*

$$\mathbf{A}_F^*/F^*U(\mathfrak{c}) \longrightarrow \mathrm{Gal}(F_\mathfrak{c}/F).$$

In other words, an idele s acting trivially on $F_\mathfrak{c}$ can be written $s = ce$ where $c \in F^*$ and $e \in U(\mathfrak{c})$.

2.3 Lattices in étale algebras

Let $W = K_1 \times \ldots \times K_r$ be an étale algebra of dimension d over $\mathbf{Q}$. This section gives a collection of results about a type of object that will be in constant use throughout the essay.

Definition 2.6 *A lattice in a number field is a free $\mathbf{Z}$-submodule of maximal rank. A lattice in W is a product $\mathfrak{a} = \mathfrak{a}_1 \times \ldots \times \mathfrak{a}_r$ such that for all i, $\mathfrak{a}_i$ is a lattice in K_i.*

Lemma 2.7 *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two lattices in W. Then there exists an integer m such that $m\mathfrak{a} \subset \mathfrak{b}$.*

Proof. Let $e_1, \ldots, e_d$ (resp. $f_1, \ldots, f_d$) be a $\mathbf{Z}$-basis of $\mathfrak{a}$ (resp. of $\mathfrak{b}$). Then $e_1, \ldots, e_d$ and $f_1, \ldots, f_d$ are both bases of the $\mathbf{Q}$-vector space W. Therefore for every i there are $a_{i1}, \ldots, a_{ij} \in \mathbf{Q}$ such that

$$e_i = a_{i1}f_1 + \ldots + a_{id}f_d.$$

Taking m to be a common multiple of the denominators of all the a_{ij}, we get $me_i \in \mathfrak{b}$ for all i, so $m\mathfrak{a} \subset \mathfrak{b}$. □

Definition 2.8 *An order in W is a subring of W that is also a lattice.*

To any lattice $\mathfrak{a}$ in W we can associate an order in the following way:

$$\mathcal{O} = \{\alpha \in W |\ \alpha\mathfrak{a} \subset \mathfrak{a}\}.$$

It is clear that $\mathcal{O}$ is a $\mathbf{Z}$-submodule and a subring of W, so it suffices to check that $\mathbf{Q}\mathcal{O} = W$. But $W = \mathbf{Q}\mathfrak{a}$ since $\mathfrak{a}$ is a lattice. Therefore for every $x \in W$ and every $a \in \mathfrak{a}$, $xa \in W = \mathbf{Q}\mathfrak{a}$, so $x\mathfrak{a} \subset \mathbf{Q}\mathfrak{a}$, so $x \in \mathbf{Q}\mathcal{O}$.
$\mathfrak{a}$ is said to be an ideal for an order $\mathcal{O}$ if $\mathcal{O}\mathfrak{a} \subset \mathfrak{a}$. In particular, $\mathfrak{a}$ is an ideal for the order associated to it. The best-known example of this kind of situation is the case of the maximal order of W, the ring of integers $\mathcal{O}_W$. Its ideals are by definition the fractional ideals of W. The terminology "maximal order" comes from the fact that it contains all other orders in W.

Lemma 2.9 *The product $\mathfrak{a}\mathfrak{b}$ of two lattices in W is again a lattice.*

Proof. $\mathfrak{a}\mathfrak{b}$ is clearly a $\mathbf{Z}$-submodule of W. Let $\mathcal{O}$ be the order associated to $\mathfrak{a}$. Then by Lemma 2.7, there are integers $m, n > 0$ such that $m\mathcal{O} \subset \mathfrak{b}$ and $n\mathfrak{b} \subset \mathcal{O}$. Thus, $m\mathfrak{a} \subset \mathfrak{a}\mathfrak{b} \subset \frac{1}{n}\mathfrak{a}$, so $\mathfrak{a}$ is free by the second inclusion, and of rank d by the first. □

3 Abelian varieties with complex multiplication

3.1 CM-fields and CM-types

Definition 3.1 *A CM-field K is a totally imaginary quadratic extension of a totally real quadratic field. In other words, it is of the form $K = K_0(\sqrt{\alpha})$ where K_0 is a totally real field, that is, a number field whose embeddings into $\mathbf{C}$ are all real and $\alpha \in K_0$ is mapped through each of these embeddings to a negative real.*

Example: Imaginary quadratic fields are clearly CM-fields. A cyclotomic field $\mathbf{Q}(\zeta)$ for a primitive m-th root of unity ζ with $m > 2$ is totally imaginary, and is a quadratic extension of the totally real field $\mathbf{Q}(\zeta + \bar{\zeta})$, so is a CM-field as well.

We can characterise CM-fields intrinsically without using generators thanks to the following lemma:

Lemma 3.2 *A number field K is a CM-field if and only if the following two conditions are satisfied:*

(i) Complex conjugation induces a non-trivial automorphism of K

(ii) Every embedding of $K \hookrightarrow \mathbf{C}$ commutes with complex conjugation.

Proof. For the *if* part, use the definition to write any element z of K as $z = x + \sqrt{\alpha}y$ with x, y in the totally real field K_0 (in particular, x, y and α are real, and $\alpha < 0$). Then $\bar{z} = x - \sqrt{\alpha}y \in K$ and condition (i) is clearly satisfied. Take an embedding $\sigma : K \hookrightarrow \mathbf{C}$. Then x^σ and y^σ are real and $(\sqrt{\alpha})^\sigma$ is a square root of the negative real α^σ, so is quadratic imaginary. Therefore we have

$$\overline{z^\sigma} = \overline{x^\sigma + (\sqrt{\alpha})^\sigma y^\sigma} = x^\sigma - (\sqrt{\alpha})^\sigma y^\sigma = \bar{z}^\sigma,$$

which proves condition (ii).

Assume now K is a number field satisfying conditions (i) and (ii). Let K_0 be the subfield of K fixed by complex conjugation. It contains $\mathbf{Q}$ and is a proper subfield of K according to condition (i). Complex conjugation being of order two, K is an extension of degree 2 of K_0, and, completing the square, we can write it as $K_0(\sqrt{\alpha})$ for some α in K_0. Let $\sigma : K_0 \hookrightarrow \mathbf{C}$ be an embedding. Then by condition (ii) and by definition of K_0, for any $x \in K_0$,

$$\overline{x^\sigma} = \bar{x}^\sigma = x^\sigma,$$

which shows K_0 is totally real. Moreover, extending σ to an embedding of K into $\mathbf{C}$, $\left((\sqrt{\alpha})^{\,\sigma}\right)^2 = \alpha^\sigma = \alpha$. If, for some σ, α is nonnegative, $\sqrt{\alpha}^\sigma$ will be real. But then by condition (ii) $(\sqrt{\alpha})^{\,\sigma} = \overline{(\sqrt{\alpha})^\sigma} = \left(\overline{\sqrt{\alpha}}\right)^\sigma$, and thus $\sqrt{\alpha}$ is real, which contradicts condition (i) and proves the second implication. □

The following lemma is a direct consequence of this criterion:

Lemma 3.3 *A composite of CM-fields is a CM-field.*

Proof. Clear, as any embedding of a composite of number fields into $\mathbf{C}$ induces embeddings of these fields. □

Another consequence is:

Lemma 3.4 *The Galois closure of a CM-field is a CM-field.*

Proof. Let K be a CM-field and L its Galois closure. As L clearly satisfies condition (i) of Lemma 3.2, we only need to check condition (ii). We can write $K = \mathbf{Q}(\alpha_1)$ and $L = \mathbf{Q}(\alpha_1, \ldots, \alpha_r)$ where $\alpha_1, \alpha_2, \ldots, \alpha_r$ are all roots of the minimal polynomial of α_1. For every i, there is an embedding $\phi_i : K \hookrightarrow \mathbf{C}$ sending α_1 to α_i. For every $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$ and for every $i = 1, \ldots, r$, applying condition (ii) for the embeddings $\phi_i\sigma$ and ϕ_i of K,

$$\overline{\alpha_i^\sigma} = \overline{\alpha_1^{\phi_i\sigma}} = \overline{\alpha_1}^{\,\phi_i\sigma} = \overline{\alpha_1^{\phi_i}}^{\,\sigma} = \overline{\alpha_i}^{\,\sigma},$$

which proves condition (ii) on L. $\square$

The set of complex embeddings of a CM-field can by definition be split into pairs $\{\phi, \bar{\phi}\}$. We will call a choice of exactly one element of each of these pairs a CM-type:

Definition 3.5 *A CM-type $\Phi = \{\phi_1, \ldots, \phi_n\}$ on a CM-field K is a set of complex embeddings of K such that $\Phi \cap \overline{\Phi} = \emptyset$ and $\Phi \cup \overline{\Phi}$ (where $\overline{\Phi} = \{\overline{\phi_1}, \ldots, \overline{\phi_n}\}$) is the set of all complex embeddings of K.*

Remark:

1. Another way of saying this is that the elements of Φ induce exactly all the distinct archimedean valuations on K.
2. We will call both the set Φ alone and the pair (K, Φ) a CM-type.

Definition 3.6 *We define the determinant and the trace of the CM-type Φ for every $x \in K$ by*

$$\det \Phi(x) = \prod_{i=1}^{n} x^{\phi_i}, \quad \operatorname{tr} \Phi(x) = \sum_{i=1}^{n} x^{\phi_i}.$$

CM-algebras. We will also need the more general notion of a CM-algebra:

Definition 3.7 *A CM-algebra is a product $K_1 \times \ldots \times K_r$ of finitely many CM-fields K_i.*

Note that in particular a CM-algebra is always commutative, and that it is an étale algebra. We can associate to a CM-algebra E a set Φ called the CM-type by simply taking $\Phi = \Phi_1 \times \ldots \times \Phi_r$ where the Φ_i are CM-types of the fields K_i: every element $\phi \in \Phi$ is of the form $(\phi_1, \ldots, \phi_n)$ where $\phi_i \in \Phi_i$ and for all $x = (x_1, \ldots, x_r) \in E$, $\phi(x) = \sum_{i=1}^{r} \phi_i(x_i)$. We can also define $\operatorname{tr} \Phi(x) = \sum_{i=1}^{r} \operatorname{tr} \Phi_i(x_i)$ for all $x = (x_1, \ldots, x_r) \in E$.

3.2 The reflex field

Let (K, Φ) be a CM-type. We are going to associate to it another CM-type, called the reflex of (K, Φ). First, let us define the underlying field:

Definition 3.8 *The reflex field of K with respect to the CM-type Φ is defined to be the field K' generated over $\mathbf{Q}$ by $\operatorname{tr} \Phi(x)$ for all $x \in K$, i.e.:*

$$K' = \mathbf{Q}\left(\{\operatorname{tr} \Phi(x)\}_{x \in K}\right) = \mathbf{Q}\left(\left\{\sum_{i=1}^{n} x^{\phi_i}\right\}_{x \in K}\right).$$

We are going to use the criterion of Lemma 3.2 to prove K' is a CM-field. First of all, it is a finite extension of $\mathbf{Q}$ because it is clearly contained in the Galois closure of K. By condition (ii) of the lemma for K, $\overline{\operatorname{tr} \Phi(x)} = \operatorname{tr} \Phi(\bar{x})$ for all $x \in K$, so complex conjugation induces an automorphism on K'. Independence of characters and the fact that Φ is a CM-type imply this automorphism is non-trivial, which proves condition (i). Now if we take $\sigma \in \operatorname{Aut}(\mathbf{C})$, using condition (ii) for K twice, first for the embeddings $\phi_i\sigma$, then for the embeddings ϕ_i,

$$\overline{\operatorname{tr} \Phi(x)^{\sigma}} = \sum_{i=1}^{n} \overline{x^{\phi_i\sigma}} = \sum_{i=1}^{n} \bar{x}^{\phi_i\sigma} = \sum_{i=1}^{n} \overline{x^{\phi_i}}^{\,\sigma} = \left(\overline{\operatorname{tr} \Phi(x)}\right)^{\sigma}.$$

This proves condition (ii) for K'. Thus, K' is a CM-field.

To define the reflex type, we are going to give another characterisation of K', in terms of Galois theory. Let L be the Galois closure of K and G its Galois group. As remarked above, we have $K' \subset L$. Denote by H and H' respectively the subgroups of G corresponding to K and K'.

Extend every ϕ_i to an element of G, again denoted ϕ_i. Every element of G, restricted to K, must coincide with some element of $\Phi \cup \bar{\Phi}$. Therefore, putting $S = \cup_{i=1}^{n} H\phi_i$,

$$G = \bigcup_{i=1}^{n} H\phi_i \cup \bigcup_{i=1}^{n} H\overline{\phi_i} = S \cup \bar{S} \quad \text{and} \quad S \cap \bar{S} = \emptyset. \tag{3}$$

Proposition 3.9 *Let G, H, H', S be as above. Then*

$$H' = \{g \in G \mid Sg = S\}. \tag{4}$$

Proof. The $\supset$ inclusion comes easily from the definition of K' as field generated by the $\operatorname{tr} \Phi(x)$. For the other direction, an element g of H' satisfies

$$\sum_{i=1}^{n} x^{\phi_i g} = \sum_{i=1}^{n} x^{\phi_i}$$

for every $x \in K$, which by independence of characters forces $Sg = S$. □

Remark This proposition enables us to understand the reflex field of K as the field generated by all symmetric polynomial expressions in $a^{\phi_1}, \ldots, a^{\phi_n}$ for all $a \in K$. Indeed, if f is a symmetric polynomial in n variables, then for every $\sigma \in H'$ and every $a \in K$, σ performs a permutation on $a^{\phi_1}, \ldots, a^{\phi_n}$, and therefore leaves $f(a^{\phi_1}, \ldots, a^{\phi_n})$ invariant, which implies $f(a^{\phi_1}, \ldots, a^{\phi_n}) \in K'$. The other inclusion is given by the definition of the reflex field as the field generated by all $\sum_{i=1}^{n} a^{\phi_i}$.

The proposition implies $H' = \{g \in G \mid gS^{-1} = S^{-1}\}$ where $S^{-1} = \{\sigma^{-1} \mid \sigma \in S\}$. The elements of S^{-1} induce a family of distinct embeddings $\psi_1, \ldots, \psi_m$ of K' into $\mathbf{C}$. Again, for every ψ_i we choose an element of S inducing ψ_i on K' and also call it ψ_i. Therefore, using what we just observed,

$$S^{-1} \subset \bigcup_{i=1}^{m} H'\psi_i \subset H'S^{-1} \subset S^{-1}, \text{ so } \quad S^{-1} = \bigcup_{i=1}^{m} H'\psi_i.$$

According to Lemma 3.4, L is a CM-field and complex conjugation commutes with all elements of G, so by (3),

$$G = S^{-1} \cup \overline{S^{-1}} \quad \text{and} \quad S^{-1} \cap \overline{S^{-1}} = \emptyset,$$

which ensures that $\psi_1, \ldots, \psi_m, \overline{\psi_1}, \ldots, \overline{\psi_m}$ are all distinct embeddings of K' into $\mathbf{C}$. Thus $[K' : Q] = [G : H'] = 2m$ and $\{\psi_1, \ldots, \psi_m\}$ is a CM-type Φ' on K'. The CM-type (K', Φ') is called the *reflex type* of (K, Φ). As seen from the construction, Φ' corresponds to the restrictions to K' of the inverses of the elements of Φ, viewed as elements of the Galois group of the Galois closure of K.

Special case: Consider a CM-type (K, Φ) with K Galois. Then we can take $K = L$ above, and $K' \subset K$. The elements ϕ_i of Φ can be considered as elements of the Galois group $\mathrm{Gal}(K/\mathbf{Q})$, and $S = \{\phi_1, \ldots, \phi_n\}$, $S' = \{\phi_1^{-1}, \ldots, \phi_n^{-1}\}$. In the particular case where K is quadratic imaginary, we get $K = K'$.

The reflex field of a CM-algebra. Let now $W \cong \prod_{i=1}^r K_i$ be a CM-algebra, Φ_i a CM-type for every K_i, and (K_i', Φ_i') the reflex of (K_i, Φ_i) for all i. Denote by K' the composite $K_1' \ldots K_r'$. It is a CM-field by Lemma 3.3. Then K' will be called the reflex field of $(W, \Phi = \prod_{i=1}^r \Phi_i)$. Note that it is generated by $\mathrm{tr}\, \Phi_i(x_i)$ for all $x_i \in K_i$, so actually it is generated by $\mathrm{tr}\, \Phi(x)$ for all $x \in W$.

The reflex norm. Let us go back to the case of a CM-field K. We already have a group homomorphism

$$\begin{array}{rccc} N_\Phi = \det \Phi' : K' & \longrightarrow & \mathbf{C} \\ x & \longmapsto & \prod_{i=1}^n x^{\psi_i} \end{array}$$

Every $h \in H$ stabilises K, so $hS = S$, so $S^{-1}h = S^{-1}$. Therefore, $h \circ N_\Phi = N_\Phi$, so actually the image of N_Φ is inside K. The map $N_\Phi : K'^* \longrightarrow K^*$ is called the *reflex norm*. For the formulation of the main theorem of complex multiplication in the adelic language, we are going to need it to be defined on $\mathbf{A}_{K'}^*$.

Proposition 3.10 *N_Φ can be extended to a homomorphism*

$$N_\Phi : \mathbf{A}_{K'}^* \longrightarrow \mathbf{A}_K^*.$$

Proof. The idea is to decompose our map $N_\Phi : K' \longrightarrow K$ into a linear map $K' \longrightarrow \mathcal{M}_m(K)$, easily extendable, and a determinant map. Write $K' = \mathbf{Q}(b)$ with $b \in \mathrm{K}'$. The coefficients of the polynomial $P(x) = \prod_{j=1}^m (x - b^{\psi_j})$ are symmetric functions in $b^{\psi_1}, \ldots, b^{\psi_m}$, and therefore lie in K. We can then choose a matrix $M \in \mathcal{M}_m(K)$ whose characteristic polynomial is P. Note that this matrix is conjugate to the matrix

$$\begin{pmatrix} b^{\psi_1} & & \\ & \ddots & \\ & & b^{\psi_m} \end{pmatrix} \in \mathcal{M}_m(L),$$

which we could have chosen directly had K been Galois. Define then a $\mathbf{Q}$-linear algebra homomorphism $f : K' \longrightarrow \mathcal{M}_m(K)$ by $f(b) = M$. For any $a = \sum_{k=0}^{2m-1} a_k b^k \in K'$ with $a_k \in \mathbf{Q}$, we get that $f(a) = \sum_{k=0}^{2m-1} a_k M^k$ is conjugate to

$$\begin{pmatrix} \sum_{k=0}^{2m-1} a_k (b^{\psi_1})^k & & \\ & \ddots & \\ & & \sum_{k=0}^{2m-1} a_k (b^{\psi_m})^k \end{pmatrix} = \begin{pmatrix} a^{\psi_1} & & \\ & \ddots & \\ & & a^{\psi_m} \end{pmatrix},$$

and therefore $\det f(a) = N_\Phi(a)$, so $N_\Phi = \det \circ f$. Now f can be extended $\mathbf{Q}_v$-linearly to $K'_v = K' \otimes \mathbf{Q}_v$ for v a place in $\mathbf{Q}$, and thus it is well-defined on $\mathbf{A}_{K'}$, with values in $\mathcal{M}_m(\mathbf{A}_K)$. Composing it with the determinant map, we get $N_\Phi : \mathbf{A}_{K'} \longrightarrow \mathbf{A}_K$. Note that in particular we have extended the ψ_j's to embeddings of K'_v into L_v and N_Φ to a map $K'_v \longrightarrow K_v$. Using these maps, for an idele s, $N_\Phi(s)$ is exactly what could be expected:

$$N_\Phi(s) = (N_\Phi(s_v))_v = \left(\prod_{j=1}^{m} s_v^{\psi_i} \right)_v .$$

In particular, we get a homomorphism $N_\Phi : \mathbf{A}^*_{K'} \longrightarrow \mathbf{A}^*_K$, as claimed. □

Remark. During the proof, we defined maps $N_\Phi : K'_p \longrightarrow K_p$ for all rational primes p. N_Φ is constructed using algebraic embeddings, so it preserves algebraic integers: there are maps $N_\Phi : \mathcal{O}_{K',p} \longrightarrow \mathcal{O}_{K,p}$ and $N_\Phi : \mathcal{O}^*_{K',p} \longrightarrow \mathcal{O}^*_{K,p}$. Using this and the fact that for any number field F,

$$\mathcal{O}^*_{F,p} \cong \prod_{\substack{\mathfrak{p}|p \\ \mathfrak{p} \text{ prime of } F}} \mathcal{O}^*_{F,\mathfrak{p}}$$

we see that $N_\Phi : \mathbf{A}'^*_K \longrightarrow \mathbf{A}^*_K$ induces also maps $N_\Phi : U_{K'}(c) \longrightarrow U_K(c)$ for all integers c, where $U_F(c)$ is defined as in 2.2. Finally, $N_\Phi : \mathbf{A}^*_{K'} \longrightarrow \mathbf{A}^*_K$ also passes to the quotient when composed with the ideal map $s \longrightarrow (s)$ and therefore induces a map $N_\Phi : I_{K'} \longrightarrow I_K$ on ideals.

The reflex norm for CM-algebras. Let now $W = \prod_{i=1}^r K_i$ be a CM-algebra, with for every K_i a CM-type Φ_i, and K' the reflex of $(W, \Phi = \prod_{i=1}^r \Phi_i)$. Put $\mathbf{A}_W = \prod_{i=1}^r \mathbf{A}_K$ and $\mathbf{A}^*_W = \prod_{i=1}^r \mathbf{A}^*_K$. We then can generalise the reflex norm, defining a map $N_\Phi : \mathbf{A}^*_{K'} \longrightarrow \mathbf{A}^*_W$ by

$$N_\Phi(x) = \left(N_{\Phi_i}(N_{K'/K'_i}(x)) \right)_{i=1}^r .$$

3.3 Abelian varieties with complex multiplication

In this subsection we follow Milne ([2]). Define for any semi-simple algebra B over a field k, with decomposition $\prod B_i$ into a product of simple algebras, its reduced degree by $[B : k]_{\text{red}} = \sum_i [B_i : k_i]^{\frac{1}{2}} [k_i : k]$, where, for all i, k_i is the centre of B_i. The following lemma is proved by comparing dimensions:

Lemma 3.11 *Let B be a semi-simple algebra over a field k. For any faithful B-module M,*

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

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

Let $A \cong \mathbf{C}^n/\Lambda$ be an abelian variety. Then $\text{End}_{\mathbf{Q}}(A)$ is a semi-simple $\mathbf{Q}$-algebra, and using (2), we see that $\mathbf{Q}\Lambda$ is a faithful $\text{End}_{\mathbf{Q}}(A)$-module: faithfulness comes from $\mathbf{R}\Lambda = \mathbf{C}^n$, as this means that any $\mathbf{C}$-linear morphism that is the identity on $\mathbf{Q}\Lambda$ is the identity on all of $\mathbf{C}^n$. Applying Lemma 3.11 to $\mathbf{Q}\Lambda$, we get

$$2 \dim A \geq [\text{End}_{\mathbf{Q}}(A) : \mathbf{Q}]_{\text{red}}. \tag{5}$$

Definition 3.12 *We say that A has complex multiplication if*

$$2\dim A = [End_{\mathbf{Q}}(A) : \mathbf{Q}]_{red}. \tag{6}$$

Note that in this case, according to Lemma 3.11, $\mathrm{End}_{\mathbf{Q}}(A)$ is a product of matrix algebras. A result from the theory of semi-simple algebras shows that (6) is equivalent to the existence of an étale $\mathbf{Q}$-subalgebra of dimension $2\dim(A)$. A is isogenous to a product $\prod_i A_i^{n_i}$ where A_i are simple varieties, and then $\mathrm{End}_{\mathbf{Q}}(A) \cong \prod_i \mathcal{M}_{n_i}(D_i)$ where, for every i, D_i is the division $\mathbf{Q}$-algebra $\mathrm{End}_{\mathbf{Q}}(A_i)$. In the case where A has complex multiplication, the D_i must be number fields of degree $2\dim(A_i)$. In particular, A has complex multiplication if and only if each of its simple factors has complex multiplication, and if A is simple, it has complex multiplication if and only if $\mathrm{End}_{\mathbf{Q}}(A)$ is a number field of degree $2\dim(A)$. The following proposition gives a more precise description of $\mathrm{End}_{\mathbf{Q}}(A)$ for A with complex multiplication:

Proposition 3.13 *(a) A simple abelian variety A has complex multiplication if and only if $End_{\mathbf{Q}}(A)$ is a CM-field of degree $2\dim(A)$ over $\mathbf{Q}$.*

(b) An isotypic abelian variety A (that is, isogenous to $A_1^{n_1}$ with A_1 simple) has complex multiplication if and only if $End_{\mathbf{Q}}(A)$ contains a number field of degree $2\dim(A)$ over $\mathbf{Q}$, which can be chosen to be a CM-field stable under the involution induced by some polarisation of A.

(c) An abelian variety A has complex multiplication if and only if $End_{\mathbf{Q}}(A)$ contains an étale $\mathbf{Q}$-algebra W of dimension $2\dim(A)$, which can be chosen to be a CM-algebra invariant under the involution induced by some polarisation of A. We then say A has complex multiplication by W.

We won't prove this proposition: subsection 3.5 will provide the construction of a polarisation inducing an involution stabilising the image of the number field K inside $\mathrm{End}_{\mathbf{Q}}(A)$. The idea in the number field case is then that any polarisation on A induces a positive involution on $\mathrm{End}_{\mathbf{Q}}(A)$ and that if it stabilises K, the latter is necessarily either totally real or a CM-field. The first possibility can be excluded by proving that a subfield of maximal dimension of $\mathrm{End}_{\mathbf{Q}}(A)$ is always totally imaginary. The étale algebra case is then deduced easily by decomposition. In what follows, as in the definitions in subsection 3.1, we will often restrict to the CM-field case before generalising to CM-algebras: this most of the time doesn't change the core of the proofs but enables us to simplify notations.

3.4 CM-type associated to an abelian variety with complex multiplication

Fix an abelian variety with complex multiplication by a CM-field K and an embedding

$$\iota : K \longrightarrow \mathrm{End}_{\mathbf{Q}}(A).$$

We are going to show how we can associate a CM-type (K, Φ) to the couple (A, ι). The information about the type of (A, ι) is contained in the map ι and can be extracted by performing a diagonalising change of basis. More precisely, the action of K on A induces an action on the tangent space of A at 0, and we are going to find a basis of this space that diagonalises this action. For this, fix a complex torus $\mathbf{C}^n/\Lambda$ isomorphic to A for some lattice $\Lambda \subset \mathbf{C}^n$: we will express this by means of the exact sequence

$$0 \longrightarrow \Lambda \longrightarrow \mathbf{C}^n \xrightarrow{\xi} A \longrightarrow 0. \tag{7}$$

We are going to denote both the map $\mathbf{C}^n \longrightarrow A$ from this exact sequence and the isomorphism $\mathbf{C}^n/\Lambda \cong A$ it induces by ξ, for convenience of notation. According to (2), each element of $\mathrm{End}_{\mathbf{Q}}(A)$ corresponds with respect to (7) to a linear transformation of $\mathbf{C}^n$ preserving $\mathbf{Q}\Lambda$. Therefore, through ι, K acts faithfully linearly on $\mathbf{C}^n$ and we get an injective ring homomorphism

$$D_\Phi : K \longrightarrow M_n(\mathbf{C}).$$

K being commutative, up to change of basis we can assume that for every $a \in K$, $D_\Phi(a)$ is a diagonal matrix, of the form

$$\begin{pmatrix} a^{\phi_1} & & \\ & \ddots & \\ & & a^{\phi_n} \end{pmatrix}.$$

By $\mathbf{Q}$-linearity and faithfulness, $\{\phi_1, \ldots, \phi_n\}$ is a CM-type for K. We say that (A, ι) is of type (K, Φ).

We continue our investigation to deduce some other properties of (A, ι) with respect to its type. $\mathbf{Q}\Lambda$ is a $\mathbf{Q}$-vector space of dimension $2n = [K : \mathbf{Q}]$, and a K-module through D_Φ. Therefore, if we take a non-zero $w \in \mathbf{Q}\Lambda$, then $\mathbf{Q}\Lambda \supset D_\Phi(K)w$, and comparing dimensions, $\mathbf{Q}\Lambda = D_\Phi(K)w$. Thus, with respect to our new basis, we have

$$\mathbf{Q}\Lambda = \left\{ \begin{pmatrix} a^{\phi_1} w_1 \\ \vdots \\ a^{\phi_n} w_n \end{pmatrix}, a \in K \right\},$$

where $w = (w_1, \ldots, w_n)$ are the coordinates of w in this basis. We can optimise our chosen basis further by noticing that none of the w_i can be zero, since $\mathbf{R}\Lambda = \mathbf{C}^n$: our coordinate system $(z_1, ..., z_n)$ can therefore be replaced by $(w_1^{-1} z_1, \ldots, w_n^{-1} z_n)$. We finally get:

$$\mathbf{Q}\Lambda = \left\{ \begin{pmatrix} a^{\phi_1} \\ \vdots \\ a^{\phi_n} \end{pmatrix}, a \in K \right\} = u_\Phi(K),$$

where

$$u_\Phi(a) = \begin{pmatrix} a^{\phi_1} \\ \vdots \\ a^{\phi_n} \end{pmatrix} = D_\Phi(a) \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.$$

u_Φ (or simply u) is a $\mathbf{Q}$-linear isomorphism from K to $\mathbf{Q}\Lambda$. Extending it $\mathbf{R}$-linearly, we get an $\mathbf{R}$-linear isomorphism $u : K \otimes \mathbf{R} = K_{\mathbf{R}} \longrightarrow \mathbf{R}\Lambda = \mathbf{C}^n$. Putting $\mathfrak{a} = u^{-1}(\Lambda) \subset K$, this gives rise to a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & K_{\mathbf{R}} & \longrightarrow & K_{\mathbf{R}}/\mathfrak{a} & \longrightarrow & 0\,. \\ & & \downarrow & & \downarrow u & & \downarrow & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbf{C}^n & \xrightarrow{\xi} & A & \longrightarrow & 0 \end{array}$$

Generalisation to CM-algebras Let A be an abelian variety with complex multiplication by a CM-algebra $W = K_1 \times \ldots \times K_r$ through the embedding

$$\iota : W \longrightarrow \mathrm{End}_{\mathbf{Q}}(A).$$

For every i, denote by e_i the vector $(0, \ldots, 0, 1, 0, \ldots, 0) \in K_1 \times \ldots \times K_r$ with a 1 in the i-th position: it corresponds to the unit of the number field K_i contained in A. Then for every e_i there is an integer m_i such that $\iota(m_i e_i) \in \mathrm{End}(A)$. Put $A_i = \iota(m_i e_i)A$ for all i, so that A is isogenous to $A_1 \times \ldots \times A_r$ and ι induces embeddings $\iota_i : K_i \longrightarrow \mathrm{End}_{\mathbf{Q}}(A_i)$. We have $[W : \mathbf{Q}] = 2\dim(A)$ and $[K_i : \mathbf{Q}] \leq 2\dim(A_i)$ for all i by (5), so actually $[K_i : \mathbf{Q}] = 2\dim(A_i)$ and therefore A_i has complex multiplication by K_i for all i. Applying the above to every K_i, we get CM-types Φ_i for each K_i, and therefore a CM-type Φ for W. We write also D_Φ for the diagonal map $D_\Phi : W \longrightarrow \mathcal{M}_n(\mathbf{C})$, and note that

$$D_\Phi(a_1, \ldots, a_r) = \mathrm{diag}(\Phi_1(a_1), \ldots, \Phi(r(a_r))$$

for CM-types Φ_i of the CM-fields K_i. Denoting by u_i the isomorphisms u obtained thanks to the CM-field case for every K_i, we define, for every $a = (a_1, \ldots, a_r) \in W$, $u(a)$ to be the column vector

$$u(a) = \begin{pmatrix} u_1(a_1) \\ \vdots \\ u_r(a_r) \end{pmatrix}.$$

If $\mathfrak{a}_i$ is the lattice obtained for K_i, put $\mathfrak{a} = \mathfrak{a}_1 \times \ldots \times \mathfrak{a}_r$, which is a lattice in W. Write $W_{\mathbf{R}} = W \otimes_{\mathbf{Q}} \mathbf{R}$. Using otherwise the same notations as above and taking the direct sum of the diagrams for every K_i, u defines an isomorphism so that the following diagram with exact rows commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & W_{\mathbf{R}} & \longrightarrow & W_{\mathbf{R}}/\mathfrak{a} & \longrightarrow & 0\,. \\ & & \downarrow & & \downarrow{\scriptstyle u} & & \downarrow & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbf{C}^n & \xrightarrow{\xi} & A & \longrightarrow & 0 \end{array}$$

We have thus written A as $W_{\mathbf{R}}/\mathfrak{a}$ with a lattice $\mathfrak{a}$ in W. The action D_Φ of W on A as the complex torus $\mathbf{C}^n/\Lambda$ becomes the obvious multiplication action on A as the torus $W_{\mathbf{R}}/\mathfrak{a}$. In the notation $W_{\mathbf{R}}/\mathfrak{a}$ the torsion points of A correspond to $W/\mathfrak{a}$. In this situation, we will sometimes say that A is of type $(W, \Phi, \mathfrak{a})$ with respect to ξ, as $\mathfrak{a}$ depends on the choice of ξ. Note that if $\mathcal{O} = \iota^{-1}(\mathrm{End}A)$,

$$\mathcal{O} = \{\alpha \in W | D_\Phi(\alpha)\Lambda \subset \Lambda\} = \{\alpha \in W | \alpha\mathfrak{a} \subset \mathfrak{a}\},$$

so $\mathcal{O}$ is the order of $\mathfrak{a}$ and $\mathfrak{a}$ is an ideal for $\mathcal{O}$. In particular, when $\mathcal{O} = \mathcal{O}_W$, $\mathfrak{a} = \mathfrak{a}_1 \times \ldots \times \mathfrak{a}_r$ is such that $\mathfrak{a}_i$ is a fractional ideal of K_i for all i. In this case, we say (A, ι) is *principal*.

Classification of abelian varieties with complex multiplication. An isogeny $\mu : (A_1, \iota_1) \longrightarrow (A_2, \iota_2)$ of abelian varieties with complex multiplication by W is an isogeny $\mu : A_1 \longrightarrow A_2$ such that for every $a \in W$ the diagram

$$\begin{array}{ccc} A_1 & \xrightarrow{\mu} & A_2 \\ {\scriptstyle \iota_1(a)}\downarrow & & \downarrow{\scriptstyle \iota_2(a)} \\ A_1 & \xrightarrow{\mu} & A_2 \end{array}$$

commutes. We will sometimes write $\mathrm{Hom}((A_1,\iota_1),(A_2,\iota_2))$ for the ring of these isogenies, and $\mathrm{Hom}_{\mathbf{Q}}((A_1,\iota_1),(A_2,\iota_2)) = \mathrm{Hom}((A_1,\iota_1),(A_2,\iota_2)) \otimes \mathbf{Q}$.

Lemma 3.14 *Let (A_1,ι_1) (resp. (A_2,ι_2)) be of type $(W,\Phi,\mathfrak{a}_1)$ (resp. $(W,\Phi,\mathfrak{a}_2)$) with respect to ξ_1 (resp. ξ_2). Let $\mu : (A_1,\iota_1) \longrightarrow (A_2,\iota_2)$ be an element of $Hom_{\mathbf{Q}}((A_1,\iota_1),(A_2,\iota_2))$. Then there is an element $\gamma \in W$ such that $\gamma\mathfrak{a}_1 \subset \mathfrak{a}_2$ and such that the following diagram*

$$\begin{array}{ccccc} W/\mathfrak{a}_1 & \xrightarrow{u} & \mathbf{C}^n/u(\mathfrak{a}_1) & \xrightarrow{\xi_1} & A_1 \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle D_\Phi(\gamma)} & & \downarrow{\scriptstyle \mu} \\ W/\mathfrak{a}_2 & \xrightarrow{u} & \mathbf{C}^n/u(\mathfrak{a}_2) & \xrightarrow{\xi_2} & A_2 \end{array}$$

(where the map in the leftmost column is multiplication by γ) commutes.

Proof. μ induces a $\mathbf{C}$-linear endomorphism (that we also call μ) of $\mathbf{C}^n$ such that $\mu(\mathbf{Q}u(\mathfrak{a}_1)) \subset \mathbf{Q}u(\mathfrak{a}_2)$. Therefore it induces a $\mathbf{Q}$-linear map $\mu : \mathbf{Q}u(\mathfrak{a}_1) \longrightarrow \mathbf{Q}u(\mathfrak{a}_2)$. The spaces $\mathbf{Q}u(\mathfrak{a}_1)$ and $\mathbf{Q}u(\mathfrak{a}_2)$ are both equal to $u(W)$, so μ comes from a $\mathbf{Q}$-linear map $\nu = u^{-1} \circ \mu \circ u : W \longrightarrow W$. In fact, ν is W-linear: indeed, μ commutes with ι_1 and ι_2, so it commutes with the action of W on the varieties. Thus ν is multiplication by some element $\gamma \in W$, and μ coincides with $D_\Phi(\gamma)$. □

The following proposition shows that abelian varieties are classified by their CM-types up to isogeny.

Proposition 3.15 *Let (A_1,ι_1), (A_2,ι_2) be abelian varieties with complex multiplication by W. (A_1,ι_1) and (A_2,ι_2) are isogenous if and only if they are of the same type (W,Φ).*

Proof.

1. *"Only if" part:* Fix an isogeny μ from (A_1,ι_1) onto (A_2,ι_2). Then there is an isomorphism

$$\begin{array}{ccc} \mathrm{End}_{\mathbf{Q}}(A_1) & \xrightarrow{\mu^*} & \mathrm{End}_{\mathbf{Q}}(A_2) \\ \alpha & \longmapsto & \mu \circ \alpha \circ \mu^{-1} \end{array}$$

   and a commutative diagram

$$\begin{array}{ccc} W & \xrightarrow{\iota_1} & \mathrm{End}_{\mathbf{Q}}(A_1) \\ & \searrow^{\iota_2} & \downarrow{\scriptstyle \mu^*} \\ & & \mathrm{End}_{\mathbf{Q}}(A_2) \end{array}$$

   Indeed, the commutativity of this diagram is equivalent to $\mu \circ \iota_1(a) = \iota_2(a) \circ \mu$ for all $a \in W$, which is true by definition of μ. Therefore for all $a \in W$, $\iota_1(a)$ and $\iota_2(a)$ induce conjugate endomorphisms on $\mathbf{C}^n$, which are codiagonalisable and have the same diagonalisation, which means that the obtained CM-types are the same.

2. *"If" part:* Suppose (A_1,ι_1), (A_2,ι_2) are of types $(W,\Phi,\mathfrak{a}_1)$ and $(W,\Phi,\mathfrak{a}_2)$ with respect to ξ_1 and ξ_2 respectively for some lattices $\mathfrak{a}_1,\mathfrak{a}_2 \in W$. By Lemma 2.7 there is an integer

$d > 0$ such that $d\mathfrak{a}_1 \subset \mathfrak{a}_2$. Thus multiplication by d defines through the isomorphisms ξ_1, ξ_2 an isogeny $\mu : A_1 \longrightarrow A_2$ such that the following diagram

$$\begin{array}{ccc} \mathbf{C}^n/u(\mathfrak{a}_1) & \xrightarrow{\xi_1} & A_1 \\ \Big\downarrow{\scriptstyle d} & & \Big\downarrow{\scriptstyle \mu} \\ \mathbf{C}^n/u(\mathfrak{a}_2) & \xrightarrow{\xi_2} & A_2 \end{array}$$

commutes. The fact that μ is actually an isogeny $(A_1, \iota_1) \longrightarrow (A_2, \iota_2)$ is then checked easily: for every $x = \xi_1(y) \in A_1$ and $a \in W$,

$$\mu \circ \iota_1(a)(x) = \mu \circ \xi_1(D_\Phi(a)(y)) = \xi_2(D_\Phi(a)dy) = \iota_2(a) \circ \xi_2(dy) = \iota_2(a) \circ \mu(x).$$

Note that $\mathbf{Q}$-linearity of $D_\Phi(a)$ is used at the second step. □

3.5 Type of a polarised abelian variety

As noticed at the end of the previous subsection, associating a CM-type to an abelian variety with complex multiplication determines the isogeny class of this variety. At present, let (A, ι) be of type (K, Φ) for a CM-field K and let $\mathcal{C}$ be a polarisation of A. We are going to define for the polarised abelian variety $(A, \iota, \mathcal{C})$ a more precise notion of type that will characterise it up to isomorphism.

The polarisation $\mathcal{C}$ must not be chosen at random. It has to be *compatible with* ι, that is,

$$\iota(K)^\gamma = \iota(K),$$

where γ is the involution determined by $\mathcal{C}$. This can be shown to be equivalent to the fact that a Riemann form associated to any divisor in $\mathcal{C}$ is Φ-*admissible*, that is

$$E(D_\Phi(a)z, w) = E(z, D_\Phi(\bar{a})w) \quad \text{for all } z, w \in \mathbf{C}^n/\Lambda \text{ and } a \in K. \tag{8}$$

We are now going to show that a polarisation of A compatible with ι always exists, by constructing an explicit Φ-admissible Riemann form. For this, let us begin by studying Φ-admissible forms more broadly and finding all necessary conditions on a Φ-admissible Riemann form associated to some divisor of $\mathcal{C}$ with respect to the isomorphism $\xi : \mathbf{C}^n/\Lambda \longrightarrow A$. Reading E through u on elements of K, we are going to show E has to be of a very particular form, and characterised entirely by a certain element $\tau \in K$. Indeed, put $f(a) = E(u(a), u(1))$ for every $a \in K$. E being a Riemann form, it is $\mathbf{R}$-bilinear, $\mathbf{Z}$-valued on Λ and $\mathbf{Q}$-valued on $\mathbf{Q}\Lambda$. Thus f is a $\mathbf{Q}$-linear map of K into $\mathbf{Q}$, and must therefore be of the form $f(a) = \mathrm{Tr}_{K/\mathbf{Q}}(\tau a)$ for some τ in K. Thanks to (8) we have then for all $a, b \in K$

$$E(u(a), u(b)) = E(u(a), D_\Phi(b)u(1)) = E(D_\Phi(\bar{b})a, u(1)) = E(u(\bar{b}a), u(1)).$$

Thus, for all elements $a, b \in K$, E must be of the form

$$E(u(a), u(b)) = \mathrm{Tr}_{K/\mathbf{Q}}(\tau a\bar{b}). \tag{9}$$

Moreover, E must be alternating, which forces $\bar{\tau} = -\tau$, i.e. τ is purely imaginary. K being a CM-field, this implies

$$\overline{\tau^{\phi_j}} = \bar{\tau}^{\phi_j} \quad \text{for } j = 1, \ldots, n. \tag{10}$$

We will now deduce from this a general expression for E on $\mathbf{C}^n$, namely

$$E(z,w) = \sum_{j=1}^{n} \tau^{\phi_j}(z_j\overline{w_j} - \overline{z_j}w_j) \quad \text{for } z,w \in \mathbf{C}^n. \tag{11}$$

Indeed, from $\mathrm{Tr}_{K/\mathbf{Q}} = \sum_{j=1}^{n}(\phi_j + \overline{\phi_j})$ and from (10) we see that (11) is true for $z,w \in u(K)$. The expression (11) is then obtained for all $z,w \in \mathbf{C}^n$ by continuity of E and density of $u(K)$ in $\mathbf{C}^n$.

We haven't yet derived any conditions from the fact that $E(z,\sqrt{-1}w)$ is symmetric and positive definite. Since

$$E(z,\sqrt{-1}w) = -\sqrt{-1}\sum_{i=1}^{n} \tau^{\phi_j}(z_j\overline{w_j} + \overline{z_j}w_j),$$

this is true if and only if

$$\mathrm{Im}(\tau^{\phi_j}) > 0 \quad \text{for } j = 1,\ldots,n.$$

In fact, the conditions we have found are necessary and sufficient, up to multiplication by a positive integer, and can be summarised by the following proposition:

Proposition 3.16 *Let (A,ι) be of type $(K,\Phi,\mathfrak{a})$. Then*

(i) Let $\tau \in K$ be such that $\overline{\tau} = -\tau$ and $Im(\tau^{\phi_j}) > 0$ for $j = 1,\ldots,n$. Let

$$E(z,w) = \sum_{j=1}^{n} \tau^{\phi_j}(z_j\overline{w_j} - \overline{z_j}w_j).$$

Then there is a positive integer d such that dE is a Φ-admissible non-degenerate Riemann form on $\mathbf{C}^n/\Phi(\mathfrak{a})$.

(ii) Conversely, every Φ-admissible non-degenerate Riemann form on $\mathbf{C}^n/\Phi(\mathfrak{a})$ is obtained from an element τ as in (i).

Proof. We have proven (ii) above, so it suffices to prove (i). E is clearly $\mathbf{R}$-bilinear. The fact that E is alternating and that $E(z,\sqrt{-1}w)$ is symmetric definite positive is also easily seen to be true from the above discussion. Checking it is Φ-admissible is an easy computation. It remains to see that there exists an integer $d > 0$ such that $dE(u(\mathfrak{a})\times u(\mathfrak{a})) \subset \mathbf{Z}$, i.e., using (9),

$$\mathrm{Tr}_{K/\mathbf{Q}}(d\tau\mathfrak{a}\bar{\mathfrak{a}}) \subset \mathbf{Z},$$

which is equivalent to $d\tau\mathfrak{a}\bar{\mathfrak{a}} \subset \mathcal{O}_K$. But $\tau\mathfrak{a}\bar{\mathfrak{a}}$ is a lattice in K by Lemma 2.9, so such an integer d exists. □

In particular, this proposition proves that Φ-admissible Riemann forms, and therefore compatible polarisations, exist. Let $(A,\iota,\mathcal{C})$ be an abelian variety polarised with a compatible polarisation. Then we can construct from it a CM-type (K,Φ), a lattice $\mathfrak{a}$ in K and, using the Riemann form determined by the basic polar divisor of $\mathcal{C}$ with respect to ξ (which will be Φ-admissible), an element $\tau \in K$ satisfying

$$\bar{\tau} = -\tau \quad \text{and} \quad \mathrm{Im}(\tau^{\phi_j}) > 0 \quad \text{for } j = 1,\ldots,n. \tag{12}$$

Note that $\mathfrak{a}$ and τ depend on the choice of ξ in (7). $(A, \iota, \mathcal{C})$ is said to be of type $(K, \Phi, \mathfrak{a}, \tau)$ with respect to ξ. The dependance of the type on the isomorphism ξ will be made more explicit below.

Conversely, from a quadruple $(K, \Phi, \mathfrak{a}, \tau)$ with (K, Φ) a CM-type, $\mathfrak{a}$ a lattice in K and $\tau \in K$ satisfying (12), we can construct some triple $(A_\Phi, \iota_\Phi, \mathcal{C}_\Phi)$. Indeed, using the CM-type $\Phi = \{\phi_1, \ldots, \phi_n\}$, define $u : K \longrightarrow \mathbf{C}^n$ as above by

$$u_\Phi(a) = \begin{pmatrix} a^{\phi_1} \\ \vdots \\ a^{\phi_n} \end{pmatrix}.$$

Then A_Φ is defined to be the complex torus $\mathbf{C}^n/\Lambda$ with $\Lambda = u_\Phi(\mathfrak{a})$. ι_Φ is recovered by defining $D_\Phi : K \longrightarrow \mathcal{M}_n(\mathbf{C})$ such that

$$D_\Phi(a) = \begin{pmatrix} a^{\phi_1} & & \\ & \ddots & \\ & & a^{\phi_n} \end{pmatrix}$$

for every $a \in K$. $D_\Phi(a)$ preserves $u_\Phi(K) = \mathbf{Q}\Lambda$ and gives therefore an element $\iota_\Phi(a) \in \mathrm{End}_{\mathbf{Q}}(A)$. Linearity and injectivity of ι_Φ follow easily from those of D_Φ. Finally, define on $\mathbf{C}^n$ the $\mathbf{R}$-bilinear form E given by (11). Then by Proposition 3.16, there is an integer $d > 0$ such that dE is a Riemann form, giving a polarisation $\mathcal{C}_\Phi$ on A_Φ.

Generalisation to CM-algebras. Let (A, ι) be an abelian variety of type (W, Φ) with $W = K_1 \times \ldots \times K_r$ a CM-algebra. We can construct a Φ-admissible Riemann form W on $\mathbf{C}^n \times \mathbf{C}^n$, satisfying

$$E(u(x), u(y)) = \mathrm{Tr}_{W/\mathbf{Q}}(\tau x \bar{y}) = \sum_{i=1}^{r} \mathrm{Tr}_{K_i/\mathbf{Q}}(\tau_i x_i \overline{y_i})$$

for all $x, y \in W$, where $\tau = (\tau_1, \ldots, \tau_r) \in W$ is such that for every i, $\tau_i \in K_i$ satisfies (12). We say that A is of type $(W, \Phi, \mathfrak{a}, \tau)$. Conversely, every such type gives rise to a variety in the same manner as above. In particular W induces Riemann forms E_i on K_i such that

$$E_i(u_i(x), u_i(y)) = \mathrm{Tr}_{K_i/\mathbf{Q}}(\tau_i x \bar{y})$$

for all $x, y \in K_i$, and therefore compatible polarisations $\mathcal{C}_i$ on the K_i.
In what follows, when speaking of a polarised abelian variety $(A, \iota, \mathcal{C})$ with complex multiplication, $\mathcal{C}$ will always be assumed compatible with ι.

Classification up to isomorphism It is natural to try to evaluate to which extent the above two constructions are inverse one to the other. This will lead us to show abelian varieties are classified by their types up to isomorphism. Let us write $\theta(A, \iota, \mathcal{C})$ for the type of the polarised abelian variety $(A, \iota, \mathcal{C})$ with complex multiplication and $\eta(W, \Phi, \mathfrak{a}, \tau)$ for the polarised abelian variety $(A_\Phi, \iota_\Phi, \mathcal{C}_\Phi)$ associated to the type $(W, \Phi, \mathfrak{a}, \tau)$ by the above inverse construction. We will now study $\eta \circ \theta$ and $\theta \circ \eta$.

Fix some triple $(A, \iota, \mathcal{C})$ and write $\theta(A, \iota, \mathcal{C}) = (W, \Phi, \mathfrak{a}, \tau)$. Then

$$\eta \circ \theta(A, \iota, \mathcal{C}) = (A_\Phi = \mathbf{C}^n/u(\mathfrak{a}), \iota_\Phi, \mathcal{C}_\Phi)$$

(A_Φ, ι_Φ) is by construction isomorphic to (A, ι) and has the same CM-type (W, Φ). By this isomorphism, the associated Riemann form is invariant as τ already comes from a Riemann form and needs no further multiplication by an integer, so $(A_\Phi, \iota_\Phi, \mathcal{C}_\Phi) \cong (A, \iota, \mathcal{C})$.

On the other hand, let us fix a type $(W, \Phi, \mathfrak{a}, \tau)$. Up to multiplication by an integer, we can assume the associated Riemann form is E defined by (11). Then

$$\eta(W, \Phi, \mathfrak{a}, \tau) = (A_\Phi = \mathbf{C}^n / u(\mathfrak{a}), \iota_\Phi, \mathcal{C}_\Phi)$$

and by construction $\theta \circ \eta(W, \Phi, \mathfrak{a}, \tau) = (W, \Phi, \mathfrak{a}', \tau')$ for some lattice $\mathfrak{a}' \subset W$ and some $\tau' \in W$ the components of which satisfy (12). As we have seen above, $\eta \circ \theta(A_{Phi}, \iota_\Phi, \mathcal{C}_\Phi)$ is isomorphic to $(A_\Phi, \iota_\Phi, \mathcal{C}_\Phi)$, and so by Lemma 3.15 there is a $\gamma \in W$ such that this isomorphism is of the form $D_\Phi(\gamma)$. Then $\mathfrak{a}' = \gamma\mathfrak{a}$, and, writing E, E' for the corresponding Riemann forms, for all $z, w \in \mathbf{C}^n$

$$E'(D_\Phi(\gamma)z, D_\Phi(\gamma)w) = E(z, w),$$

which read through u gives for all $a, b \in W$

$$\mathrm{Tr}_{W/\mathbf{Q}}(\tau'\gamma\bar{\gamma}a\bar{b}) = \mathrm{Tr}_{W/\mathbf{Q}}(\tau a\bar{b}),$$

which gives $\tau' = \frac{1}{\gamma\bar{\gamma}}\tau$.

In view of what we just obtained, let us define the following equivalence relation on types:

Definition 3.17 *Two types $(W, \Phi, \mathfrak{a}_1, \tau_1)$ and $(W, \Phi, \mathfrak{a}_2, \tau_2)$ are equivalent*[1] *if there is an element $a \in W$ such that*

$$\mathfrak{a}_1 = a\mathfrak{a}_2 \quad \textit{and} \quad \tau_1 = (a\bar{a})^{-1}\tau_2.$$

Remark To be really precise, we should say that types are equivalent if the underlying CM-algebras are isomorphic and the CM-types compatible under this isomorphism, instead of just being the same, and express the condition on the lattices and the τ's in terms of this isomorphism. As it is not really important for our purpose, we allow ourselves this little abuse of definition.

We have thus proved the following classification:

Proposition 3.18 *There is an exact correspondence*

$$\begin{array}{ccc} \{\textit{isomorphism classes of triples } (A, \iota, \mathcal{C})\ \} & \longleftrightarrow & \{\textit{equivalence classes of types } (W, \Phi, \mathfrak{a}, \tau)\} \\ (A, \iota, \mathcal{C}) & \overset{\theta}{\mapsto} & \textit{associated type } (W, \Phi, \mathfrak{a}, \tau) \end{array}$$

Let us moreover state here a result partly proven in the previous reasoning, explaining how a change in the choice of ξ affects the type of the triple $(A, \iota, \mathcal{C})$.

Lemma 3.19 *Let $(A, \iota, \mathcal{C})$ be of type $(W, \Phi, \mathfrak{a}, \tau)$ with respect to ξ_1. If ξ_1 is replaced by $\xi_2 = \xi_1 \circ D_\Phi(a)^{-1}$ for some $a \in W^*$, then $(A, \iota, \mathcal{C})$ is of type $(W, \Phi, a\mathfrak{a}, (a\bar{a})^{-1}\tau)$ with respect to ξ_2.*

[1] This terminology is non-standard.

Proof. The fact that the new associated lattice is $a\mathfrak{a}$ is clear. Then the situation is shown by the following diagram:

$$\begin{array}{ccc} \mathbf{C}^n/u(a\mathfrak{a}) & \xrightarrow{D_\Phi(a)^{-1}} & \mathbf{C}^n/u(\mathfrak{a}) \\ & \searrow^{\xi_2} & \downarrow{\scriptstyle \xi_1} \\ & & A \end{array}$$

Let E_1 (resp. E_2) be the Riemann form determined by the basic polar divisor of $\mathcal{C}$ with respect to ξ_1 (resp ξ_2), and τ_1 (resp.τ_2) the associated elements of W. Then for all $z, w \in \mathbf{C}^n$ and for all $a \in W$,

$$E_1(D_\Phi(a)^{-1}z, D_\Phi(a)^{-1}w) = E_2(z, w).$$

As above we get

$$\mathrm{Tr}_{W/\mathbf{Q}}(\tau_1 a^{-1}x\overline{a^{-1}y}) = \mathrm{Tr}_{W/\mathbf{Q}}(\tau_2 x\bar{y})$$

for all $x, y, a \in W$. Therefore $\tau_2 = (a\bar{a})^{-1}\tau_1$. □

4 The main theorem of complex multiplication

4.1 Multiplication by an idele

In order to state the main theorem of complex multiplication, we need to define one last thing: the action of the group of ideles on torsion points. Let K be a number field, $\mathfrak{a} \subset K$ a lattice and $t \in \mathbf{A}_K^*$ an idele. For each rational prime p, we write t_p for the p-component of t in K_p^*, and $\mathfrak{a}_p = \mathfrak{a} \otimes_{\mathbf{Z}} \mathbf{Z}_p$. Define moreover $t\mathfrak{a}$ by putting $t\mathfrak{a} := (t)\mathfrak{a}$. it is a lattice by Lemma 2.9 and satisfies $(t\mathfrak{a})_p = t_p\mathfrak{a}_p$ for all p. We will now associate to t an isomorphism $K/\mathfrak{a} \longrightarrow K/t\mathfrak{a}$. For this, first note there is an isomorphism

$$K/\mathfrak{a} \cong \bigoplus_p K_p/\mathfrak{a}_p. \tag{13}$$

Indeed, by decomposition into p-primary components of the torsion $\mathbf{Z}$-module $K/\mathfrak{a}$, we have $K/\mathfrak{a} \cong \bigoplus_p (K/\mathfrak{a})^{(p)}$ where $(K/\mathfrak{a})^{(p)}$ denotes the p-primary part, and it is well known that $(K/\mathfrak{a})^{(p)} \cong K_p/\mathfrak{a}_p$ for all p. For each p the multiplication by t_p map defines an isomorphism $K_p/\mathfrak{a}_p \longrightarrow K_p/t_p\mathfrak{a}_p$, and combining all these isomorphisms thanks to (13), we get an isomorphism

$$\begin{array}{rcl} K/\mathfrak{a} & \longrightarrow & K/t\mathfrak{a} \\ x = (x_p)_p & \mapsto & (t_p x_p)_p \end{array}$$

The image $(t_p x_p)$ of an element $x \in K/\mathfrak{a}$ by this isomorphism will be denoted tx.

This multiplication action extends easily to an étale algebra $W = \prod_{i=1}^r K_i$: take $t = (t_1, \ldots, t_r) \in \mathbf{A}_W^* = \prod_{i=1}^r \mathbf{A}_{K_i}$, and for a lattice $\mathfrak{a} = \prod_{i=1}^r \mathfrak{a}_i \in W$, define $t\mathfrak{a} = \prod_{i=1}^r t_i\mathfrak{a}_i$. Then $W/\mathfrak{a} \cong \prod_{i=1}^r K_i/\mathfrak{a}_i$, $W/t\mathfrak{a} \cong \prod_{i=1}^r K_i/t_i\mathfrak{a}_i$, and multiplication by t will be the map

$$\begin{array}{rcl} W/\mathfrak{a} & \longrightarrow & W/t\mathfrak{a} \\ x = (x_1, \ldots, x_r) & \mapsto & tx = (t_1x_1, \ldots, t_rx_r) \end{array}$$

4.2 The main theorem of complex multiplication

Let K be a CM field and $(A, \iota, \mathcal{C})$ be of type (K, Φ) and let $\sigma \in \mathrm{Aut}(\mathbf{C})$. Then the CM-type of $(A^\sigma, \iota^\sigma, \mathcal{C}^\sigma)$ can be proved to be (K, Φ^σ), and its complete type is given by the theorem of Tate and Deligne. In this section we are going to restrict to the special case treated by Shimura, and which is the one useful for deducing explicit class field theory results. We are therefore going to assume

$$\sigma \text{ fixes the reflex field } K' \text{ of } K. \tag{14}$$

This has two crucial consequences:

(a) By Proposition 3.9 $\Phi^\sigma = \Phi$, and therefore A and A^σ are isogenous.

(b) There is an $s \in \mathbf{A}_{K'}^*$ such that its image $[s, K']$ by the reciprocity map

$$\mathbf{A}_{K'}^* \longrightarrow \mathrm{Gal}\left(K'^{\mathrm{ab}}/K'\right)$$

satisfies $[s, K'] = \sigma_{|K'^{\mathrm{ab}}}$.

The theorem below then states in particular that the isogeny of (a) is given by

$$\mathbf{C}^n/u(\mathfrak{a}) \longrightarrow \mathbf{C}^n/u(N_\Phi(s)^{-1}\mathfrak{a})$$

so that in particular, $\mathbf{C}^n/u(N_\Phi(s)^{-1}\mathfrak{a})$ is isomorphic to A^σ, and that this isomorphism can be chosen in a manner that makes this isogeny, restricted to torsion points of the variety, correspond through u to multiplication by the idele $N_\Phi(s)^{-1}$.

Theorem 4.1 *Let $\mathcal{P} = (A, \iota, \mathcal{C})$ be a polarised abelian variety of type $(K, \Phi; \mathfrak{a}, \tau)$ as above. Fix $\sigma \in Aut(\mathbf{C}/K')$ and choose $s \in \mathbf{A}_K^*$ such that $\sigma_{|K'^{ab}} = [s, K']$. Then there is a unique complex analytic isomorphism*

$$\xi' : \mathbf{C}^n/u(N_\Phi(s)^{-1}\mathfrak{a}) \longrightarrow A^\sigma$$

having the following properties:

(1) $\mathcal{P}^\sigma$ is of type $(K, \Phi, N_\Phi(s)^{-1}\mathfrak{a}, N((s))\tau)$ with respect to ξ'.

(2) There is a commutative diagram

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{N_\Phi(s)^{-1}} & K/N_\Phi(s)^{-1}\mathfrak{a} \\ {\scriptstyle \xi\circ u}\downarrow & & \downarrow{\scriptstyle \xi'\circ u} \\ A & \xrightarrow{\sigma} & A^\sigma \end{array} \tag{15}$$

There are two parts in this theorem, which, though deeply related, answer two different questions. The first part gives a precise description of the type, and therefore of the isomorphism class of the image of the polarised abelian variety $(A, \iota, \mathcal{C})$ under an algebraic automorphism fixing the reflex field. The second one states, as Silverman ([5]) puts it, that on torsion points, such an algebraic action can be reinterpreted as an analytic action of multiplication by an idele.

The proof of this theorem requires quite a few results from the theory of good reduction of abelian varieties and more generally from algebraic geometry, which we don't want to develop here. Our account of the proof is therefore quite elliptical in the steps concerned with them: this is the main reason why it bears the title "Detailed sketch of proof" rather than just "Proof".

Summary of proof. After some useful reductions, we begin by proving the theorem for M-torsion points for some fixed M. We choose a convenient big number field L containing everything we need, as well as a prime $\mathfrak{P}$ of this number field satisfying some conditions. Thanks to this and class field theory, we can decompose s as $s = c\varpi e$ where $c \in K'^*$ and e is a unit idele (so that $N_\Phi(e)^{-1}\mathfrak{a} = \mathfrak{a}$), in order to divide up the proof into two smaller and easier steps: we split up the isogeny $\mathbf{C}^n/u(\mathfrak{a}) \longrightarrow \mathbf{C}^n/u(N_\Phi(s)^{-1}\mathfrak{a})$ into an isogeny

$$\mathbf{C}^n/u(\mathfrak{a}) \longrightarrow \mathbf{C}^n/u(N_\Phi(\varpi)^{-1}\mathfrak{a})$$

and an isomorphism

$$\mathbf{C}^n/u(N_\Phi(\varpi)^{-1}\mathfrak{a}) \longrightarrow \mathbf{C}^n/u(N_\Phi(s)^{-1}\mathfrak{a}).$$

The core of the proof is to prove that $\mathbf{C}^n/u(N_\Phi(\varpi)^{-1}\mathfrak{a}) \cong A^\sigma$, and to choose the isomorphism ξ' properly so that the corresponding isogeny $\kappa : A \longrightarrow A^\sigma$ coincides with σ on m-torsion: this is important to relate σ to multiplication by $N_\Phi(s)^{-1}$ on torsion points. The map ξ' is then obtained using ξ^* as shown in the following diagram:

$$\begin{array}{ccccc}
\mathbf{C}^n/u(\mathfrak{a}) & \longrightarrow & \mathbf{C}^n/u(N_\Phi(\varpi)^{-1}\mathfrak{a}) & \longrightarrow & \mathbf{C}^n/u(N_\Phi(s)^{-1}\mathfrak{a}) \\
\downarrow{\scriptstyle \xi} & & \downarrow{\scriptstyle \xi^*} & & \downarrow{\scriptstyle \xi'} \\
A & \xrightarrow{\kappa} & A^\sigma & \xrightarrow{\mathrm{id}} & A^\sigma
\end{array}$$

Finally a simple computation using the properties of ϖ and e proves requirement (2) for M-torsion points, and a last check shows that all the constructed ξ' for different values of M are the same.

Detailed sketch of proof.

1. Though the theorem doesn't require $\mathcal{P}$ to be defined over an algebraic number field, we will need to reduce to this case here as the proof uses reduction modulo primes in number fields. According to Shimura ([4], Proposition 26 of 12.3), an abelian variety with complex multiplication is always isomorphic to an abelian variety defined over a number field. Moreover, some results from algebraic geometry enable us to define $\mathcal{C}$ over a number field as well. Observing that if the theorem is true for some structure $\mathcal{P}$, it is also true for any structure isomorphic to it, we can assume $\mathcal{P}$ is defined over an algebraic number field.

2. We also reduce to the case where $\iota(\mathcal{O}_K) \subset \mathrm{End}(A)$, i.e. A is principal. We won't give details on this here.

3. We will begin by constructing the map ξ' so that it has the required properties only on M-torsion points for some sufficiently big integer M, and then show in the last step of the proof that all the maps we have constructed are the same. Fix therefore a positive integer M.

4. We choose a sufficiently big number field L over which to work: it has to be Galois, it has to contain the ray class field $K'_{(M)}$ of K' modulo M and be a field of definition for A and a set $\{A_i\}_i$ of representatives of isomorphism classes of abelian varieties of type (K, Φ) and for all homomorphisms between these varieties.

5. The proof will work by reduction modulo a well-chosen prime $\mathfrak{P}$ of L. Using the Tchebotarev density theorem, it can be chosen so that

   - $\sigma_{|L}$ is a Frobenius element for $\mathfrak{P}$,
   - the prime $\mathfrak{p} = \mathfrak{P} \cap K'$ is of inertia degree one with respect to $p = \mathfrak{p} \cap \mathbf{Q}$ (i.e. $N(\mathfrak{p}) = p$),

   and also so that $\mathfrak{P}$ satisfies some other properties each excluding only a finite number of primes:

   - $\mathfrak{p}$ is unramified in L,
   - the finite number of abelian varieties we are working with all have good reduction modulo $\mathfrak{P}$,
   - M is prime to $\mathfrak{P}$.

6. We are going to decompose the multiplication action by the idele s thanks to class field theory. Let $\varpi \in \mathbf{A}_{K'}^*$ be such that $\varpi_\mathfrak{q} = 1$ for every prime $\mathfrak{q} \neq \mathfrak{p}$, and $\varpi_\mathfrak{p}$ is a uniformiser of $K'_\mathfrak{p}$. Then $[s, K']$ agrees on $K'_{(M)}$ with $[\varpi, K']$, as they are both Frobenius elements for $\mathfrak{P}$. Therefore, according to 2.5 we can write $s\varpi^{-1} = ce$, where $c \in (K')^*$ and $e \in U(M)$, i.e.

$$e_\mathfrak{q} \in \mathcal{O}_{K',\mathfrak{q}}^* \quad \text{and} \quad e_\mathfrak{q} \equiv 1 \pmod{M\mathcal{O}_{K',\mathfrak{q}}} \quad \text{for all primes } \mathfrak{q}.$$

   Then $N_\Phi(s)^{-1}\mathfrak{a} = N_\Phi(\varpi)^{-1}N_\Phi(c)^{-1}N_\Phi(e)^{-1}\mathfrak{a} = N_\Phi(\mathfrak{p})^{-1}N_\Phi(c)^{-1}\mathfrak{a}$ (where $N_\Phi(\mathfrak{p})$ is the reflex norm of the ideal $\mathfrak{p}$, defined in the Remark below Proposition 3.10), since $(N_\Phi(e)) = \mathcal{O}_K$. In view of this decomposition, our new goal is to construct ξ^* and ξ' such that there is a commutative diagram

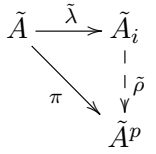
$$\begin{array}{ccccc}
\mathbf{C}^n & \xrightarrow{\text{id}} & \mathbf{C}^n & \xrightarrow{D_\Phi(N_\Phi(c))^{-1}} & \mathbf{C}^n \\
\downarrow & & \downarrow & & \downarrow \\
\mathbf{C}^n/u(\mathfrak{a}) & \longrightarrow & \mathbf{C}^n/u(N_\Phi(\mathfrak{p})^{-1}\mathfrak{a}) & \longrightarrow & \mathbf{C}^n/u(N_\Phi(s)^{-1}\mathfrak{a}) \\
\downarrow \xi & & \downarrow \xi^* & & \downarrow \xi' \\
A & \longrightarrow & A^\sigma & \xrightarrow{\text{id}} & A^\sigma
\end{array} \tag{16}$$

   and that the composition of the maps in the second line agrees on torsion points with multiplication by $N_\Phi(s)^{-1}$.

7. Let us first establish the $N_\Phi(\mathfrak{p})$-part, i.e. the left hand side of the above diagram. According to Proposition 3.15, $\mathbf{C}^n/u(N_\Phi(\mathfrak{p})^{-1}\mathfrak{a})$ is of type (K, Φ), so is isomorphic to some A_i. We therefore must prove that this A_i is isomorphic to A^σ. This isomorphism is constructed modulo $\mathfrak{P}$ and then lifted up as follows. Reduction modulo $\mathfrak{P}$ is denoted with tildes.

   a. The reduction $\tilde{\lambda}$ of the isogeny $\lambda : A \longrightarrow A_i$ is proven to be a totally inseparable map using differential forms. From this, denoting $\pi : \tilde{A} \longrightarrow \tilde{A}^p$ the p-th power map,

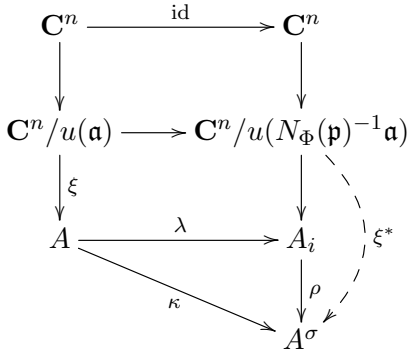
an isomorphism $\tilde{\rho} : \tilde{A}_i \longrightarrow \tilde{A}^p$ such that



is constructed.

b. Since σ modulo $\mathfrak{P}$ acts as the p-th power map, $\tilde{\rho}$ is lifted up to an isomorphism $\rho : A_i \longrightarrow A^\sigma$. Replacing λ by $\kappa = \rho \circ \lambda$, we get an isogeny $\kappa : A \longrightarrow A^\sigma$ whose reduction modulo $\mathfrak{P}$ is the p-th power map $\pi = \tilde{\rho} \circ \tilde{\lambda}$.

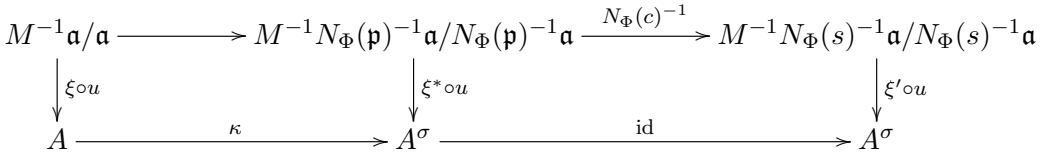
The map ξ^* is then obtained as shown in the following diagram.



8. The right-hand side of diagram (16) together with the map ξ' is then obtained easily from the left-hand side. Thanks to this diagram, we can finalise our proof of the first part of the theorem, and of the second part for M-torsion.

   a. *Computation of the type of* $(A^\sigma, \iota^\sigma, \mathcal{C}^\sigma)$: according to the diagram, the lattice associated to $(A^\sigma, \iota^\sigma, \mathcal{C}^\sigma)$ with respect to ξ' is $N_\Phi(s)^{-1}\mathfrak{a}$. A computation in terms of divisors and ℓ-adic representations shows that the element of K associated to $(A^\sigma, \iota^\sigma, \mathcal{C}^\sigma)$ via ξ^* is $p\tau$. Then, using Lemma 3.19, we get that the element corresponding to $(A^\sigma, \iota^\sigma, \mathcal{C}^\sigma)$ via ξ' is $N_\Phi(c)\overline{N_\Phi(c)}p\tau = N((c))N(\mathfrak{p})\tau = N((s))\tau$.

   b. Turning our attention to M-torsion points, we get



   Note that in this diagram, κ can be replaced by σ. Indeed, these two maps both reduce modulo $\mathfrak{P}$ to the p-th power map. M being prime to $\mathfrak{P}$, reduction modulo $\mathfrak{P}$ is injective on M-torsion, and therefore σ and κ agree on M-torsion.

   To check the constructed ξ' has the required properties, we need to prove that the action of σ on M-torsion points of A corresponds to multiplication by $N_\Phi(s)^{-1}$, that is, for $x \in M^{-1}\mathfrak{a}/\mathfrak{a}$

$$\xi \circ u(x)^\sigma = \xi' \circ u(N_\Phi(s)^{-1}x \bmod N_\Phi(s)^{-1}\mathfrak{a}).$$

Using the above diagram and the fact that σ and κ agree on M-torsion, we get

$$\begin{aligned}\xi \circ u(x)^\sigma = \kappa(\xi \circ u(x)) &= \xi^* \circ u(x \bmod N_\Phi(\mathfrak{p})^{-1}\mathfrak{a}) \\ &= \xi' \circ u(N_\Phi(c)^{-1}x \bmod N_\Phi(s)^{-1}\mathfrak{a}).\end{aligned}$$

$\xi' \circ u$ being injective, it suffices to prove that for every $t \in M^{-1}\mathfrak{a}$

$$N_\Phi(c)^{-1}t - N_\Phi(s)^{-1}t \in N_\Phi(s)^{-1}\mathfrak{a}. \tag{17}$$

Thanks to the decomposition $s = c\varpi e$ and after multiplication by M, this is equivalent to

$$t_q - (N_\Phi(\varpi)N_\Phi(e)t)_q \in M\mathfrak{a}_q \quad \text{for all primes } q \text{ and for all } t \in \mathfrak{a},$$

or simply to

$$(1 - N_\Phi(\varpi)_q N_\Phi(e)_q)\mathfrak{a}_q \subset M\mathfrak{a}_q \quad \text{for all primes } q.$$

According to the remark below Proposition 3.10, $N_\Phi(e)_q \equiv 1 \pmod{M\mathcal{O}_{K,q}}$ and $N_\Phi(e) \in \mathcal{O}_{K,q}^*$ for all q, so this reduces to

$$(1 - N_\Phi(\varpi)_q)\mathfrak{a}_q \subset M\mathfrak{a}_q.$$

If $q \neq p$, then $N_\Phi(\varpi)_q = 1$, so the above equation is true in this case. Now suppose $q = p$. M being prime to p, $M\mathfrak{a}_p = \mathfrak{a}_p$, so we have to prove

$$N_\Phi(\varpi)_p\mathfrak{a}_p \subset \mathfrak{a}_p.$$

But by construction of ϖ, $N_\Phi(\varpi)_p \in N_\Phi(\mathfrak{p})_p \subset \mathcal{O}_{K,p}$, which concludes the proof of (17) also in this case, $\mathfrak{a}$ being a fractional ideal.

9. Finally we have to prove ξ' doesn't in fact depend on the integer M. Take MN a multiple of M, denote ξ'_M the isomorphism we have constructed above, and ξ'_{MN} the isomorphism obtained by replacing M by MN, satisfying exactly the same properties for MN-torsion. Note that $\xi'_{MN} \circ \xi'^{-1}_M$ is an automorphism of (A^σ, ι^σ). Indeed, by definition ι^σ corresponds to D_Φ^σ both through ξ_M and through ξ'_{MN}, that is, we have $\xi'_M \circ D_\Phi^\sigma(a) = \iota^\sigma(a) \circ \xi'_M$ for all $a \in K$, and an analogous relation is true for ξ'_{MN}. Using this, we see that $\xi'_{MN} \circ \xi'^{-1}_M$ commutes with $\iota^\sigma(a)$ for all a. Therefore by Lemma 3.15, there is an element $b \in \mathcal{O}_K^*$ such that

$$\xi'_{MN} \circ \xi'^{-1}_M = \iota^\sigma(b).$$

This can be rewritten as $\xi'_{MN} = \xi'_M \circ D_\Phi^\sigma(b)$, thanks to which we can apply Lemma 3.19: A^σ is of the same type with respect to both ξ'_M and ξ'_{MN}, so we get $b\bar{b} = 1$. Using Lemma 3.2, we therefore have proved that $|b^\phi| = 1$ for every embedding $\phi : K \longrightarrow \mathbf{C}$, that is, b is a root of unity. We are going to show that, provided the initial M was sufficiently large, $b = 1$. For this, as $\mathrm{Aut}(\mathcal{P})$ is finite, we can choose b inside a finite set of representatives of

$$\iota^{-1}(\mathrm{Aut}(\mathcal{P})) \cap \{\text{roots of unity in } K\} \tag{18}$$

without changing $\iota(b)$. By assumption, ξ'_M and ξ'_{MN} both make diagram (15) commute on M-torsion. For every $w \in M^{-1}\mathfrak{a}/\mathfrak{a}$, $\xi \circ u(w)^\sigma$ can thus be expressed in two different ways, as done in the following calculation:

$$\begin{aligned}
\xi \circ u(bw)^\sigma &= \iota(b)^\sigma(\xi \circ u(w))^\sigma \text{ as through } \xi \circ u \text{ multiplication by } b \text{ becomes } \iota(b), \\
&= \iota(b)^\sigma \xi'_M \circ u(N_\Phi(s)^{-1}w) \text{ using assumption on } \xi'_M, \\
&= \xi'_{MN} \circ u(N_\Phi(s)^{-1}w) \text{ using } \xi'_{MN} \circ \xi'^{-1}_M = \iota^\sigma(b), \\
&= \xi \circ u(w)^\sigma \text{ using assumption on } \xi'_{MN},
\end{aligned}$$

so $bw = w$, which, w being M-torsion, implies $b \equiv 1 \pmod{M\mathcal{O}_K}$. But we have chosen b in a finite set of roots of unity. Therefore, if the initial M was sufficiently big, b is necessarily 1, which shows that $\xi'_M = \xi'_{MN}$. We conclude that diagram (15) commutes also on MN-torsion for all $N > 0$, which completes the proof. □

Theorem 4.2 *Theorem 4.1 holds if K is replaced by a CM-algebra W.*

Proof. First of all, by the same argument as in Step 2 of the proof of Theorem 4.1, we can assume $\mathfrak{a} = \prod_{i=1}^r \mathfrak{a}_i$ where $\mathfrak{a}_i$ is a fractional ideal of K_i for all i. This is needed to ensure that the isogeny $A \longrightarrow A_1 \times \ldots \times A_r$ constructed in the generalisation to CM-algebras of subsection 3.4 is actually an isomorphism. Then we can apply Theorem 4.1 to $(A_i, \iota_i, \mathcal{C}_i)$ with $\mathcal{C}_i$ determined in the generalisation to CM-algebras of subsection 3.5. To conclude, it suffices to combine the results for all i by taking the product. □

5 Construction of class fields

5.1 Fields of moduli

Let (W, Φ) be a CM-type. Consider a structure $\mathcal{P} = (A, \iota, \mathcal{C}, \{t_1, \ldots, t_r\})$ composed of an abelian variety A polarised by $\mathcal{C}$, an embedding $\iota : W \longrightarrow \mathrm{End}_{\mathbf{Q}}(A)$ and a set $\{t_1, \ldots, t_r\}$ of torsion points of A. For another such structure $\mathcal{P}' = (A', \iota', \mathcal{C}', \{t'_1, \ldots, t'_r\})$, an isomorphism $\mathcal{P} \longrightarrow \mathcal{P}'$ is defined to be an isomorphism $f : (A, \mathcal{C}) \longrightarrow (A', \mathcal{C}')$ such that $f(t_i) = t'_i$ for all $i = 1, \ldots, r$. A field of definition for $\mathcal{P}$ is a field k over which A, $\mathcal{C}$, every element of $\iota(W)$, as well as t_i for all i are rational.

Proposition 5.1 *Let $\mathcal{P}$ be such a structure. There exists a subfield $k_\mathcal{P}$ of $\mathbf{C}$ with the following properties:*

1. *Every field of definition for $\mathcal{P}$ contains $k_\mathcal{P}$.*
2. *If $\mathcal{P}$ is defined over a field k and $\sigma : k \hookrightarrow \mathbf{C}$ is an embedding of k into $\mathbf{C}$ then*
$$\sigma_{|k_\mathcal{P}} = id \quad \text{if and only if} \quad \mathcal{P} \text{ is isomorphic to } \mathcal{P}^\sigma.$$
3. *$k_\mathcal{P}$ is uniquely determined by these properties.*

We are not going to prove this proposition, but will merely remark that in the case where $\mathcal{P}$ is defined over some number field k, which without loss of generality we can assume to be a Galois extension of $\mathbf{Q}$, $k_\mathcal{P}$ is easily given by Galois theory, considering the field corresponding to the subgroup $H_\mathcal{P}$ of $\mathrm{Gal}(k/\mathbf{Q})$ defined by

$$H_\mathcal{P} = \{\sigma \in \mathrm{Gal}(k/\mathbf{Q}) |\ \mathcal{P} \text{ isomorphic to } \mathcal{P}^\sigma\}.$$

Lemma 5.2 *Let $k_{\mathcal{P}}$ be as above the field of moduli of the structure $\mathcal{P}$ of type (W, Φ). Then $k_{\mathcal{P}}$ contains the reflex field K' of K.*

Proof. It suffices to show that any automorphism σ of $\mathbf{C}$ fixing $k_{\mathcal{P}}$ also fixes K', i.e., satisfies

$$(\text{tr } \Phi(a))^{\sigma} = \text{tr } \Phi(a) \quad \text{for all} \quad a \in W.$$

Fix $a \in W$. In view of the chosen isomorphism $A \cong \mathbf{C}^n/\Lambda$, the element tr $\Phi(a)$ of K' is nothing other than the trace of the endomorphism $D_\Phi(a)$ of $\mathbf{C}^n$, obtained by lifting $\iota(a) \in \text{End}_{\mathbf{Q}}(A)$ as we did in 3.4, using the analytic representation of $\text{End}_{\mathbf{Q}}(A)$.For σ fixing $k_{\mathcal{P}}$, take an isomorphism $\lambda : \mathcal{P} \longrightarrow \mathcal{P}^{\sigma}$. It satisfies $\lambda\iota(a) = \iota(a)^{\sigma}\lambda$. λ induces an isomorphism of $\mathbf{C}^n$ that we also denote by λ. By this method, we have actually lifted $\iota(a)$ to an endomorphism of the tangent space $\text{Tgt}_0(A)$ of A at 0, and λ to an isomorphism $\text{Tgt}_0(A) \longrightarrow \text{Tgt}_0(A^{\sigma})$. σ induces an isomorphism between these tangent spaces, so in particular the lift of $\iota(a)^{\sigma}$ is $D_\Phi(a)^{\sigma}$. Then $\lambda D_\Phi(a) = D_\Phi(a)^{\sigma}\lambda$, and $D_\Phi(a)$ and $D_\Phi(a)^{\sigma}$, being conjugate, have the same trace. □

Kummer varieties An abelian variety on its own can have an infinite number of automorphisms. Weil's fundamental idea when introducing polarisations was that

Proposition 5.3 *A polarised abelian variety has only a finite number of automorphisms.*

Therefore, considering an abelian variety A together with a polarisation $\mathcal{C}$, we can prove that an analogue of a Weber function, namely a quotient $h : A \longrightarrow A/\text{Aut}(A, \mathcal{C})$, can be defined. An alternative definition that also works is $h : A \longrightarrow A/\text{Aut}(A, \iota, \mathcal{C})$, since $\text{Aut}(A, \iota, \mathcal{C})$ is also finite. In what follows, we will always denote the Kummer variety of $(A, \iota, \mathcal{C})$ by (V, h) where $V = A/\text{Aut}(A, \iota, \mathcal{C})$ and $h : A \longrightarrow V$ the above quotient map.

The field of moduli of a structure $\{A, \iota, \mathcal{C}, \{t_i\}\}$ can be constructed explicitly in terms of the $h(t_i)$ and the field of moduli of $A, \iota, \mathcal{C}$, as stated in the following proposition which we won't prove:

Proposition 5.4 *Let $(A, \iota, \mathcal{C})$ be a polarised abelian variety with complex multiplication and (V, h) the Kummer variety of A. Then for every $t \in A$ the field of moduli $k_{A,\iota,\mathcal{C},t}$ is equal to $k_{A,\iota,\mathcal{C}}(h(t))$.*

5.2 Construction of class fields

Let, (W, Φ) be a CM-pair, (K', Φ') its reflex, $\mathcal{P} = (A, \iota, \mathcal{C}, \{t_1, \ldots, t_r\})$ a structure with $(A, \iota, \mathcal{C})$ a polarised abelian variety of type $(W, \Phi, \mathfrak{a}, \tau)$ and $t_1, \ldots, t_r$ torsion points of A. Define also $w_i \in W/\mathfrak{a}$ such that $\xi \circ u(w_i) = t_i$ for all i. Denote by k the field of moduli $k_{\mathcal{P}}$ of $\mathcal{P}$. Let us begin with a general theorem from which we will derive all other results:

Theorem 5.5 *Let T be the subgroup of $\mathbf{A}^*_{K'}$ defined by*

$$T = \left\{ s \in \mathbf{A}^*_{K'} \middle| \; \exists b \in W^* \text{ such that } \begin{array}{c} N_\Phi(s)^{-1}\mathfrak{a} = b\mathfrak{a}, \\ b\bar{b}N((s)) = 1 \\ N_\Phi(s)^{-1}w_i = bw_i \text{ for all } i \end{array} \right\}.$$

Then k is an abelian extension of K' corresponding to the subgroup T.

Proof. Note first of all that by Lemma 5.2, k contains K', so any automorphism σ of $\mathbf{C}$ fixing k induces $[s, K']$ on K'^{ab} for some idele s. Denote by F the extension of K' corresponding to T. Take ξ' as in Theorem 4.1, so that $\xi' \circ u(N_\Phi(s)^{-1} w_i) = (\xi \circ u(w_i))^\sigma$.

Proof that $k \subset F$. It suffices to prove that if s is an element of T and σ is an automorphism of $\mathbf{C}$ inducing $[s, K']$ on K'^{ab}, then σ fixes k, i.e. $\mathcal{P}$ is isomorphic to $\mathcal{P}^\sigma$. But using the main theorem of complex multiplication and the assumption on s we see that there is a $b \in W$ such that $(A, \iota, \mathcal{C})^\sigma$ is of type $(W, \Phi, b\mathfrak{a}, (b\bar{b})^{-1}\tau)$. This type is equivalent to the type of $(A, \iota, \mathcal{C})$, so $(A, \iota, \mathcal{C})$ and $(A, \iota, \mathcal{C})^\sigma$ are isomorphic by Proposition 3.18, the isomorphism being given by $\lambda = \iota(b)$. We now need to check $\lambda(t_i) = t_i^\sigma$ for all i. The left-hand side is by definition of λ given by $\xi' \circ u(bw_i)$, and the right-hand side, using the property (15) of ξ' from the main theorem, is $\xi' \circ u(N_\Phi(s)^{-1} w_i)$. Both sides are equal since $s \in T$.

Proof that $k \supset F$. Let σ be an automorphism fixing k and inducing $[s, K']$ on K'^{ab} for some $s \in \mathbf{A}_W^*$. To conclude, we must prove that $s \in T$. By definition of k, there is an isomorphism $\lambda : \mathcal{P} \longrightarrow \mathcal{P}^\sigma$. Using the main theorem of complex multiplication, we know that $\mathcal{P}^\sigma$ is of type $(W, \Phi, N_\Phi(s)^{-1}\mathfrak{a}, N((s))\tau)$ By Lemma 3.14, λ comes from a multiplication by b map on W for some $b \in W$, so we already know $N_\Phi(s)^{-1}\mathfrak{a} = b\mathfrak{a}$ and $b\bar{b}N((s)) = 1$ by Proposition 3.19. On the other hand, since λ is an isomorphism, we must by definition have $\lambda(t_i) = t_i^\sigma$ for every i. Therefore

$$\xi' \circ u(N_\Phi(s)^{-1}(w_i)) = (\xi \circ u(w_i))^\sigma = \lambda(\xi \circ u(w_i)) = \xi' \circ u(bw_i),$$

and thus, $\xi' \circ u$ being injective, $s \in T$. □

This proposition shows how the fact of considering CM-algebras and not only CM-fields enlarges the scope of our results by allowing us to impose more conditions on the elements in the group T.

As in the elliptic curves case, we can be more precise in the case where A is principal, that is $\iota(\mathcal{O}_W) \subset \mathrm{End}(E)$.

Corollary 5.6 *Let (W, Φ) and $(A, \iota, \mathcal{C})$ of type $(W, \Phi, \mathfrak{a}, \tau)$ as above. Suppose in addition that A is principal. Then the field of moduli $k_{A,\iota,\mathcal{C}}$ is an unramified abelian extension of K'.*

Proof. Apply Theorem 5.5 omitting the w_i. Then it suffices to prove that the group T contains the group of unit ideles of K'

$$U(1) = \{s \in \mathbf{A}_{K'}^* \mid s_\mathfrak{p} \in \mathcal{O}_{\mathfrak{p},K'}^* \text{ for all } \mathfrak{p}\}.$$

If $s \in U(1)$, then $(s) = \mathcal{O}_{K'}$ (so $N((s)) = 1$) and $(N_\Phi(s)^{-1}) = \mathcal{O}_W$. Since A is principal, $\mathfrak{a}$ is a fractional ideal of K, so $N_\Phi(s)^{-1}\mathfrak{a} = \mathfrak{a}$. Therefore, taking $b = 1$ we see $s \in T$. □

A result analogous to the elliptic curves case also holds for unramified extensions. One must however be prudent as there are different fields with different ideals involved: the best bound we can give on the conductor is therefore a rational integer. Denote by

$$A[\mathfrak{c}] = \{t \in A \mid at = 0 \text{ for all } a \in \mathfrak{c}\}$$

the group of $\mathfrak{c}$-torsion points of A for any integral ideal $\mathfrak{c}$ in W.

Corollary 5.7 *Let (W, Φ),$(A, \iota, \mathcal{C})$ be as above, and (V, h) the Kummer variety of $(A, \iota, \mathcal{C})$. Let moreover $\mathfrak{c} = \mathfrak{c}_1 \times \ldots \times \mathfrak{c}_r$ be an integral ideal of W, c_i the smallest positive integer contained in $\mathfrak{c}_i$ for all i, and c the least common multiple of the c_i. Then $k_{A,\iota,\mathcal{C}}(h(A[\mathfrak{c}]))$ is an abelian extension of K', of conductor dividing c.*

Proof. According to Proposition 5.4, $k_{A,\iota,\mathcal{C}}(h(A[\mathfrak{c}])) = k_{A,\iota,\mathcal{C},A[\mathfrak{c}]}$. Applying Theorem 5.5 with the set $\{t_i\}_i = A[\mathfrak{c}]$, it is therefore sufficient to check that the corresponding group T contains the group of unit ideles modulo $\mathfrak{c}$:

$$U(c) = \{s \in \mathbf{A}_{K'}^* \mid s_\mathfrak{p} \in \mathcal{O}_{\mathfrak{p},K'}^* \text{ and } s_\mathfrak{p} \equiv 1 \pmod{c\mathcal{O}_{\mathfrak{p},K'}} \text{ for all } \mathfrak{p}\}.$$

Let $s \in U(\mathfrak{c})$. As in the proof of Corollary 5.6, we have $N((s)) = 1$ and $(N_\Phi(s)^{-1}) = \mathcal{O}_W$. But we have moreover that $N_\Phi(s)$ is a unit idele modulo c in W, so for every $t = \xi \circ u(w) \in A[\mathfrak{c}]$, $N_\Phi(s)(t) = t$. Therefore $s \in T$ and the proof is finished. □

References

[1] Lang, S., Complex Multiplication, Springer, 1983

[2] Milne, J.S., Complex Multiplication, on www.jmilne.org, 2006

[3] Shimura, G., Abelian varieties with complex multiplication and modular functions, Princeton University Press, 1998

[4] Shimura, G., Introduction to the arithmetic theory of automorphic functions, Princeton University Press, 1994

[5] Silverman, J.H., Advanced topics in the Arithmetic of Elliptic Curves, Springer, 1994

[6] Silverman, J.H., The Arithmetic of Elliptic Curves, Springer, 1986