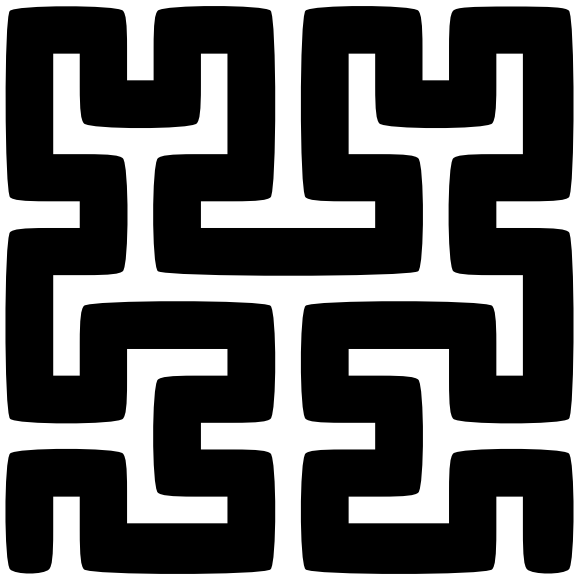

Polynesian Journal of Mathematics

Volume 1, Issue 5

Polarized products of elliptic curves with complex multiplication and field of moduli $\mathbb{Q}$

Fabien Narbonne

with an appendix by

Francesc Fité Xavier Guitart

Received 1 Jul 2024
Revised 17 Dec 2024
Published 20 Dec 2024
Communicated by Gaetan Bisson

DOI: 10.69763/polyjmath.1.5

Polynesian Journal of Mathematics
Volume 1, Issue 5 (Dec. 2024)

Polarized products of elliptic curves with complex multiplication and field of moduli $\mathbb{Q}$

Fabien Narbonne[1]

with an appendix by

Francesc Fité[2] Xavier Guitart[2]

[1]Université de Rennes, IRMAR - UMR CNRS 6625, Rennes, France
[2]Departament de matemàtiques i informàtica, Universitat de Barcelona

Abstract

Let R be the maximal order in an imaginary quadratic field K. We give an equivalence of categories between the category of polarized abelian varieties isomorphic to a product of elliptic curves over $\mathbb{C}$ with complex multiplication (CM) by R and the category of integral hermitian R-lattices. Then we apply this equivalence to enumerate all the genus 2 and 3 curves with field of moduli $\mathbb{Q}$ and with Jacobian isomorphic to a product of elliptic curves with CM by R.

Introduction

Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by a maximal order R in an imaginary quadratic field K. Then E admits a model over $\overline{\mathbb{Q}}$. It even admits one over $\mathbb{Q}(j(E))$, which has degree $\#\mathrm{Cl}(R)$ over $\mathbb{Q}$, and not over any sub-extension. It may then be surprising that powers of CM elliptic curves may be defined over smaller fields than expected, sometimes even over $\mathbb{Q}$. In [7, Theorem 1.1 and 1.2] the authors show for instance that there are abelian surfaces defined over $\mathbb{Q}$, $\overline{\mathbb{Q}}$-isogenous to the square of a CM elliptic curve, for exactly 45 discriminants even though there are only 13 CM elliptic curves over $\mathbb{Q}$. From this, they deduce [7, Corollary 1.3] that there are exactly 92 $\overline{\mathbb{Q}}$-endomorphism algebras of geometrically split abelian surfaces over $\mathbb{Q}$. This study is motivated by the conjecture on the possible finiteness of the set of endomorphism rings of abelian varieties of a given dimension over a fixed-degree extension field of $\mathbb{Q}$.

A weaker requirement is to ask for the field of moduli of a (polarized) abelian variety to be $\mathbb{Q}$. In [9] the authors give the finite list of indecomposable principally polarized abelian surfaces (also known as Jacobian of genus 2 curves) with field of moduli $\mathbb{Q}$ which are isomorphic to E^2.

In the present article we address the case of abelian varieties with field of moduli $\mathbb{Q}$ isomorphic over $\mathbb{C}$ to products $E_1 \times \cdots \times E_g$, $g > 1$, of elliptic curves with CM by a maximal order R and we give an exhaustive list of these principally polarized abelian varieties for the case $g = 2$ in Table 1 and for $g = 3$ in Table 2. Before explaining the structure of the paper and our strategy, we mention the following natural generalization to abelian varieties isomorphic to products $E_1 \times \cdots \times E_g$, $g > 1$, of elliptic curves with CM by possibly distinct orders in the same imaginary quadratic field K. By [13, Theorem 2], this is equivalent to considering abelian varieties isogenous to E^g over $\mathbb{C}$ for a given elliptic curve E with CM by K. In my PhD thesis, I presented heuristic results for $g = 2$ in this direction, see [21, Table A.1, A.2 and A.3]. Note that in [21, Théorème 2.2.33], the equivalence of categories of Theorem 2.4 is already proved for arbitrary orders. To finish the proof, one would need to check the validity of Theorem 3.1 and Theorem 3.2 in this generality. We also hope to address the finer question the existence of a model over $\mathbb{Q}$ for principally polarized abelian variety with field of moduli $\mathbb{Q}$. This theoretical result would also lead to the more refined project of having certified models over $\mathbb{Q}$ when the descent is possible. Very recent results contained in [16] would help to achieve this. Some certified models of genus 2 curves over $\mathbb{Q}$ with Jacobian isomorphic to a product of CM elliptic curves can be found in [5].

In Section 1 we recall some properties of the classical equivalence of categories between the complex abelian varieties and polarizable tori and how it behaves with respect to polarizations. Polarizations on abelian varieties give rise to positive definite hermitian forms with a compatibility condition on the lattice.

In Section 2, we restrict the equivalence of categories to the abelian varieties isomorphic to the product of elliptic curves with complex multiplication by R. For these abelian varieties, we associate the complex tori V/Γ, where V is a $\mathbb{C}$-vector space and Γ is a lattice in V. The lattice Γ can be endowed with the structure of an R-module, providing additional structure than the $\mathbb{Z}$-module one it already has. The corresponding hermitian form endows the R-module Γ with the structure of an *integral hermitian lattice* (up to rescaling the hermitian form by a constant that only depends on R). This restriction leads to an equivalence of categories between polarized abelian varieties isomorphic to a product of elliptic curves with CM by R and integral hermitian R-lattices (Theorem 2.4). Moreover, hermitian forms corresponding to principal polarization give *unimodular lattices* through the equivalence. We may note that a similar functor is developed in [12] in a much wider framework since it is defined for any field, not only $\mathbb{C}$. Under some conditions, it is also an equivalence of categories. However, we chose to focus our attention on a much simpler functor since we will need to refine it in the next section.

The goal of Section 3 is to translate the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on abelian varieties $\overline{\mathbb{Q}}$-isomorphic to $E_1 \times \cdots \times E_g$ into the category of integral hermitian lattices through the previous functor. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ can be decomposed into two steps: the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and the action of $\mathrm{Gal}(K/\mathbb{Q})$, the complex conjugation. For the first one, we use the existence of a surjective morphism $F\colon \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{Cl}(R)$ such that the action of $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ on abelian varieties corresponds to the tensor product of the associated lattice by a representative of $F(\sigma)$ (and a rescaling of the hermitian form).

Still, for both actions, we need to rigidify the choice of the target objects under the previous equivalences of categories, which are defined only up to $\mathbb{C}$-isomorphisms. Indeed, unlike [9] where the compatibilities between the various abelian varieties and their conjugate were obvious, we could not find a simple way to impose them from abstract nonsense. We therefore use the explicit algebraization by the Weierstrass function for elliptic curves to be able to work out the explicit Galois action on the associated hermitian R-lattices (see Proposition 3.6) and we then extend it, component by component, to products of elliptic curves in order to obtain our main results (Theorems 3.1 and 3.2). Notice that the main difficulty is to be able to keep the abelian varieties, their isogenies *and* their analytic representation defined over $\overline{\mathbb{Q}}$ to be able to translate the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

In Section 4, we look at the case when $\mathbb{Q}$ is the field of moduli of the indecomposable principally polarized abelian varieties $A \simeq E_1 \times \cdots \times E_g$ with E_i with CM by R. We first extend the result of [9] showing that if $\mathbb{Q}$ is the field of moduli then $\mathrm{Cl}(R)$ has exponent dividing g. We also show that the Steinitz class of the R-lattice associated with A is of order at most 2 (see Proposition 4.1). From this, we deduce the surprising Corollary 4.2 that odd-dimensional A with field of moduli $\mathbb{Q}$ must be isomorphic to the power of an elliptic curve. At the end of Section 4 we present the computations using the algorithms previously developed. In Table 1 we give the complete classification of all principally polarized indecomposable abelian surfaces with field of moduli $\mathbb{Q}$ sorted by discriminants. In Table 2 we give a similar classification for abelian varieties of dimension $g = 3$. The classifications are complete thanks to the results of Appendix A written by Francesc Fité and Xavier Guitart. Proposition 4.1, shows that we should consider discriminants of quadratic fields with class group exponent g where g is the dimension of the abelian varieties. This condition is too weak to have an unconditional classification. Indeed, even if it is known that there are only finitely many discriminants of exponent 2 and 3, the complete list is known only under the Extended Riemann Hypothesis (see [4]). Proposition A.1 shows that a dimension 2 split Jacobian $(E_1 \times E_2)$ with field of moduli $\mathbb{Q}$ and E_i with CM by the same field K must satisfy $\#\,\mathrm{Cl}(K) \in \{1, 2, 4\}$. There exist imaginary quadratic fields with class group exponent 2 of order 8 and 16 (and no other according to ERH) but the proposition guarantees that we will not find any curve corresponding to these discriminants. Proposition A.5 gives a similar bound in dimension $g = 3$; $\#\,\mathrm{Cl}(K) \in \{1, 3\}$. It is interesting to note also that we can run the computations for the exponent 2 discriminant of class number 8 and 16 and, unsurprisingly, we find no Jacobian with field of moduli $\mathbb{Q}$. However, the computations are too expensive for the discriminant $\Delta = -4027$ with class group $\mathrm{Cl}(\Delta) \simeq (\mathbb{Z}/3\mathbb{Z})^2$. Hence, even under ERH, the classification would not have been complete without the Appendix A.

Acknowledgments

I would like to acknowledge Francesc Fité and Xavier Guitart who motivated this project and helped until its fulfillment. As mentioned before, they also wrote the Appendix A which allows the Extended Riemann Hypothesis to be dropped in the classifications. Thank you also for meaningful discussions we had at the COUNT conference.

In addition, I want to thank Marco Streng for his attention and advice along the way of this work. I would also like to address a special thank to Markus Kirschmer for his advice and patience answering all of my questions about hermitian lattices. He also gave me an extension of the Magma library of [15] to handle more efficiently the classification of free hermitian unimodular R-lattices which we used for the computation of the dimension $g = 3$ case in Section 4.3. Finally, I want to thank Harun Kir for the rich discussions we had on this subject and for his precious support for this work.

1 Complex abelian varieties and complex tori

1.1 Abelian varieties and polarizable tori

Let us first recall that there is an equivalence of categories between abelian varieties over $\mathbb{C}$ and the category of polarizable tori given by $\mathbf{T}\colon A \mapsto A(\mathbb{C})$, see [19, Theorem 2.9]. A *complex torus* is a quotient of groups $X = V/\Gamma$ with V a complex vector space of finite dimension and Γ a $\mathbb{Z}$-*lattice* of V, i.e., a subgroup of V generating V over the reals. A torus $X = V/\Gamma$, or a lattice $\Gamma \subset V$, is said to be *polarizable* if there exists a positive definite hermitian form $h\colon V \times V \to \mathbb{C}$ such that

$$\operatorname{im} h(\Gamma, \Gamma) \subset \mathbb{Z}$$

where im is the imaginary part. Morphisms of complex tori are, in particular, morphisms of groups $\varphi\colon X = V/\Gamma \to X' = V'/\Gamma'$. Such a map can be lifted to a $\mathbb{C}$-linear map $\varphi_{\mathrm{an}}\colon V \to V'$ that sends Γ to Γ' called the *analytic representation* of φ. The group morphism $\varphi_{\mathrm{rat}} = \varphi_{\mathrm{an}|\Gamma}\colon \Gamma \to \Gamma'$ is called the *rational representation* of φ. We denote the set of the analytic representations of morphisms between X and X' by $\operatorname{Hom}_{\mathbb{C}}(\Gamma, \Gamma')$. We will often consider analytic representations directly as morphisms of polarizable tori.

A surjective morphism $f\colon A \to B$ between abelian varieties A and B over $\mathbb{C}$ of equal dimension is called an *isogeny*; its kernel is finite and its cardinality $\#\ker f$ is called the *degree* of f, denoted $\deg f$. Via the functor $\mathbf{T}$, we will also call $\varphi\colon V/\Gamma \longrightarrow V/\Gamma'$ an isogeny. The degree of φ is defined in the same way as $\deg\varphi = \#\ker\varphi$. Moreover, it satisfies

$$\deg\varphi = [\Gamma'\colon \varphi_{\mathrm{an}}(\Gamma)] = \deg f$$

with $[\Gamma'\colon \varphi_{\mathrm{an}}(\Gamma)] = \#(\Gamma'/\varphi_{\mathrm{an}}(\Gamma))$, the index of $\varphi_{\mathrm{an}}(\Gamma)$ in Γ'.

1.2 Duality

Let V be a g-dimensional complex vector space and $\Gamma \subset V$ a $\mathbb{Z}$-lattice. The dual lattice associated with Γ is defined by

$$\widehat{\Gamma} = \{\ell \in V^* \mid \operatorname{im}\ell(\Gamma) \subset \mathbb{Z}\}$$

where V^* denotes the set of antilinear forms $\ell\colon V \to \mathbb{C}$. This defines the dual complex torus of V/Γ, denoted $\widehat{V/\Gamma} = V^*/\widehat{\Gamma}$.

If A is a complex abelian variety such that $A(\mathbb{C}) \simeq V/\Gamma$ then there exists an isomorphism $\widehat{A}(\mathbb{C}) \simeq \widehat{V/\Gamma}$, where $\widehat{A}$ is the dual abelian variety of A (see [20]). Moreover, for a morphism $f\colon A \to B$ and $\varphi = \mathbf{T}(f)\colon V/\Gamma \to V'/\Gamma'$ we have $\mathbf{T}(\widehat{f})_{\mathrm{an}} = \varphi_{\mathrm{an}}^*$ with

$$\varphi_{\mathrm{an}}^*\colon \begin{cases} V'^* \longrightarrow V^* \\ \ell \longmapsto \ell \circ \varphi_{\mathrm{an}} \end{cases}$$

where $\widehat{f}\colon \widehat{B} \to \widehat{A}$ is the dual morphism of f (see [1, Section 2.4]).

1.3 Polarizations and hermitian forms

Let A be an abelian variety and let $\mathcal{L}$ be a line bundle. We consider the map

$$a_{\mathcal{L}}\colon \begin{cases} A \longrightarrow \widehat{A} \\ x \longmapsto t_x^*\mathcal{L} \otimes \mathcal{L}^{-1} \end{cases}$$

with t_x the translation by x map. Consider isomorphisms $A(\mathbb{C}) \simeq V/\Gamma$ and $\widehat{A}(\mathbb{C}) \simeq V^*/\widehat{\Gamma}$. Let $h = c_1(\mathcal{L})$ be the first Chern class of $\mathcal{L}$, which we identify with a hermitian form on V (see [1, Lemma 2.4.5]). Then the map $\rho_h \in \mathrm{Hom}_{\mathbb{C}}(\Gamma, \widehat{\Gamma})$ defined by

$$\rho_h\colon \begin{cases} V \longrightarrow V^* \\ v \longmapsto h(v, \_) \end{cases}$$

is the analytic representation of $a_{\mathcal{L}}$. A polarization on an abelian variety A is an isogeny $a_{\mathcal{L}}$ with $\mathcal{L}$ an ample line bundle. In this case, its first Chern class h is a positive definite hermitian form (see [1, Proposition 4.5.2]).

A pair (A, a) with A an abelian variety and a a polarization is called a *polarized abelian variety*. Morphisms of polarized abelian varieties are defined by maps $f\colon (A, a) \to (B, b)$ such that $\widehat{f}bf = a$ and we call them *polarized isogenies*. The distinction between polarized and non-polarized isogenies is essential; when we do not specify that an isogeny between polarized varieties is itself polarized, it refers to a morphism between the underlying abelian varieties without their polarizations. A *polarized torus* is a pair $(V/\Gamma, \rho_h)$, also denoted by (Γ, h), with V/Γ a complex torus and $\rho_h \in \mathrm{Hom}_{\mathbb{C}}(\Gamma, \widehat{\Gamma})$ induced by a positive definite hermitian form h, i.e., $\rho_h(v) = h(v, \_)$. We analogously define morphisms $\varphi\colon (V/\Gamma, \rho_h) \to (V'/\Gamma', \rho_{h'})$ between polarized tori. Their analytic representation must satisfy $\varphi_{\mathrm{an}}^*\rho_{h'}\varphi_{\mathrm{an}} = \rho_h$ which means that for $v, w \in V$,

$$\rho_h(v)(w) = h(v, w) = h'(\varphi_{\mathrm{an}}(v), \varphi_{\mathrm{an}}(w)).$$

In particular, analytic representations of polarized isogenies define isometries on the associated hermitian vector spaces. In the following we will call a pair (V, h) made of a $\mathbb{C}$-vector space and h a positive definite hermitian form a *hermitian space*. Since the functor $\mathbf{T}$ is an equivalence of categories, it also defines an equivalence of categories $\mathbf{T}^p$ between polarized abelian varieties and polarized tori $(A, a) \mapsto (X = \mathbf{T}(A), \rho_h = \mathbf{T}(a))$.

For any group schemes A and B over a field k there is an isomorphism of groups

$$A(k) \times B(k) \simeq (A \times_k B)(k).$$

We can apply it to abelian varieties over $\mathbb{C}$. For $A(\mathbb{C}) \simeq V_A/\Gamma_A$, $B(\mathbb{C}) \simeq V_B/\Gamma_B$ and $(A \times B)(\mathbb{C}) \simeq V/\Gamma$ we have

$$V/\Gamma \simeq (V_A/\Gamma_A) \times (V_B/\Gamma_B).$$

Hence $\Gamma \simeq \Gamma_A \times \Gamma_B$ and in terms of categories, the functor $\mathbf{T}$ commutes with products. In the same way, the functor $\mathbf{T}^p$ also commutes with products.

2 Totally split CM abelian varieties and R-module structure

Let R be the maximal order of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ with d a positive square-free integer. An R-lattice is a finitely presented, torsion-free R-module. We denote by $\boldsymbol{\mathcal{L}}_R$ the category of R-lattices. In this section, we want to show that there exist equivalences of categories

- between $\boldsymbol{\mathcal{A}}_R$, the category of complex abelian varieties isomorphic to a product of elliptic curves with CM by R, and $\boldsymbol{\mathcal{L}}_R$;
- between $\boldsymbol{\mathcal{A}}_R^p$, the category of complex polarized abelian varieties isomorphic to a product of elliptic curves with CM by R, and $\boldsymbol{\mathcal{L}}_R^{h,int}$, the category of integral hermitian R-lattices, i.e. R-lattices L equipped with a positive definite hermitian form H on $KL = L \otimes_R K$, such that $H(L, L) \subset R$.

For the rest of the article we fix field extensions

$$\mathbb{Q} \longrightarrow K \longrightarrow \overline{\mathbb{Q}} \longrightarrow \mathbb{C}.$$

2.1 Elliptic curves with complex multiplication over $\mathbb{C}$

Let $R = \mathbb{Z}[\omega]$ be the maximal order of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta < 0$ the discriminant of $K/\mathbb{Q}$ and $\alpha_R = \operatorname{im} \omega > 0$. Notice that α_R does not depend on the chosen generator ω with positive imaginary part.

Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by R, i.e., there exists a ring isomorphism $\operatorname{End}(E) \simeq R$. Let $\Lambda \subset \mathbb{C}$ be a lattice such that there is an isomorphism $\eta : \mathbb{C}/\Lambda \to E(\mathbb{C})$ (of Lie groups). Then we will denote E by E_Λ. By [24, Proposition II.1.1.] there is a unique isomorphism

$$[.]_E : R \to \operatorname{End}(E)$$

characterized, for any $\alpha \in R$, by the commutativity of the diagram of Figure 1. This isomorphism does not depend on η and we will use it when we identify R with $\operatorname{End}(E)$.

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{z\mapsto\alpha z} & \mathbb{C}/\Lambda \\ \eta \downarrow & & \downarrow \eta \\ E_\Lambda(\mathbb{C}) & \xrightarrow{[\alpha]} & E_\Lambda(\mathbb{C}) \end{array}$$

Figure 1: The bracket isomorphism

According to [24, Proposition 2.1] all CM elliptic curves over $\mathbb{C}$ admit a model over $\overline{\mathbb{Q}}$. We denote by $\mathrm{Ell}(R)$ the set of isomorphism classes of elliptic curves over $\overline{\mathbb{Q}}$ with CM by R. We recall from [24, Proposition 1.2] that $\mathrm{Cl}(R)$, the class group of R, acts simply transitively on $\mathrm{Ell}(R)$ and the action is given by

$$\mathfrak{a} \star E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda},$$

where $\mathfrak{a}$ is a fractional ideal of R. The action is well defined on the isomorphism classes because another representative $\mathfrak{b}$ of the class of $\mathfrak{a}$ in $\mathrm{Cl}(R)$ differs from $\mathfrak{a}$ by a scalar and then $\mathfrak{a}^{-1}\Lambda$ and $\mathfrak{b}^{-1}\Lambda$ are homothetic lattices.

2.2 Totally split complex tori and R-lattice structure

Let L be an R-lattice, i.e., a finitely presented, torsion-free R-module. Since R is maximal, L is a module over a Dedekind domain and by [22, Theorem 81.3], we can always write L as a sum

$$L = \bigoplus_{i=1}^{g} \mathfrak{a}_i x_i,$$

with $(x_1, \ldots, x_g)$ a basis of KL and $\mathfrak{a}_1, \ldots, \mathfrak{a}_g$ fractional ideals of R. The family $(\mathfrak{a}_i, x_i)$ is called a *pseudo-basis* of L and the *Steinitz class* $\mathrm{st}(L)$ of L is defined by the class of the product $\mathfrak{a}_1 \cdots \mathfrak{a}_g$ in $\mathrm{Cl}(R)$. The Steinitz class of a lattice together with its rank determines its R-isomorphism class by [2, Theorem 13].

For an R-ideal $\mathfrak{a}$, the norm of $\mathfrak{a}$ is defined by $N(\mathfrak{a}) = \#(R/\mathfrak{a})$. We can extend the definition of the norm to any fractional ideal by the equality $N(\lambda\mathfrak{a}) = |\lambda|^2 N(\mathfrak{a})$ for any $\lambda \in K$.

Throughout this article, different notations will be used to denote lattices depending on the context:

- The notation Γ will denote a lattice in a $\mathbb{C}$-vector space.
- The notation Λ will denote a lattice in $\mathbb{C}$ only.
- The notation L will denote a lattice over an imaginary quadratic order R.

Thus, the notations Γ and Λ will be reserved for the analytical aspect, for complex tori, while L will be used for the algebraic aspect. The functor **F**, defined in Theorem 2.1, connects complex tori to hermitian lattices, and these notations will help clarify the

category in which we are working. For the same reasons we write h for the hermitian forms coming from polarizable tori and H for R-lattices.

Theorem 2.1. *Let R be an order in an imaginary quadratic field K. There is an equivalence of categories between the category $\boldsymbol{\mathcal{A}}_R$ of abelian varieties isomorphic to a product of elliptic curves with CM by R, and the category $\boldsymbol{\mathcal{L}}_R$ of R-lattices given by*

$$\mathbf{F}\colon \begin{cases} \boldsymbol{\mathcal{A}}_R \longrightarrow \boldsymbol{\mathcal{L}}_R \\ A \text{ s.t. } A(\mathbb{C}) \simeq V/\Gamma \longmapsto \Gamma \\ (\mathbb{C}L)/L \longmapsto L \end{cases}$$

on objects and, for arrows, $f\colon A(\mathbb{C}) \simeq V/\Gamma \to A'(\mathbb{C}) \simeq V'/\Gamma'$, given by $\mathbf{F}(f) = f_{rat}$.

Proof. Let $A \in \boldsymbol{\mathcal{A}}_R$ such that $\mathbf{T}(A) = A(\mathbb{C}) = V/\Gamma$. There is an isomorphism $\varphi\colon V/\Gamma \to \mathbb{C}^g/\bigoplus \Lambda_i$. The $\mathbb{Z}$-lattices Λ_i have a natural structure of and $R = \mathrm{End}(\Lambda_i)$-module. The lattice Γ is stable by multiplication by R. Indeed,

$$\varphi_{\mathrm{an}}(R\Gamma) = R\varphi_{\mathrm{an}}(\Gamma) = R\bigoplus_i \Lambda_i = \bigoplus_i \Lambda_i = \varphi_{\mathrm{an}}(\Gamma)$$

so $R\Gamma = \Gamma$. Moreover, the isomorphism φ endows Γ with a structure of an R-module in a natural way

$$r.\gamma = \varphi_{\mathrm{an}}^{-1}(r\varphi_{\mathrm{an}}(\gamma)) = r\gamma, \text{ for } r \in R, \gamma \in \Gamma. \tag{1}$$

Hence Γ has a structure of R-module and we can see in (1) that this structure does not depend on the isomorphism φ we chose.

Conversely, let L be an R-lattice and $(\mathfrak{a}_i, x_i)$ a pseudo-basis of it. Since the $\mathfrak{a}_i$ are fractional ideals, there exists an integer n such that $n\mathfrak{a}_i \subset R$ for all i, so the multiplication by n map defines an isogeny $\mathrm{Hom}_{\mathbb{C}}(L, R^g)$. If we endow R^g with the canonical hermitian form $h_0(x, y) = {}^t x\overline{y}$, we have $h_0(R^g, R^g) = R$, hence

$$\mathrm{im}\, h_0(R^g, R^g) = (\mathrm{im}\, \omega)\mathbb{Z} = \alpha_R\mathbb{Z}.$$

Thus, $\left(R^g, \frac{1}{\alpha_R}h_0\right)$ defines a polarized torus and so does $\left(L, \frac{n^2}{\alpha_R}h_0\right)$. This proves that the underlying $\mathbb{Z}$-lattice Γ of an R-lattice L is polarizable.

Finally, given a morphism $f\colon V/\Gamma \to V'/\Gamma'$, $\mathbf{F}(f) = f_{\mathrm{rat}}\colon \Gamma \to \Gamma'$. Since $f_{\mathrm{rat}} = f_{\mathrm{an}|\Gamma}$ and f_{an} is $\mathbb{C}$-linear it is then R-linear. Hence $\mathbf{F}$ maps arrows in a full and faithful way.

Hence there is an equivalence of categories between R-lattices and polarizable tori X such that there exists an isomorphism $X \to \mathbb{C}^g/\bigoplus \Lambda_i$. The latter being in equivalence with the category of abelian varieties isomorphic to a power of elliptic curves with CM by R. This proves the equivalence of categories between $\boldsymbol{\mathcal{A}}_R$ and $\boldsymbol{\mathcal{L}}_R$. □

It may be worth elaborating why the CM case is so special. If we consider the functor $\mathbf{F}$ from abelian varieties over $\mathbb{C}$ without restriction to the category of $\mathbb{Z}$-lattices of a finite dimensional $\mathbb{C}$-vector space then $\mathbf{F}$ is not essentially surjective. Indeed, some $\mathbb{Z}$-lattices Γ of V of dimension greater than 2 are not polarizable. Even if we restrict $\mathbf{F}$ on its essential image it is not full. Indeed, even in dimension 1 there are morphisms

of polarizable $\mathbb{Z}$-lattices (i.e., morphisms of groups) which are not the restriction of a $\mathbb{C}$-linear map.

Hence the structure of a $\mathbb{Z}$-module is not enough. Fortunately, considering the R-module structure given by the complex multiplication makes $\mathbf{F}$ an equivalence.

2.3 Polarizable tori and integral lattices

A *hermitian R-lattice* is defined as a pair (L, H) with L an R-lattice and H a positive definite hermitian form on the ambient space KL. The *scale* of a hermitian lattice (L, H) is defined as the set $\mathfrak{s}(L) = H(L, L) \subset K$. It is a fractional ideal of K (see [14, Remark 2.3.4]). The *dual lattice* $L^\#$ of a hermitian lattice is the lattice defined by $L^\# = \{v \in KL \mid H(v, L) \subset R\}$. For $\mathfrak{a}$ a fractional ideal of K, we say that (L, H) is $\mathfrak{a}$-*modular* if $\mathfrak{a}L^\# = L$. If (L, H) is $\mathfrak{a}$-modular then its scale satisfies $\mathfrak{s}(L) = \mathfrak{a}$. A hermitian R-lattice (L, H) is said to be *integral* if

$$H(L, L) \subset R,$$

i.e., it is integral if its scale is an integral ideal (or equivalently $L \subset L^\#$). An R-modular hermitian lattice (L, H) is called unimodular (this is equivalent to (L, H) being integral and its scale being $\mathfrak{s}(L) = R$). One also defines the *volume* of a hermitian lattice (L, H) as the fractional ideal

$$\mathfrak{v}(L) = \left(\prod_{i=1}^{g} N(\mathfrak{a}_i)\right) \det(G(x_1, \ldots, x_g))R$$

where $G(x_1, \ldots, x_g) = (H(x_i, x_j))_{1 \leqslant i,j \leqslant g}$, the Gram matrix of $(x_1, \ldots, x_g)$. A hermitian lattice (L, H) is $\mathfrak{a}$-modular if, and only if,

$$\mathfrak{v}(L) = \mathfrak{a}^g \text{ and } \mathfrak{s}(L) = \mathfrak{a}$$

(see [10, Section 2]).

In this section, we explain the link between polarized tori and integral lattices.

Let (V, H) be a hermitian $\mathbb{C}$-vector space and let $\alpha \in \mathbb{R}_{>0}$. We denote by V^α the vector space V provided with the hermitian form $H^\alpha(x, y) = \alpha H(x, y)$. For a lattice L in (V, H) we denote by L^α the hermitian lattice L regarded in the hermitian space (V^α, H^α) as in [22, Section 82J.].

Lemma 2.2. *Let $R = \mathbb{Z}[\omega]$ be an order of an imaginary quadratic field and $\mathfrak{a}$ be a sub-R-module in $\mathbb{C}$. Then $\mathfrak{a}$ is an integral ideal in R if, and only if,* $\operatorname{im}\mathfrak{a} \subset \alpha_R\mathbb{Z}$ *with* $\alpha_R = \operatorname{im}(\omega)$.

Proof. The left-to-right direction is straightforward.

Let $a = x + y\omega \in \mathfrak{a}$ with $x, y \in \mathbb{R}$. Since $\operatorname{im} a = y\alpha_R \in \alpha_R\mathbb{Z}$ we have $y \in \mathbb{Z}$. Moreover, $\overline{\omega} \in R$ so $a\overline{\omega} \in \mathfrak{a}$ and $\operatorname{im} a\overline{\omega} = -x\alpha_R$ so $x \in \mathbb{Z}$. Hence $a \in R$ and therefore $\mathfrak{a} \subset R$. □

Proposition 2.3. *Let $(V/\Gamma, \rho_h)$ be a polarized torus such that $\Gamma \simeq \bigoplus_{i=1}^{g} \Lambda_i$ with $End_{\mathbb{C}}(\Lambda_i) \simeq R$ with $R = \mathbb{Z}[\omega]$. Then $\mathfrak{s}(\Gamma^{\alpha_R})$ is an integral ideal of R. Moreover, we have the equality*

$$\deg \rho_h = \left[(\Gamma^{\alpha_R})^\# \colon \Gamma^{\alpha_R}\right].$$

Proof. We know that $h(\Gamma,\Gamma)$ is a R-module in $\mathbb{C}$ and since (Γ, h) is a polarizable torus we must have $\operatorname{im} h(\Gamma,\Gamma) \subset \mathbb{Z}$. Hence by Lemma 2.2, we have $\mathfrak{s}(\Gamma^{\alpha_R}) = \alpha_R h(\Gamma,\Gamma) \subset R$. Moreover,

$$\begin{aligned}
\deg \rho_h &= \left[\widehat{\Gamma} \colon \rho_h(\Gamma)\right] \\
&= \left[\rho_h^{-1}(\widehat{\Gamma}) \colon \Gamma\right] \\
&= \#\left\{v \in V \mid \operatorname{im} h(v,\Gamma) \subset \mathbb{Z}\right\}/\Gamma \\
&= \#\left\{v \in V \mid (\operatorname{im}\omega) h(v,\Gamma) \subset R\right\}/\Gamma \qquad \text{(by Lemma 2.2)} \\
&= \#\left((\Gamma^{\alpha_R})^{\#}/\Gamma\right) \\
&= \left[(\Gamma^{\alpha_R})^{\#} \colon \Gamma^{\alpha_R}\right].
\end{aligned}$$

□

Let $\Lambda \subset \mathbb{C}$ be a lattice such that $\operatorname{End}(\Lambda) = R$. We define $\mathcal{T}_R^p$ the subcategory of polarized tori $(X = V/\Gamma, \rho_h)$, with $\Gamma \simeq \bigoplus \Lambda_i$ and $\operatorname{End}(\Lambda_i) \simeq R$. We conclude the section with the following theorem.

Theorem 2.4. *With the notation above, there is an equivalence of categories given on objects by*

$$\begin{aligned}
\mathcal{T}_R^p &\longrightarrow \mathcal{L}_R^{h,int} \\
(X = V/\Gamma, \rho_h) &\longmapsto (\Gamma^{\alpha_R}, h^{\alpha_R}) \\
\left((\mathbb{C}L)/L, H^{1/\alpha_R}\right) &\longleftarrow\!\shortmid (L, H).
\end{aligned}$$

Since $\mathcal{T}_R^p$ is equivalent to the category $\mathcal{A}_R^p$ via the functor $\mathbf{T}$, we have the equivalence between $\mathcal{A}_R^p$ and $\mathcal{L}_R^{h,int}$. We call this functor $\mathbf{F}_h$ and note that it satisfies

$$\mathbf{F}_h \colon \begin{cases} \mathcal{A}_R^p \longrightarrow \mathcal{L}_R^{h,int} \\ (A,a) \longmapsto \left(\mathbf{F}(A)^{\alpha_R}, \mathbf{F}(a)^{\alpha_R}\right). \end{cases}$$

Since every elliptic curve over $\mathbb{C}$ with CM has a model over $\overline{\mathbb{Q}}$, the category of polarized abelian varieties over $\overline{\mathbb{Q}}$ isomorphic to a product of elliptic curves E_i with CM by R is equivalent to $\mathcal{A}_R^p$ by the base change functor

$$A \mapsto A_{\mathbb{C}}.$$

Note that morphisms over $\mathbb{C}$ of abelian varieties over $\overline{\mathbb{Q}}$ isomorphic to a product of CM elliptic curves are actually defined over $\overline{\mathbb{Q}}$ by [24, Theorem 2.2.(c)].

3 Action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

The *field of moduli* of a polarized abelian variety (A, a) over $\overline{\mathbb{Q}}$ is the field fixed by the subgroup

$$\left\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid (A^\sigma, a^\sigma) \simeq (A, a)\right\}.$$

Given a maximal order in an imaginary quadratic field K, we would like to construct an algorithm to enumerate all the isomorphism classes of $\mathcal{A}_R^p$ which have field of moduli $\mathbb{Q}$. In order to do this, we first need to understand the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the hermitian lattices through the functor $\mathbf{F}_h$ described in Section 2. In other words, given $(A, a) \in \mathcal{A}_R^p$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we want to understand the isometry class of $\mathbf{F}_h(A^\sigma, a^\sigma)$ in terms of $\mathbf{F}_h(A, a)$ and σ.

In order to do so, we need to understand the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and the action of $\mathrm{Gal}(K/\mathbb{Q})$, by complex conjugation, separately in order to recover the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \simeq \mathrm{Gal}(\overline{\mathbb{Q}}/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$. We describe the action of $\mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ in Theorem 3.1 and Theorem 3.2 respectively. The end of this section is devoted to their proofs.

Let us first introduce the necessary notation.

Let (L, H) be a hermitian lattice. Let $\iota\colon (KL, H) \to (K^g, H')$ be an isometry. We define $(\overline{L}, \overline{H})$ by $\overline{L} = \iota^{-1}\overline{\iota(L)}$ and

$$\overline{H}(x, y) = \overline{H(\iota^{-1}\overline{\iota(x)}, \iota^{-1}\overline{\iota(y)})} = \overline{H'(\overline{\iota(x)}, \overline{\iota(y)})}$$

where $\bar{\cdot}$ refers to the complex conjugation which is the unique non-trivial automorphism of $\mathrm{Gal}(K/\mathbb{Q})$. The isometry class of $(\overline{L}, \overline{H})$ is independent of the choice of ι. We can now describe the action of the complex conjugation.

Theorem 3.1 (Description of the action of $\mathrm{Gal}(K/\mathbb{Q})$)**.** *Let $(A, a) \in \mathcal{A}_R^p$ considered over $\overline{\mathbb{Q}}$ and let $\mathbf{F}_h(A, a) = (L, H)$. Then there is an isometry*

$$\mathbf{F}_h\left(\overline{A}, \overline{a}\right) \simeq \left(\overline{L}, \overline{H}\right).$$

Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by R. Let $\Lambda \subset \mathbb{C}$ be a lattice such that $E_{\mathbb{C}} \simeq E_\Lambda$. We will often abuse notation slightly and also denote by E the base change $E_{\mathbb{C}}$ of E, to avoid heavy notation such as $E_{\mathbb{C}}(\mathbb{C})$. Recall that for $\dot{\mathfrak{a}} \in \mathrm{Cl}(R)$, the elliptic curve $\dot{\mathfrak{a}} \star E_\Lambda$ is defined by $E_{\mathfrak{a}^{-1}\Lambda}$. By [24, Proposition 2.4], there is a surjective group morphism

$$F\colon \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{Cl}(R) \tag{2}$$

such that the elliptic curves E^σ and $F(\sigma) \star E$ are isomorphic. We can now state the description of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$.

Theorem 3.2 (Description of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$)**.** *Let $(A, a) \in \mathcal{A}_R^p$ considered over $\overline{\mathbb{Q}}$. Let $\mathbf{F}_h(A, a) = (L, H), \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and let $F(\sigma) = \dot{\mathfrak{a}}^{-1} \in \mathrm{Cl}(R)$. Then there is an isometry*

$$\mathbf{F}_h(A^\sigma, a^\sigma) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})}H\right),$$

where $N(\mathfrak{a})$ is the norm of $\mathfrak{a}$.

3.1 Positioning of the problem

Let us recall from Section 2.1 that for every elliptic curve with CM by R and any isomorphism $\eta\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ there is a unique isomorphism $[\cdot]_E\colon R \to \mathrm{End}(E)$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\alpha} & \mathbb{C}/\Lambda \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta} \\ E_\Lambda(\mathbb{C}) & \xrightarrow{[\alpha]} & E_\Lambda(\mathbb{C}) \end{array}$$

By [24, Theorem 2.2] the bracket isomorphism satisfies

$$([\alpha]_E)^\sigma = [\alpha^\sigma]_{E^\sigma} \text{ for all } \sigma \in \mathrm{Aut}(\mathbb{C}), \alpha \in R.$$

This is true for any Λ and $\eta\colon \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ we choose and for any lattice identification $\eta_\sigma\colon \mathbb{C}/\Lambda_\sigma \xrightarrow{\sim} E^\sigma(\mathbb{C})$ of E^σ as long as we choose the same η_σ on both sides of the diagram. Of course if we do not take the same isomorphisms on both sides of the diagram, for instance we chose η and $-\eta$, this property does not hold anymore. The main difficulty we will encounter is that we want to deal with isogenies $f\colon E \to E'$ between possibly non-isomorphic elliptic curves. If we expect diagrams like

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\alpha} & \mathbb{C}/\Lambda' \\ {\scriptstyle\eta}\downarrow & & \downarrow{\scriptstyle\eta'} \\ E(\mathbb{C}) & \xrightarrow{f} & E'(\mathbb{C}) \end{array}$$

to have a nice behavior with respect to $\mathrm{Aut}(\mathbb{C})$ or $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we need a kind of canonical way of describing the action of $\mathrm{Aut}(\mathbb{C})$ (or $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) on lattices, and a canonical way of choosing the isomorphisms η (to avoid the $-\eta$ issue for instance). We will show that the $\wp$-function of Weierstrass will do the job.

First we need to specify the isomorphisms we refer to when we consider the analytic representation of a morphism between abelian varieties. Let A and A' be abelian varieties over $\mathbb{C}$. Consider isomorphisms $\eta\colon V/\Gamma \xrightarrow{\sim} A(\mathbb{C})$ and $\eta'\colon V'/\Lambda' \xrightarrow{\sim} A'(\mathbb{C})$. Every morphism $f\colon A \to A'$ induces a morphism φ such that the diagram in Figure 2 commutes. The morphism φ of tori can be lifted to a linear map $\beta\colon V \to V'$ such that $\beta(\Gamma) \subset \Gamma'$. We call β the analytic representation of f associated with the isomorphisms η and η' or simply the analytic representation of (f, η, η').

We will use the Weierstrass $\wp$-function and Eisenstein series as in [25] as a canonical way of identifying an elliptic curve over $\mathbb{C}$ with a complex torus and we will study the field of definition of the induced analytic representation of isogenies between CM elliptic curves in Section 3.2. Then we will extend the results for elliptic curves to product of elliptic curves, component by component, in Section 3.3 and finally prove Theorem 3.1 and 3.2.

$$\begin{array}{ccc} V/\Gamma & \xrightarrow{\varphi} & V'/\Gamma' \\ \eta \downarrow & & \downarrow \eta' \\ A(\mathbb{C}) & \xrightarrow{f} & A'(\mathbb{C}) \end{array}$$

Figure 2: Analytic representation of an isogeny

3.2 Action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on CM elliptic curves

3.2.1 Fixing isomorphisms with the Weierstrass $\wp$-function

By [25, Therorem 5.1], for any $A, B \in \mathbb{C}$ such that $4A^3 - 27B^2 \neq 0$, there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that

$$A = g_2(\Lambda) = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4} \quad \text{and} \quad B = g_3(\Lambda) = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$$

where $g_2(\Lambda)$ and $g_3(\Lambda)$ are Eisenstein series of weight 4 and 6 of Λ, respectively. Let $E/\mathbb{C}$ be the elliptic curve defined by the Weierstrass model $E\colon y^2 = 4x^3 - Ax - B$. According to [25, Proposition 3.6] there is an isomorphism of Lie groups

$$\phi_\Lambda\colon \begin{cases} \mathbb{C}/\Lambda \longrightarrow E_\Lambda(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}) \\ \quad z \longmapsto [\wp(z,\Lambda)\colon \wp'(z,\Lambda)\colon 1] \end{cases} \tag{3}$$

with $\wp$ the Weierstrass $\wp$-function. Moreover, by [25, VI.5.1], every elliptic curve E over $\mathbb{C}$ is isomorphic to some E_Λ via ϕ_Λ.

From now on, the notation E_Λ means that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ with the isomorphism given by ϕ_Λ.

Let $\kappa \hookrightarrow \mathbb{C}$ be a field extension and $E\colon y^2 = 4x^3 - Ax - B$ with $A, B \in \kappa$ and let Λ be a lattice such that $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$. For every $\sigma \in \mathrm{Aut}(\kappa)$ we define Λ_σ as the unique lattice such that $g_2(\Lambda_\sigma) = A^\sigma$ and $g_3(\Lambda_\sigma) = B^\sigma$.

By definition of Λ_σ we have an isomorphism $\phi_{\Lambda_\sigma}\colon \mathbb{C}/\Lambda_\sigma \to E^\sigma(\mathbb{C})$ with $E^\sigma\colon y^2 = 4x^3 - A^\sigma x - B^\sigma$.

Lemma 3.3. *For any lattice $\Lambda \subset \mathbb{C}$, we have $\Lambda_{\bar{\cdot}} = \overline{\Lambda}$.*

Proof. The Eisenstein series $g_2(\Lambda)$ and $g_3(\Lambda)$ are absolutely convergent and the complex conjugation is an antilinear map so $g_k(\overline{\Lambda}) = \overline{g_k(\Lambda)}$. □

3.2.2 Algebraicity of analytic representations for CM elliptic curves

The results here are simple consequences of the chapter of [24, Chapter II]. We simply state them in a form which will be adapted to our formalism later. Let E, E' be two elliptic curves over $\overline{\mathbb{Q}}$ by Weierstrass models. By [24, Theorem 2.2.(c)] an isogeny $f\colon E \to E'$ is

also defined over $\overline{\mathbb{Q}}$. In this section, we want to study the analytic representation α of $(f, \phi_\Lambda, \phi_{\Lambda'})$ when E and E' have Weierstrass models over $\overline{\mathbb{Q}}$, with $\phi_\Lambda \colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ and $\phi_{\Lambda'} \colon \mathbb{C}/\Lambda' \to E'(\mathbb{C})$ as defined in (3). In particular, we wish to know:

- Is α in $\overline{\mathbb{Q}}$?
- If $\alpha \in \overline{\mathbb{Q}}$, does α behave well with $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, i.e., is α^σ the analytic representation of $(f^\sigma, \phi_{\Lambda_\sigma}, \phi_{\Lambda'_\sigma})$?

We will positively answer these questions in Proposition 3.6. This is partially addressed in [24, Chapter II], but we require greater precision and control over the analytic representations than the author does for the purposes of his book. Therefore, we will elaborate on this in the current section.

Lemma 3.4. *Let $\Lambda \subset \mathbb{C}$ be a lattice and $E \colon y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ be the elliptic curve over $\mathbb{C}$ associated with Λ by ϕ_Λ. Let $r \in \mathbb{C} \setminus \{0\}$, let E' be the elliptic curve associated with $r\Lambda$ and let ν_r be the map defined by*

$$\nu_r \colon \begin{cases} \mathbb{P}^2(\mathbb{C}) \longrightarrow \mathbb{P}^2(\mathbb{C}) \\ [x \colon y \colon 1] \longmapsto [\frac{1}{r^2}x \colon \frac{1}{r^3}y \colon 1]. \end{cases}$$

Then the restriction of ν_r to $E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$ defines an isomorphism on its image $E'(\mathbb{C})$. Moreover, r is the analytic representation of $(\nu_{r\,|E(\mathbb{C})}, \phi_\Lambda, \phi_{r\Lambda})$.

Proof. For all $z \in \mathbb{C} \setminus r\Lambda, r \in \mathbb{C} \setminus \{0\}$, $\wp(z, r\Lambda) = \frac{1}{r^2}\wp(\frac{z}{r}, \Lambda)$ and $\wp'(z, r\Lambda) = \frac{1}{r^3}\wp'(\frac{z}{r}, \Lambda)$. Hence

$$\begin{aligned} \phi_{r\Lambda}(z) &= [\wp(z, r\Lambda) \colon \wp'(z, r\Lambda) \colon 1] \\ &= [\frac{1}{r^2}\wp\left(\frac{z}{r}, \Lambda\right) \colon \frac{1}{r^3}\wp'\left(\frac{z}{r}, \Lambda\right) \colon 1] \\ &= \nu_r\left(\phi_\Lambda\left(\frac{z}{r}\right)\right). \end{aligned}$$

This proves that the following diagram commutes

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{r} & \mathbb{C}/r\Lambda \\ {\scriptstyle \phi_\Lambda}\downarrow & & \downarrow{\scriptstyle \phi_{r\Lambda}} \\ E(\mathbb{C}) & \xrightarrow{\nu_{r\,|E(\mathbb{C})}} & E'(\mathbb{C}) \end{array}$$

which shows that $(\nu_{r\,|E(\mathbb{C})}, \phi_\Lambda, \phi_{r\Lambda})$ has analytic representation r. □

Let $\mathfrak{a}$ be a fractional ideal of R, and let Λ be an R-lattice such that $E = E_\Lambda \in \boldsymbol{\mathcal{A}}_R$. We defined $\mathfrak{a} \star E$ earlier as the isomorphism class of $E_{\mathfrak{a}^{-1}\Lambda}$.

From now on, we will refer to $\mathfrak{a} \star E$ as the elliptic curve defined by the Weierstrass equation

$$\mathfrak{a} \star E \colon y^2 = 4x^3 - g_2(\mathfrak{a}^{-1}\Lambda)x - g_3(\mathfrak{a}^{-1}\Lambda).$$

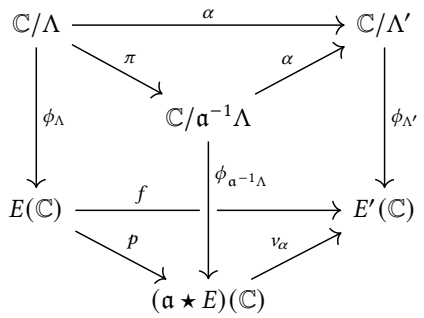

Figure 3: Factorization of isogenies

Let $f\colon E \to E'$ be an isogeny between elliptic curves with CM by R with $E' = E_{\Lambda'}$. Let $\mathfrak{a}$ be the integral ideal of R such that $\ker f = E[\mathfrak{a}] = \cap_{a\in\mathfrak{a}} \ker[a]_E$. According to [24, Proposition 1.4], $\mathfrak{a}\star E \simeq E/E[\mathfrak{a}]$ and we can factor $f\colon E \to E'$ and $\alpha\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ as in Figure 3 where $\pi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda$ is the natural projections and $p\colon E \to \mathfrak{a}\star E$ induced by π.

Lemma 3.5. *Let Λ be a lattice with complex multiplication such that $g_k(\Lambda) \in \overline{\mathbb{Q}}$ for $k = 2, 3$. Then for any fractional ideal we have $\mathfrak{a} \subset K, g_k(\mathfrak{a}^{-1}\Lambda) \in \overline{\mathbb{Q}}$.*

Proof. Let $E\colon y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ be defined over $\overline{\mathbb{Q}}$. Since all CM elliptic curves have a model over $\overline{\mathbb{Q}}$ we consider $E'\colon y^2 = 4x^3 - A'x - B'$, a model of $\mathfrak{a}\star E$ over $\overline{\mathbb{Q}}$ and Λ' such that $E' = E_{\Lambda'}$. Consider any isogeny $f\colon E \to E'$ over $\overline{\mathbb{Q}}$ and $\alpha \in \mathbb{C}$ the analytic representation of $(f, \phi_\Lambda, \phi_{\Lambda'})$. Let $r \in \overline{\mathbb{Q}}$ be the coefficient of the induced map on differentials $f^*\frac{dx'}{y'} = r\frac{dx}{y}$. By the proof of [25, Proposition 3.6.(b)] we have $\phi_\Lambda^*\left(\frac{dx}{y}\right) = dz$. Thus,

$$(f\circ\phi_\Lambda)^*\left(\frac{dx'}{y'}\right) = \phi_\Lambda^*\circ f^*\left(\frac{dx'}{y'}\right) = \phi_\Lambda^*\left(r\frac{dx}{y}\right) = rdz$$

and

$$(\phi_{\Lambda'}\circ\alpha)^*\left(\frac{dx'}{y'}\right) = \alpha dz' = \alpha dz.$$

Since the following diagram commutes

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\alpha} & \mathbb{C}/\Lambda' \\ {\scriptstyle\phi_\Lambda}\downarrow & & \downarrow{\scriptstyle\phi_{\Lambda'}} \\ E(\mathbb{C}) & \xrightarrow{f} & E'(\mathbb{C}) \end{array}$$

we have equality of the differentials $rdz = \alpha dz$. Hence $r = \alpha \in \overline{\mathbb{Q}}$. Let $\mathfrak{b}$ be the integral ideal such that $\ker f = E[\mathfrak{b}]$. By Figure 3 we have $\Lambda' = \alpha\mathfrak{b}^{-1}\Lambda$ so, for $k \in \{2, 3\}$, $g_k(\mathfrak{b}^{-1}\Lambda) = \alpha^{2k}g_k(\Lambda') \in \overline{\mathbb{Q}}$. Finally, $\mathfrak{b}^{-1}\Lambda$ and $\mathfrak{a}^{-1}\Lambda$ give isomorphic

elliptic curves so they must be homothetic by some $\lambda \in \mathrm{Hom}_{\mathbb{C}}(\mathfrak{b}^{-1}\Lambda, \mathfrak{a}^{-1}\Lambda) = \left\{\mu \in \mathbb{C} \mid \mu\mathfrak{b}^{-1}\Lambda \subset \mathfrak{a}^{-1}\Lambda\right\} \subset K$. Hence

$$g_k(\mathfrak{a}^{-1}\Lambda) = \lambda^{-2k} g_k(\mathfrak{b}^{-1}\Lambda) \in \overline{\mathbb{Q}}.$$

□

Proposition 3.6. *Let $E\colon y^2 = 4x^3 - Ax - B$ over $\overline{\mathbb{Q}}$ and $E'\colon y^2 = 4x^3 - A'x - B'$ over $\mathbb{C}$ be elliptic curves both with CM by R. Let Λ and Λ' be lattices with $g_2(\Lambda) = A, g_3(\Lambda) = B, g_2(\Lambda') = A'$ and $g_3(\Lambda') = B'$. Let $f\colon E \to E'$ be an isogeny over $\mathbb{C}$. Consider $\alpha \in \mathbb{C}$ the analytic representation of $(f, \phi_\Lambda, \phi_{\Lambda'})$. Then*

1. *$\alpha \in \overline{\mathbb{Q}}$ if, and only if, $g_2(\Lambda') \in \overline{\mathbb{Q}}$ and $g_3(\Lambda') \in \overline{\mathbb{Q}}$.*
2. *If 1. is satisfied then, for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, α^σ is the analytic representation of $(f^\sigma, \phi_{\Lambda_\sigma}, \phi_{\Lambda'_\sigma})$ with f identified with the induced map over $\overline{\mathbb{Q}}$.*
3. *For every fractional ideal $\mathfrak{a}$ and for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have $(\mathfrak{a}\Lambda)_\sigma = \mathfrak{a}^\sigma\Lambda_\sigma$.*

Proof. 1. Since $\Lambda' = \alpha\mathfrak{a}^{-1}\Lambda$ we have $g_k(\Lambda') = \alpha^{-2k} g_k(\mathfrak{a}^{-1}\Lambda)$. By Lemma 3.5, $g_k(\mathfrak{a}^{-1}\Lambda) \in \overline{\mathbb{Q}}$ so $\alpha \in \overline{\mathbb{Q}}$ if, and only if, $g_k(\Lambda') \in \overline{\mathbb{Q}}$.

2. We define α_σ the analytic representation of $(f^\sigma, \phi_{\Lambda_\sigma}, \phi_{\Lambda'_\sigma})$. We want to show that $\alpha_\sigma = \alpha^\sigma$. Since Λ_σ and Λ'_σ are such that $g_i(\Lambda_\sigma) \in \overline{\mathbb{Q}}$ and $g_i(\Lambda'_\sigma) \in \overline{\mathbb{Q}}$, by 1. $\alpha_\sigma \in \overline{\mathbb{Q}}$. According to [24, Theorem 2.2],

$$\ker(f^\sigma) = (\ker f)^\sigma = \cap_{a\in\mathfrak{a}}(\ker[a]_E)^\sigma = \cap_{a\in\mathfrak{a}} \ker[a^\sigma]_{E^\sigma} = E^\sigma[\mathfrak{a}^\sigma]. \tag{4}$$

Since $f^\sigma = \left(\nu_{\alpha_{|(\mathfrak{a}\star E)(\overline{\mathbb{Q}})}}\right)^\sigma \circ p^\sigma$ and $\left(\nu_{\alpha_{|(\mathfrak{a}\star E)(\overline{\mathbb{Q}})}}\right)^\sigma$ is an isomorphism, $\ker f^\sigma = \ker p^\sigma$. By definition of $E[\mathfrak{a}]$ we have

$$[\wp(z,\Lambda)\colon \wp'(z,\Lambda)\colon 1] \in E[\mathfrak{a}] \text{ if, and only if, } z \in \mathfrak{a}^{-1}\Lambda. \tag{5}$$

Moreover, $[\wp(z,\Lambda_\sigma)\colon \wp(z,\Lambda_\sigma)\colon 1] \in \ker p^\sigma$ if, and only if, $z \in (\mathfrak{a}^{-1}\Lambda)_\sigma$ by definition of p^σ but, $z \in (\mathfrak{a}^\sigma)^{-1}\Lambda_\sigma$ because $\ker p^\sigma = E^\sigma[\mathfrak{a}^\sigma]$. Thus, by the relations (4) and (5), we have $(\mathfrak{a}^{-1}\Lambda)_\sigma = (\mathfrak{a}^\sigma)^{-1}\Lambda_\sigma$ (this proves the point 3 of the proposition). This proves that $(\mathfrak{a}\star E)^\sigma = \mathfrak{a}^\sigma \star E^\sigma$. We also have the factorization

$$f^\sigma = \left(\nu_{\alpha_{|(\mathfrak{a}\star E)(\overline{\mathbb{Q}})}}\right)^\sigma \circ p^\sigma = \nu_{\alpha_\sigma|(\mathfrak{a}^\sigma\star E^\sigma)(\overline{\mathbb{Q}})} \circ p^\sigma.$$

Since p^σ is an isogeny it is surjective. So the maps $(\nu_{\alpha_{|\mathbb{P}^2(\overline{\mathbb{Q}})}})^\sigma$ and $\nu_{\alpha_\sigma|\mathbb{P}^2(\overline{\mathbb{Q}})}$ coincide and then

$$\frac{1}{\alpha_\sigma^2} = \frac{1}{(\alpha^\sigma)^2} \text{ so } \alpha_\sigma = \pm\alpha^\sigma \text{ and } \frac{1}{\alpha_\sigma^3} = \frac{1}{(\alpha^\sigma)^3} \text{ so } \alpha_\sigma = j\alpha^\sigma$$

for some $j^3 = 1$. Hence $\alpha_\sigma = \alpha^\sigma$.

□

A nice consequence is that if we take E_Λ with $g_2(\Lambda) \in \overline{\mathbb{Q}}$ and $g_3(\Lambda) \in \overline{\mathbb{Q}}$ then $E_{\mathfrak{a}^{-1}\Lambda}$ has also its Weierstrass model over $\overline{\mathbb{Q}}$ and $\mathrm{Hom}_{\mathbb{C}}(E_\Lambda, E_{\mathfrak{a}^{-1}\Lambda}) = \mathrm{Hom}_{\overline{\mathbb{Q}}}(E_\Lambda, E_{\mathfrak{a}^{-1}\Lambda})$ so the analytic representations of these isogenies associated with the isomorphisms ϕ_Λ and $\phi_{\mathfrak{a}^{-1}\Lambda}$ are in $\mathrm{Hom}_{\mathbb{C}}(\Lambda, \mathfrak{a}^{-1}\Lambda) \subset K$. We recall from [24, Proposition 1.2] that $\mathrm{Cl}(R)$ acts simply transitively on the elliptic curves with CM by R. Thus, given two elliptic curves E and E' over $\overline{\mathbb{Q}}$ we can always find a model E'' of E' such that the analytic representations of isogenies from E to E'' are in K.

Given an automorphism $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $F(\sigma) = \dot{\mathfrak{a}}$, with F defined in (1), by [24, Proposition 2.4] we know that E^σ and $\mathfrak{a} \star E$ are isomorphic. This means that their corresponding lattices Λ_σ and $\mathfrak{a}^{-1}\Lambda$ (via the $\wp$-function) are homothetic by some constant $r_\sigma \in \mathbb{C}$ which depends, a priori, on Λ, σ and the choice of the representative $\mathfrak{a}$ of $F(\sigma)$ we chose. An immediate consequence of Proposition 3.6 is that r_σ is in $\overline{\mathbb{Q}}$. The issue is that choosing another lattice Λ' could lead to another $r'_\sigma \in \overline{\mathbb{Q}}$ such that $r'_\sigma \Lambda'_\sigma = \mathfrak{a}^{-1}\Lambda'$. The next proposition shows that, under some condition, we can choose the same r_σ for different lattices.

Proposition 3.7 (Action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ on elliptic curves)**.** *Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ be an automorphism and $\mathfrak{a}$ be a fractional ideal with $F(\sigma) = \dot{\mathfrak{a}} \in \mathrm{Cl}(R)$. Consider an elliptic curve E_Λ over $\overline{\mathbb{Q}}$. Then there exists $r_\sigma \in \overline{\mathbb{Q}}$ such that for all $E'(\mathbb{C}) \underset{\phi_{\Lambda'}}{\simeq} \mathbb{C}/\Lambda'$ such that* $\mathrm{Hom}_{\mathbb{C}}(\Lambda, \Lambda') \subset K$ *and all isogenies $f : E_\Lambda \to E_{\Lambda'}$ over $\overline{\mathbb{Q}}$ we have a commutative diagram*

$$\begin{array}{ccc}
E^\sigma(\mathbb{C}) & \xrightarrow{f^\sigma} & E'^\sigma(\mathbb{C}) \\
\uparrow{\scriptstyle \phi_{\Lambda_\sigma}} & & \uparrow{\scriptstyle \phi_{\Lambda'_\sigma}} \\
\mathbb{C}/\Lambda_\sigma & \xrightarrow{\alpha} & \mathbb{C}/\Lambda'_\sigma \\
\downarrow{\scriptstyle r_\sigma} & & \downarrow{\scriptstyle r_\sigma} \\
\mathbb{C}/\mathfrak{a}^{-1}\Lambda & \xrightarrow{\alpha} & \mathbb{C}/\mathfrak{a}^{-1}\Lambda'
\end{array}$$

where $\alpha \in K$ is the analytic representation of $(f, \phi_\Lambda, \phi_{\Lambda'})$.

Proof. Since the group of fractional ideals acts transitively on CM elliptic curves over $\overline{\mathbb{Q}}$ there exists an isomorphism $E^\sigma \to \mathfrak{a} \star E$ which induces an isomorphism on the associated tori $r_\sigma : \mathbb{C}/\Lambda_\sigma \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda$. Let $\alpha \in K$ be the analytic representation of $(f, \phi_\Lambda, \phi_{\Lambda'})$. There exists an ideal $\mathfrak{b} \subset R$ such that $\alpha\Lambda = \mathfrak{b}^{-1}\Lambda'$ and Proposition 3.6.3 implies that $\alpha^\sigma \Lambda_\sigma = (\mathfrak{b}^{-1})^\sigma \Lambda'_\sigma$. Since $\alpha \in K$ and $\mathfrak{b} \subset K$ they are invariant by σ. To prove the proposition, we need to show that $r_\sigma \Lambda'_\sigma = \mathfrak{a}^{-1}\Lambda'$.

On one hand, we have

$$\alpha\Lambda_\sigma = \mathfrak{b}^{-1}\Lambda'_\sigma, \tag{6}$$

on the other hand

$$\alpha\mathfrak{a}^{-1}\Lambda = \mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda'. \tag{7}$$

Combined with $r_\sigma \Lambda_\sigma = \mathfrak{a}^{-1}\Lambda$, (6) and (7), it gives

$$\begin{aligned} r_\sigma \Lambda'_\sigma &= \mathfrak{b}\alpha\mathfrak{a}^{-1}\Lambda \\ &= \mathfrak{b}\mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda' \\ &= \mathfrak{a}^{-1}\Lambda' \end{aligned}$$

which concludes the proof. □

3.2.3 Galois action on polarizations of CM elliptic curves

The canonical polarization on an elliptic curve E is defined by

$$a_{0,E}\colon \begin{cases} E \longrightarrow \widehat{E} \\ P \longmapsto [P] - [O] \end{cases}$$

with O the neutral element of the group E. We use this isomorphism to identify any polarization a of E with an element of $\mathrm{End}(E)$ by $a_{0,E}^{-1} \circ a$.

Lemma 3.8. *Let $\mathfrak{a} \subset K$ be a fractional R-ideal and let $x \in \mathbb{C}$. Let $E(\mathbb{C}) \underset{\phi_\Lambda}{\simeq} \mathbb{C}/\Lambda$ be the elliptic curve associated with the lattice $\Lambda = \mathfrak{a}x$. The principal polarization $a_{0,E}$ induces the hermitian form*

$$h_{0,\Lambda}\colon \begin{cases} \mathbb{C}\times\mathbb{C} \longrightarrow \mathbb{C} \\ (z,w) \longmapsto \frac{z\overline{w}}{\alpha_R N(\mathfrak{a}) N(x)} \end{cases}$$

with $\alpha_R = \operatorname{im}\omega > 0$ and $R = \mathbb{Z}[\omega]$.

Proof. The induced hermitian form is necessarily of the form $h_{0,\Lambda} = \mu h_0$ with $\mu \in \mathbb{R}_{>0}$ and $h_0(z,w) = z\overline{w}$ because the conjugacy classes of hermitian forms on $\mathbb{C}$-vector spaces are determined by their rank and signature. Moreover, since $h_{0,\Lambda}$ is a principal polarization $\operatorname{im} h_{0,\Lambda}(\Lambda,\Lambda) = \deg a_{0,E}\mathbb{Z} = \mathbb{Z}$. Hence

$$\begin{aligned} \operatorname{im} h_{0,\Lambda}(\Lambda,\Lambda) &= \operatorname{im} h_{0,\Lambda}(\mathfrak{a}x, \mathfrak{a}x) \\ &= \operatorname{im} \mu N(\mathfrak{a}) N(x) R \\ &= \mu N(\mathfrak{a}) N(x) \operatorname{im} R \\ &= \mu N(\mathfrak{a}) N(x) \alpha_R \mathbb{Z} = \mathbb{Z}. \end{aligned}$$

Hence $\mu = \frac{1}{N(\mathfrak{a})N(x)\alpha_R}$. □

We want to investigate first how $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ acts on polarizations.

Let $\phi_\Lambda\colon \mathbb{C}/\Lambda \to E(\mathbb{C})$ with $\Lambda = \mathfrak{b}x$. We write $\mathbf{F}_h(E_\Lambda, a_{0,E}) = (\Lambda, H_{0,\Lambda})$ with $H_{0,\Lambda} = h_{0,\Lambda}^{\alpha_R}$ and, by Lemma 3.8, we can write the Gram matrix of $H_{0,\Lambda}$ in the K basis x of $K\Lambda$, by $G_\Lambda(x) = \frac{1}{N(\mathfrak{b})}$. It is then clear that for all fractional ideal $\mathfrak{a}$, we have $\mathfrak{a}\Lambda = \mathfrak{a}\mathfrak{b}x$ and thus, the Gram matrix of the analytic representation of the canonical polarization of $E_{\mathfrak{a}\Lambda}$ in the basis x is $G_{\mathfrak{a}\Lambda}(x) = \frac{1}{\mathfrak{a}\mathfrak{b}} = \frac{1}{N(\mathfrak{a})} G_\Lambda(x)$.

Moreover, $a^{\sigma}_{0,E}$ is the canonical polarization a_{0,E^σ} of E^σ for any E and $\sigma \in \mathrm{Aut}(\mathbb{C})$ and every polarization on elliptic curves is of the form $na_{0,E}$ for some $n \in \mathbb{N}^*$. What we did can easily be generalized for any polarization of elliptic curves.

We can conclude with this proposition.

Proposition 3.9. *Let $E = E_\Lambda \in \mathcal{A}_R$, $a_{0,E}$ the canonical polarization on E and $\mathbf{F}_h(E, a_{0,E}) = (\Lambda, H_{0,\Lambda})$. Then for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $\dot{\mathfrak{a}}^{-1} = F(\sigma)$ there is an isometry*

$$\mathbf{F}_h(E^\sigma, a_{0,E}) \simeq \left(\mathfrak{a}\Lambda, \frac{1}{N(\mathfrak{a})} H_{0,\Lambda}\right).$$

Proof. Let $\mathbf{F}_h(E^\sigma, a_{0,E^\sigma}) = (\Lambda_\sigma, H_{0,\Lambda_\sigma})$. By Proposition 3.7 and Lemma 3.4 we have an isomorphism

$$\nu_{r_\sigma} : E^\sigma \longrightarrow \mathfrak{a}^{-1} \star E$$

and $(\mathfrak{a}^{-1} \star E)(\mathbb{C}) \simeq \mathbb{C}/\mathfrak{a}\Lambda$. We have $\mathbf{F}_h(\mathfrak{a}^{-1} \star E, a_{0,\mathfrak{a}^{-1}E}) = \left(\mathfrak{a}\Lambda, \frac{1}{N(\mathfrak{a})} H_{0,\Lambda}\right)$. Since every isogeny between elliptic curves is a polarized isogeny for the canonical polarizations, the isomorphism ν_{r_σ} is a polarized isogeny and then its analytic representation $r_\sigma : (\Lambda_\sigma, H_{0,\Lambda_\sigma}) \longrightarrow \left(\mathfrak{a}\Lambda, \frac{1}{N(\mathfrak{a})} H_{0,\Lambda}\right)$ defines an isometry on the induced hermitian lattices. □

3.3 Product of CM elliptic curves

Let $A = \bigoplus_{i=1}^{g} E_i$ be the product of g elliptic curves with CM by R over $\overline{\mathbb{Q}}$. Let $\Lambda_i \subset \mathbb{C}$ be lattices such that $\phi_{\Lambda_i} : \mathbb{C}/\Lambda_i \to E_i(\mathbb{C})$ is the canonical isomorphism with $g_k(\Lambda_i) \in \overline{\mathbb{Q}}$. Then there is a canonical isomorphism $\phi_\Gamma : \mathbb{C}^g/\Gamma \to A(\mathbb{C})$ with $\Gamma = \bigoplus \Lambda_i$ and $\phi_\Gamma = (\phi_{\Lambda_i})_{i=1\ldots g}$. In this section, we show how the results of Section 3.2 apply to products of elliptic curves and we conclude with the proofs of Theorem 3.1 and 3.2.

3.3.1 Isogenies between products of elliptic curves

Proposition 3.10. *Let $A, A' \in \mathcal{A}_R$ considered over $\overline{\mathbb{Q}}$ with $A = E_{\Lambda_1} \times \cdots \times E_{\Lambda_g}$ and $A' = E_{\Lambda'_1} \times \cdots \times E_{\Lambda'_g}$. Let $\Gamma = \bigoplus_i \Lambda_i$ and $\Gamma' = \bigoplus_j \Lambda'_j$. Then, for any morphism $f : A \to A'$, the matrix M_f of the analytic representation of $(f, \phi_\Gamma, \phi_{\Gamma'})$ in the canonical basis of $\mathbb{C}\Gamma$ and $\mathbb{C}\Gamma'$ has coefficients in $\overline{\mathbb{Q}}$ and for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $M_{f^\sigma} = M_f^\sigma$.*

Proof. Consider the following diagram for all k, l

$$\begin{array}{ccccccc}
\mathbb{C}/\Lambda_k & \xhookrightarrow{j_k} & \mathbb{C}^g/\Gamma & \xrightarrow{M_f} & \mathbb{C}^g/\Gamma' & \xrightarrow{p'_l} & \mathbb{C}/\Lambda'_l \\
\downarrow{\scriptstyle \phi_{\Lambda_k}} & & \downarrow{\scriptstyle \phi_\Gamma} & & \downarrow{\scriptstyle \phi_{\Gamma'}} & & \downarrow{\scriptstyle \phi_{\Lambda'_l}} \\
E_{\Lambda_k}(\mathbb{C}) & \xhookrightarrow{\iota_k} & A(\mathbb{C}) & \xrightarrow{f} & A'(\mathbb{C}) & \xrightarrow{\pi'_l} & E_{\Lambda'_l}(\mathbb{C})
\end{array}$$

with j_k, ι_k and p'_l, π'_l the k^{th} component inclusion and l^{th} component projection respectively.

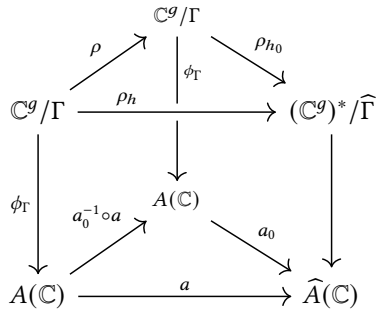

Figure 4: Analytic representation of polarizations

Through those morphisms, we can see the k, l coefficient $m_{l,k}$ of M_f as a map

$$m_{l,k}\colon \mathbb{C}/\Lambda_k \to \mathbb{C}/\Lambda'_l$$

which is in $\overline{\mathbb{Q}}$; furthermore, by Proposition 3.6, $m_{l,k}^\sigma$ is the analytic representation of $\big((p'_l \circ f \circ \iota_k)^\sigma, \phi_{\Lambda_k}, \phi_{\Lambda_l}\big)$. □

Let $(A, a) \in \mathcal{A}_R^p$ with $A \simeq E_{\Lambda_1} \times \cdots \times E_{\Lambda_g}$. Let $\Gamma = \bigoplus_i \Lambda_i$. We denote by h the hermitian form on $\mathbb{C}^g$ and $\rho_h \in \mathrm{Hom}_{\mathbb{C}}(\Gamma, \widehat{\Gamma})$ the map induced by the polarization a. Consider a_0 the product polarization of the canonical polarizations on each elliptic curve $a_{0,E_i}\colon E_i \to \widehat{E}_i$. It is an isomorphism

$$a_0\colon \bigoplus_{i=1}^g E_i \longrightarrow \bigoplus_{i=1}^g \widehat{E}_i$$

which induces

$$\rho_{h_0} = \big(\rho_{h_{0,\Lambda_i}}\big)\colon \mathbb{C}^g/\bigoplus_i \Lambda_i \longrightarrow (\mathbb{C}^g)^*/\bigoplus_i \widehat{\Lambda}_i$$

with each $\rho_{h_{0,\Lambda_i}}$ induced by the canonical polarization on E_{Λ_i}. We can now consider the analytic representation ρ of $(a_0^{-1} \circ a, \phi_\Gamma, \phi_\Gamma)$. By definition, the diagram of Figure 4 commutes. Recall that we denoted $\alpha_R = \mathrm{im}\,\omega > 0$ with $R = \mathbb{Z}[\omega]$. Let $\Lambda_i = \mathfrak{a}_i x_i$ then $\Gamma = \bigoplus \mathfrak{a}_i x_i$ and, with Lemma 2.2 we can show that

$$\widehat{\Gamma} = \{\ell \in (\mathbb{C}^g)^* \mid \mathrm{im}\,\ell(\Gamma) \subset \mathbb{Z}\} = \{\ell \in (\mathbb{C}^g)^* \mid \alpha_R \ell(\Gamma) \subset R\} = \bigoplus \frac{1}{\alpha_R}\overline{\mathfrak{a}_j}^{-1} x_j^*$$

with $x_j^* \in (\mathbb{C}^g)^*$ defined by $x_j^*(x_i) = \delta_{i,j}$ with $\delta_{i,j} = 1$ for $i = j$ and 0 otherwise.

Proposition 3.11. *With the notation above let $b = (x_i)_{i=1,\dots,g}$. Let $M_{b,b}(\rho)$ be the matrix of ρ in the basis b and $G_\Gamma(b) = \big(h^{\alpha_R}(x_i, x_j)\big)_{i,j}$ the Gram matrix of the hermitian form $h^{\alpha_R} = \alpha_R h$ in the basis b. Then*

$$M_{b,b}(\rho) = G_\Gamma(b) \cdot D$$

with $D = \operatorname{diag}\big(N(\mathfrak{a}_1), \dots, N(\mathfrak{a}_g)\big)$*, the diagonal matrix with coefficients* $d_{i,i} = N(\mathfrak{a}_i)$.

Proof. By definition of $\rho_{h_{0,\Lambda_i}} \in \operatorname{Hom}_{\mathbb{C}}(\Lambda_i, \widehat{\Lambda}_i)$ and Lemma 3.8,

$$\rho_{h_{0,\Lambda_i}} : \begin{cases} \mathbb{C}/\Lambda_i \longrightarrow \mathbb{C}^*/\widehat{\Lambda}_i \\ \quad z \longmapsto \left(\ell_z \colon w \mapsto \frac{z\overline{w}}{\alpha_R N(\mathfrak{a}) N(x_i)}\right). \end{cases}$$

Hence $\rho_{h_0}(x_i) = \ell_{x_i} = \frac{1}{N(\mathfrak{a}_i)\alpha_R} x_i^*$ so $\rho_{h_0}^{-1}(x_i^*) = N(\mathfrak{a}_i)\alpha_R x_i$. Thus, for any $\ell = \sum_i u_i x_i^* \in (\mathbb{C}^g)^*$,

$$\rho_{h_0}^{-1}(\ell) = \sum_{i=1}^{g} u_i N(\mathfrak{a}_i)\alpha_R x_i \tag{8}$$

and then its j^{th} component is

$$\big(\rho_{h_0}^{-1}(\ell)\big)_j = u_j N(\mathfrak{a}_j)\alpha_R = \alpha_R \ell(x_j). \tag{9}$$

Now, since $\rho = \rho_{h_0}^{-1} \circ \rho_h$ we have

$$\begin{aligned} \rho_{ij} &= \big(\rho(x_i)\big)_j \\ &= \big(\rho_{h_0}^{-1} \circ \rho_h(x_i)\big)_j \\ &= N(\mathfrak{a}_j)\alpha_R \rho_h(x_i)(x_j) \text{ by (8) and (9)} \\ &= N(\mathfrak{a}_j)\alpha_R h(x_i, x_j) \\ &= N(\mathfrak{a}_j) h^{\alpha_R}(x_i, x_j) \\ &= (G_\Gamma(b) \cdot D)_{i,j}. \end{aligned}$$

□

Proposition 3.12. *Let* $A, A' \in \boldsymbol{\mathcal{A}}_R$ *considered over* $\overline{\mathbb{Q}}$ *with* $A = E_{\Lambda_1} \times \cdots \times E_{\Lambda_g}$ *and* $A' = E_{\Lambda'_1} \times \cdots \times E_{\Lambda_{g'}}$*. Let* $\Gamma = \bigoplus_i \Lambda_i$ *and* $\Gamma' = \bigoplus_j \Lambda'_j$*. Assume that for all* $i, j, \operatorname{Hom}_{\mathbb{C}}(\Lambda_i, \Lambda'_j) \subset K$*. Then for any* $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/K)$ *and* $\mathfrak{a}$ *a fractional* R*-ideal such that* $F(\sigma) = \dot{\mathfrak{a}} \in \operatorname{Cl}(R)$ *there exists* $r_\sigma \in \overline{\mathbb{Q}}$ *such that for any* $f \colon A \to A'$ *with analytic representation* M *there is a commutative diagram*

$$\begin{array}{ccc} A^\sigma(\mathbb{C}) & \xrightarrow{f^\sigma} & A'^\sigma(\mathbb{C}) \\ \uparrow{\scriptstyle \phi_\Gamma} & & \uparrow{\scriptstyle \phi_{\Gamma'_\sigma}} \\ \mathbb{C}^g/\Gamma_\sigma & \xrightarrow{M} & \mathbb{C}^{g'}/\Gamma'_\sigma \\ \downarrow{\scriptstyle r_\sigma I_g} & & \downarrow{\scriptstyle r_\sigma I_{g'}} \\ \mathbb{C}^g/\mathfrak{a}^{-1}\Gamma & \xrightarrow{M} & \mathbb{C}/\mathfrak{a}^{-1}\Gamma'. \end{array}$$

Proof. Apply Lemma 3.7 and following the same steps as in the proof of Proposition 3.10. □

Proposition 3.13. *Let $E_1, \dots, E_g$ be elliptic curves over $\overline{\mathbb{Q}}$ with CM by R and the isomorphisms $\phi_{\Lambda_i} : \mathbb{C}/\Lambda_i \to E_i(\mathbb{C})$ with $\mathrm{Hom}_{\mathbb{C}}(\Lambda_i, \Lambda_j) \subset K$. Let a_{0,E_i} be the canonical polarization on E_i, let a_0 be the product polarization on $E_1 \times \cdots \times E_g$ and $\mathbf{F}_h(\bigoplus_i E_i, a_0) = (\bigoplus_i \Lambda_i, H_0)$. Then for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $\dot{\mathfrak{a}}^{-1} = F(\sigma)$ there is an isometry*

$$\mathbf{F}_h\left(\bigoplus_i E_i^\sigma, a_0^\sigma\right) \simeq \left(\mathfrak{a}\bigoplus_i \Lambda_i, \frac{1}{N(\mathfrak{a})} H_0\right).$$

Proof. Apply Lemma 3.9 component by component. □

3.3.2 Proof of Theorem 3.1 and 3.2

We have now the necessary tools to prove both Theorem 3.1 and 3.2. Since both theorems aim to describe the isometry class of $\mathbf{F}_h(A^\sigma, a^\sigma)$, for $(A, a) \in \mathcal{A}_R^p$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ or $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, it is enough to show that there is such an isometry for a particular object in the isomorphism class of (A^σ, a^σ). By definition of $\mathcal{A}_R^p$, each isomorphism class of polarized abelian variety contains an element of the form $(E_1 \times \cdots \times E_g, a)$ so we will show the isometry for this particular case.

Let (L, H) be an integral rank g hermitian R-lattice. Fixing a basis b of KL gives an isomorphism $KL \simeq K^g$ and pushing forward H on K^g gives an isometry $(KL, H) \to (K^g, H)$. We identify (L, H) with its image in (K^g, H). The hermitian form H is determined by the Gram matrix of b given by $G = G(b) = \big(H(v, w)\big)_{v,w \in b} \in M_{g,g}(K)$. Indeed, with $x, y \in K^g$, we have

$$H(x, y) = {}^t x G \overline{y}$$

and then, by definition,

$$\overline{H}(x, y) = \overline{H(\overline{x}, \overline{y})} = \overline{{}^t \overline{x} G \overline{\overline{y}}} = {}^t x \overline{G} \overline{y}.$$

Hence $(\overline{L}, \overline{H})$ has Gram matrix $\overline{G}$.

Proof of Theorem 3.1. Let $(A, a) \in \mathcal{A}_R^p$ considered over $\overline{\mathbb{Q}}$ with $A = E_{\Lambda_1} \times \cdots \times E_{\Lambda_g}$ with $\mathrm{Hom}_{\mathbb{C}}(\Lambda_i, \Lambda_j) \subset K$. Let $\mathbf{F}_h(A, a) = (L, H)$ and let $\mathbf{F}_h(\overline{A}, \overline{a}) = (L', H')$. We write $\Lambda_i = \mathfrak{a}_i x_i$ and $b = (x_1, \dots, x_g)$ such that $(\mathfrak{a}_i, x_i)$ is a pseudo-basis of $L = \bigoplus_i \Lambda_i$. By Lemma 3.3, $L' = \overline{L}$. Moreover, by Proposition 3.11, the matrix $M(b, b)$ of the analytic representation ρ of $(a_0^{-1} \circ a, \phi_L, \phi_L)$ satisfies $M_{b,b}(\rho) = G_L(b) \cdot D$ with D the diagonal matrix $\mathrm{diag}\big(N(\mathfrak{a}_1), \dots, N(\mathfrak{a}_g)\big)$. By Proposition 3.10 and by applying the complex conjugation to the diagram

$$\begin{array}{ccc} \mathbb{C}^g/L & \xrightarrow{\rho} & \mathbb{C}^g/L \\ \downarrow{\scriptstyle \phi_L} & & \downarrow{\scriptstyle \phi_L} \\ A(\mathbb{C}) & \xrightarrow{a_0^{-1} \circ a} & A(\mathbb{C}) \end{array}$$

the analytic representation of $(\overline{a_0}^{-1} \circ \overline{a}, \phi_{\overline{L}}, \phi_{\overline{L}})$ is $\overline{M_{b,b}(\rho)} = \overline{G_L(b)}$. Hence $(\overline{L}, H')$ has Gram matrix $\overline{G_L(b)}$ so $H' = \overline{H}$. □

Proof of Theorem 3.2. Let $(A,a) \in \mathcal{A}_R^p$ considered over $\overline{\mathbb{Q}}$ such that $A = E_{\Lambda_1} \times \cdots \times E_{\Lambda_g}$ with $\mathrm{End}(\Lambda_i, \Lambda_j) \subset K$ for all i, j. We will write $E_i = E_{\Lambda_i}$ for simplicity. Let $\Gamma = \bigoplus \Lambda_i$ and $\mathbf{F}_h(A,a) = (L,H), \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ with $L = \Gamma$ and $\dot{\mathfrak{a}}^{-1} = F(\sigma)$.

First step: find a polarized isogeny $(E^n, D \cdot \lambda_0) \to (A,a)$ with D diagonal with integer entries. Let $\Lambda = \Lambda_1$ and $E = E_1$ and λ_0 the product polarization on E^g. There exist $\alpha_i \in K$ such that for all $i, \alpha_i\Lambda \subset \Lambda_i$. This induces an isogeny $q\colon E^g \to A$. We denote by $Q = \mathrm{diag}(\alpha_1, \ldots, \alpha_g)$ the analytic representation of $(q, \phi_{\Lambda^g}, \phi_\Gamma)$. We consider $\lambda\colon E^g \to \widehat{E}^g$ the pullback polarization of a on E^g, i.e., the unique polarization on E^g that makes q a polarized isogeny. We consider $M = \lambda_0^{-1} \circ \lambda \in \mathrm{End}(E^g) \simeq M_g(R)$, and since $\lambda = \widehat{\lambda}$ the matrix M is a hermitian matrix, i.e., ${}^t\overline{M} = M$. Now consider a matrix $P \in M_g(R)$ such that ${}^t\overline{P}MP = D$ with D a diagonal matrix. Since M is positive definite and hermitian, so does D. Since $R \cap \mathbb{R}^+ = \mathbb{N}$ the matrix D has integer entries that are positive. So we have a polarized isogeny $f = q \circ P\colon (E^g, D \cdot \lambda_0) \to (A,a)$.

$$\begin{array}{ccccc}
E^g & \xrightarrow{P} & E^g & \xrightarrow{q} & \bigoplus E_i \\
\downarrow{\scriptstyle D} & & \downarrow{\scriptstyle M} & & \downarrow{\scriptstyle a} \\
E^g & \xleftarrow[{}^t\overline{P}]{} & E^g & \xleftarrow[\widehat{q}]{} & \widehat{\bigoplus E_i} \simeq \bigoplus E_i
\end{array}$$

We will denote by $S = QP$ the analytic representation of $(f, \phi_{\Lambda^g}, \phi_\Gamma)$. Since f is a polarized isogeny,

$$S\colon (K\Lambda^g, D) \to (KL, H) \tag{10}$$

is an isometry.

Second step: conclude. By Proposition 3.13, $\mathbf{F}_h\big((E^g)^\sigma, D^\sigma\big) \underset{r_\sigma}{\simeq} \left(\mathfrak{a}\Lambda^g, \frac{1}{N(\mathfrak{a})}D\right)$. We now consider $\mathbf{F}_h(A^\sigma, a^\sigma) = (L_\sigma, H_\sigma)$ and $\iota_\sigma = \mathbf{F}_h(f^\sigma)$. By Proposition 3.7 we have $r_\sigma L_\sigma = \mathfrak{a}L$ and there is a commutative diagram

$$\begin{array}{ccc}
(E^g)^\sigma(\mathbb{C}) & \xrightarrow{f^\sigma} & A^\sigma(\mathbb{C}) \\
\uparrow{\scriptstyle \phi_{P_\sigma}} & & \uparrow{\scriptstyle \phi_{L_\sigma}} \\
\mathbb{C}^g/\Lambda_\sigma^g & \xrightarrow{S} & \mathbb{C}^g/L_\sigma \\
\downarrow{\scriptstyle r_\sigma I_g} & & \downarrow{\scriptstyle r_\sigma I_g} \\
\mathbb{C}/\mathfrak{a}\Lambda^g & \xrightarrow{S} & \mathbb{C}^g/\mathfrak{a}L.
\end{array}$$

Moreover, the maps

$$r_\sigma I_g \colon (KL_\sigma, H_\sigma) \to \left(K\mathfrak{a}L, H' = \frac{1}{N(r_\sigma)} H_\sigma\right) \text{ and}$$
$$S \colon \left(K\mathfrak{a}\Lambda^g, \frac{1}{N(\mathfrak{a})} D\right) \to (K\mathfrak{a}L, H')$$

are isometries. Hence we have $H' = \frac{1}{N(\mathfrak{a})} \overline{{}^t S^{-1}} D S^{-1} = \frac{1}{N(\mathfrak{a})} H$. Hence

$$\mathbf{F}_h(A^\sigma, a^\sigma) = (L_\sigma, H_\sigma) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})} H\right).$$

This concludes the proof of Theorem 3.2. □

4 Application to the field of moduli of varieties in $\mathcal{A}_R^p$

4.1 General results on the field of moduli of principally polarized abelian varieties in $\mathcal{A}_R^p$

We recall that the *field of moduli* of a polarized abelian variety (A, a) over $\overline{\mathbb{Q}}$ is the field fixed by the subgroup

$$\left\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid (A^\sigma, a^\sigma) \simeq (A, a)\right\}.$$

In the same way we define the field of moduli of a curve C over $\overline{\mathbb{Q}}$ by the fixed field of $\left\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mid C^\sigma \simeq C\right\}$.

The Abel–Jacobi map $C \mapsto (\mathrm{Jac}(C), j)$ which to a curve associates its polarized Jacobian variety induces a morphism

$$[\mathrm{Jac}] \colon \begin{cases} M_g \longrightarrow A_g \\ [C] \longmapsto [\mathrm{Jac}(C), j] \end{cases}$$

between the moduli space of smooth absolutely irreducible projective genus g curves and the moduli space of principally polarized abelian varieties of dimension g. By [3, Chapter VII,Corollary 12.2], [Jac] is injective so C and $(\mathrm{Jac}(C), j)$ have the same field of moduli.

For $g = 2$ and $g = 3$ the moduli spaces M_g and A_g have the same dimension and are irreducible. Thus, the Jacobian map is dominant if the field is algebraically closed. More specifically, every indecomposable principally polarized abelian variety is the Jacobian of a curve (see [11]).

We give a necessary condition on the class group of R and on $\mathbf{F}_h(A, a)$ for an abelian variety $(A, a) \in \mathcal{A}_R^p$ to have field of moduli $\mathbb{Q}$.

Proposition 4.1. *Let $(A,a) \in \mathcal{A}_R^p$ considered over $\overline{\mathbb{Q}}$ and $\mathbf{F}_h(A,a) = (L,H)$ be a hermitian lattice of rank g. If (A,a) has field of moduli $\mathbb{Q}$ then $\mathrm{Cl}(R)$ has exponent dividing g and $\mathrm{st}(L)$ has order at most 2.*

Proof. If (L,H) corresponds to a polarized abelian variety with field of moduli $\mathbb{Q}$ then $(L,H) \simeq \left(\mathfrak{a}L, \frac{1}{N(\mathfrak{a})}H\right)$ for all fractional ideal $\mathfrak{a}$. In particular, $L \simeq \mathfrak{a}L$ for all $\mathfrak{a}$ and then, their Steinitz classes are the same

$$\mathrm{st}(L) = \mathrm{st}(\mathfrak{a}L) = \mathfrak{a}^g \,\mathrm{st}(L) \in \mathrm{Cl}(R).$$

Hence $\mathfrak{a}^g = 1 \in \mathrm{Cl}(R)$ so $\mathrm{Cl}(R)$ has exponent dividing g.

The hermitian lattice isometry class must also be invariant by the action of the complex conjugation so

$$\mathrm{st}(L) = \mathrm{st}(\overline{L}) = \overline{\mathrm{st}(L)}.$$

By the formula $\overline{\mathfrak{a}}\mathfrak{a} = N(\mathfrak{a})R$, it means that $\mathrm{st}(L)$ must have order at most 2. □

Corollary 4.2. *Let $(A,a) \in \mathcal{A}_R^p$ with odd dimension g. Suppose (A,a) has field of moduli $\mathbb{Q}$. Then there exists an elliptic curve E with CM by R such that $A \simeq E^g$.*

Proof. Let $(L,H) = \mathbf{F}_h(A,a)$ be the corresponding unimodular hermitian lattice. By Proposition 4.1, its Steinitz class $\mathrm{st}(L)$ has order dividing g and 2 hence it must be 1. In other words L is free over R, i.e., $L \simeq R^g$ and then $A \simeq E^g$ with $\mathbf{F}(E) \simeq R$. □

4.2 Enumeration of the indecomposable principally polarized abelian varieties in $\mathcal{A}_R^p$ with field of moduli $\mathbb{Q}$

Since we are able to understand the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $\mathrm{Gal}(K/\mathbb{Q})$ through the equivalence of categories $\mathbf{F}_h$ developed in Section 2 we are able to check when $(A,a) \simeq (A^\sigma, a^\sigma)$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ when $(A,a) \in \mathcal{A}_R^p$ by looking for isometries between hermitian R-lattices. This is what Algorithm 1 does.

We denote by $\mathcal{A}_R(g)$ the set of all classes of dimension g indecomposable principally polarized abelian varieties $(A,a) \in \mathcal{A}_R^p$ and by $\mathcal{A}_{R,\mathbb{Q}}(g)$ the subset of $\mathcal{A}_R(g)$ corresponding to elements of $\mathcal{A}_R(g)$ with field of moduli $\mathbb{Q}$.

To compute the list of elements of $\mathcal{A}_{R,\mathbb{Q}}(g)$ for a given maximal order R we need the list of all unimodular indecomposable hermitian R-lattices of rank g. This can be done using the classification of these lattices developed by authors in [15].

We want to run the algorithm over all maximal orders of a given exponent dividing g. By [4], the complete list of the corresponding discriminants is finite for all g and known for g up to 8 under the Extended Riemann Hypothesis. However, we can get rid of the Extended Riemann Hypothesis for the genus 2 thanks to Proposition A.1 and for the genus 3 thanks to Proposition A.5, presented in the Appendix. Indeed, these two propositions provide an upper bound for the class number of a maximal order R that an abelian variety isomorphic to a product of elliptic curves with complex multiplication by R can have. This allows us to use the classification of imaginary quadratic fields with a given class number h, which is complete for $h \leqslant 100$ by [26].

Algorithm 1 Enumeration algorithm

Require: An integer g and a maximal order R with exponent dividing g.
Ensure: The list of unimodular indecomposable hermitian lattices (L, H) corresponding to the elements of $\mathcal{A}_{R,\mathbb{Q}}(g)$.

```
LList ← {Unimodular indecomposable hermitian lattices of rank g}/≃
LList_{FM−ℚ} ← { } {List of abelian varieties with field of moduli ℚ.}
for (L, H) ∈ LList do
    bool ← true
    for 𝔞 ∈ {generators of Cl(R)} do
        bool ← bool and (L, H) ≃ (𝔞L, 1/N(𝔞) H).
    end for
    if bool and (L, H) ≃ (L̄, H̄) then
        LList_{FM−ℚ} ← LList_{FM−ℚ} ∪{(L, H)}
    end if
end for
return LList_{FM−ℚ}
```

4.3 Enumeration of dimension 2 and 3 principally polarized abelian varieties of $\mathcal{A}_R^p$ with field of moduli $\mathbb{Q}$

As the computations become quickly time-consuming as the dimension g and the discriminant of the order grow we restricted to $g = 2$ and 3 to be able to have complete tables. We used the Magma library developed in [15].

We use Algorithm 1 to compute the cardinality of $\mathcal{A}_{R,\mathbb{Q}}(2)$ and present the results in the Table 1. In the column $\mathcal{P}$ we copy the number of $(A, a) \in \mathcal{A}_R^p$ such that A is the square of an elliptic curve with field of moduli $\mathbb{Q}$ to confirm we find the same values as in [9, Table 2].

In fact, for $g = 2$, the following proposition shows that it is not necessary to check if $(L, H) \simeq (\overline{L}, \overline{H})$.

Proposition 4.3. *Let (A, a) be a dimension 2 principally polarized abelian variety over $\mathbb{C}$ with A isomorphic to the power of elliptic curves E_i with CM by R maximal. Let $\mathbf{F}_h(A, a) = (L, H)$ be a hermitian integral lattice and let $\mathfrak{a}$ be the Steinitz class of L. Then*

$$\mathbf{F}_h(\overline{A}, \overline{a}) = (\overline{L}, \overline{H}) \simeq \left(\overline{\mathfrak{a}}L, \frac{1}{N(\mathfrak{a})}H\right).$$

Hence in this particular case, the action of the complex conjugation corresponds to the action of an automorphism of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$.

Proof. Let us write $L = Rx \oplus \mathfrak{a}y$. Let $G = \begin{pmatrix} \alpha & \beta \\ \overline{\beta} & \delta \end{pmatrix}$ be the Gram matrix of H in the basis (x, y) of KL. Since (A, a) is principally polarized (L, H) must be unimodular and then its volume $\mathfrak{v}(L) = N(\mathfrak{a}) \det(G)R = R$ so $N(\mathfrak{a}) \det(G)$ is invertible and real in R so $N(\mathfrak{a}) \det(G) = 1$.

h_R	Δ	$\mathcal{P}$	$\#\mathcal{A}_{R,\mathbb{Q}}$	$\#\mathcal{A}_R$	h_R	Δ	$\mathcal{P}$	$\#\mathcal{A}_{R,\mathbb{Q}}$	$\#\mathcal{A}_R$	h_R	Δ	$\mathcal{P}$	$\#\mathcal{A}_{R,\mathbb{Q}}$	$\#\mathcal{A}_R$
1	-3	0	0	0	2	-15	0	1	1	2	-115	0	3	11
	-4	0	0	0		-20	1	1	3		-123	0	4	12
	-7	0	0	0		-24	1	3	3		-148	3	5	13
	-8	1	1	1		-35	0	1	5		-187	0	3	17
	-11	1	1	1		-40	2	4	4		-232	5	10	20
	-19	1	1	1		-51	0	2	6		-235	0	5	21
	-43	2	2	2		-52	2	3	5		-267	0	6	24
	-67	3	3	3		-88	2	6	8		-403	0	3	35
	-163	7	7	7		-91	0	1	9		-427	0	3	37

h_R	Δ	$\mathcal{P}$	$\#\mathcal{A}_{R,\mathbb{Q}}$	$\#\mathcal{A}_R$	h_R	Δ	$\mathcal{P}$	$\#\mathcal{A}_{R,\mathbb{Q}}$	$\#\mathcal{A}_R$	h_R	Δ	$\mathcal{P}$	$\#\mathcal{A}_{R,\mathbb{Q}}$	$\#\mathcal{A}_R$
4	-84	0	2	18	4	-340	0	2	60	4	-595	2	2	106
	-120	3	4	24		-372	0	2	66		-627	0	0	112
	-132	1	2	26		-408	0	4	72		-708	1	2	122
	-168	0	4	32		-435	0	2	80		-715	0	2	126
	-195	0	2	40		-483	0	0	88		-760	1	4	130
	-228	1	2	42		-520	3	4	90		-795	2	2	140
	-280	0	4	50		-532	0	2	92		-1012	0	2	172
	-312	1	4	56		-555	0	2	100		-1435	0	2	246

h_R: Class number of the maximal order R of $\mathbb{Q}(\sqrt{\Delta})$.
$\#\mathcal{A}_R$: Number of elements of $\mathcal{A}_R(2)$ defined in Section 4.2.
$\#\mathcal{A}_{R,\mathbb{Q}}$: Number of elements of $\mathcal{A}_{R,\mathbb{Q}}(2)$.
$\mathcal{P}$: Number of elements (A, a) of $\mathcal{A}_{R,\mathbb{Q}}(2)$ such that $A \simeq E^2$ for some E.

Table 1: Computations for $g = 2$

Now consider $P = N(\mathfrak{a})\begin{pmatrix} \overline{\beta} & \delta \\ -\alpha & -\beta \end{pmatrix}$, matrix of a linear map $K\overline{x} + K\overline{y} \to Kx + Ky$. It satisfies the relation

$$ {}^tP\frac{1}{N(\mathfrak{a})}G\overline{P} = N(\mathfrak{a})\det(G)\overline{G} = \overline{G}. $$

So P defines an isometry between hermitian spaces.

Moreover, $\alpha = H(x,x) = N(x) \in R \cap \mathbb{R} = \mathbb{Z}$, $\beta = H(x,y)$, so $\overline{\mathfrak{a}}\beta = H(x, \mathfrak{a}y) \subset R$ so $\beta \in \overline{\mathfrak{a}}^{-1} = \frac{\mathfrak{a}}{N(\mathfrak{a})}$ and, in the same way, $\delta \in \frac{1}{N(\mathfrak{a})}\mathbb{Z}$. Hence

$$ P\overline{x} = N(\mathfrak{a})(\overline{\beta}x - ay) \in \overline{\mathfrak{a}}x + N(\mathfrak{a})y = \overline{\mathfrak{a}}L $$
$$ P\overline{ay} = N(\mathfrak{a})\overline{\mathfrak{a}}(\delta x - by) \in \overline{\mathfrak{a}}x + N(\mathfrak{a})y = \overline{\mathfrak{a}}L. $$

Thus, P defines an isometry $(\overline{L}, \overline{H}) \to \left(\overline{\mathfrak{a}}L, \frac{1}{N(\mathfrak{a})}H\right)$ □

h_R	Δ	$\#\mathcal{A}_{R,\mathbb{Q}}$	$\#\mathcal{A}_R^{\text{free}}$	h_R	Δ	$\#\mathcal{A}_{R,\mathbb{Q}}$	$\#\mathcal{A}_R^{\text{free}}$
1	-3	0	0	3	-107	2	44
	-4	0	0		-139	1	79
	-7	0	0		-211	0	209
	-8	0	0		-283	1	417
	-11	0	0		-307	0	507
	-19	1	1		-331	2	613
	-43	3	5		-379	0	851
	-67	5	13		-499	1	1665
	-163	13	103		-547	1	2059
					-643	1	3075
3	-23	0	3		-883	0	6703
	-31	0	6		-907	1	7163
	-59	1	10				
	-83	0	24	9	-4027	0	0

h_R: Class number of the maximal order R of $\mathbb{Q}(\sqrt{\Delta})$.
$\#\mathcal{A}_R^{\text{free}}$: Number of classes (A, a) in $\mathcal{A}_R(3)$ with $A \simeq E^3$ for some E.
$\#\mathcal{A}_{R,\mathbb{Q}}$: Number of elements of $\mathcal{A}_{R,\mathbb{Q}}(3)$.

Table 2: Computations for $g = 3$

In dimension $g = 3$ computations are more time consuming. Fortunately, by Corollary 4.2, in odd dimension all isomorphism class of (A, a) in $\mathcal{A}_{R,\mathbb{Q}}(3)$ are actually isomorphic to some a power of an elliptic curve. Hence we can run the algorithm only on free unimodular hermitian lattices and the latter are easier to enumerate and to work with.

We summarize the calculations in Table 2. All computations use Algorithm 1, except for the discriminant -4027, for which Proposition A.5 allows us to complete this missing entry.

A Class groups of CM fields from polarized products of CM elliptic curves with field of moduli $\mathbb{Q}$

by Francesc Fité and Xavier Guitart

Let K be an imaginary quadratic field and let H_K be its Hilbert class field. We denote by C_g the cyclic group of g elements.

Proposition A.1. *Let $E_1/\overline{\mathbb{Q}}$ and $E_2/\overline{\mathbb{Q}}$ be elliptic curves with CM by K, and let φ be an indecomposable principal polarization on $E_1 \times E_2$. If the field of moduli of $(E_1 \times E_2, \varphi)$ is $\mathbb{Q}$, then $\mathrm{Cl}(K)$ is isomorphic to one of the groups $\mathrm{C}_1, \mathrm{C}_2$, or $\mathrm{C}_2 \times \mathrm{C}_2$.*

Proof. Since φ is indecomposable there exists a curve $C/\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}$ such that $\mathrm{Jac}(C) \simeq E_1 \times E_2$. The curve C is not necessarily defined over $\mathbb{Q}$. By [18, §2.4] there exists a number field k' with $[k' : \mathbb{Q}] \leqslant 2$ such that C admits a model over k'. Since k' can be chosen to be any field over which Mestre's conic has a rational point, we can choose it so that $k' \cap H_K = \mathbb{Q}$.

Put $k = Kk'$, and suppose from now on that C is defined over k. In particular, $A = \mathrm{Jac}(C)$ is an abelian surface defined over k such that $A_{\overline{\mathbb{Q}}} \sim E^2$, where $E/\overline{\mathbb{Q}}$ is an elliptic curve with CM by K. Denote by L the smallest field of definition of the endomorphisms of A. Since k contains K, by [6, Theorem 2.14] the field $F = Hk$ is a subfield of L and $\mathrm{Gal}(F/k)$ has exponent $\leqslant 2$. By [6, Remark 3.1] $\mathrm{Gal}(L/k)$ is either C_n for $n \in \{1, 2, 3, 4, 6\}$, D_n for $n \in \{2, 3, 4, 6\}$, A_4 or S_4. Since $\mathrm{Gal}(F/k)$ is a quotient of exponent $\leqslant 2$ of $\mathrm{Gal}(L/k)$, we see that $\mathrm{Gal}(F/k) \simeq \mathrm{C}_1, \mathrm{C}_2$, or $\mathrm{C}_2 \times \mathrm{C}_2$ (cf. [6, Table1]). By our choice of k', we have that $H_K \cap k = K$, and hence $\mathrm{Gal}(F/k) \simeq \mathrm{Gal}(H_K/K) \simeq \mathrm{Cl}(K)$. □

Remark A.2. The above proposition dispenses with the assumption of the Generalized Riemann Hypothesis in [9, Table 4]. Moreover the complete list of imaginary quadratic fields with a given class number h is known up to $h = 100$ by [26]. Hence the table 1 is unconditionally complete.

A key property used in the proof of Proposition A.1 is that a curve of genus 2 can be defined over a quadratic extension of its field of moduli. The same is true for curves of genus 3.

Proposition A.3. *Let C be a curve of genus 3 with field of moduli $\mathbb{Q}$. There exist infinitely many quadratic extensions $k/\mathbb{Q}$ such that C admits a model over k.*

Proof. The curve C is either a hyperelliptic curve or a smooth plane quartic. If C is hyperelliptic, it is well known that it can be defined over infinitely many fields k with $[k : \mathbb{Q}] \leqslant 2$ (the curve $C/\mathrm{Aut}(C)$ is a conic that can be defined over $\mathbb{Q}$ and k can be taken to be any field where it has rational points). Suppose that C is a plane quartic. If $|\mathrm{Aut}(C)| = 1$, the curve admits a model over its field of moduli by Weil descent. If $|\mathrm{Aut}(C)| > 2$, then the curve also admits a model over its field of moduli (cf. [17, Prop. 2.3 and §3.2]). If $|\mathrm{Aut}(C)| = 2$ the result is Lemma A.4 below, which is probably well known but we include a proof for completeness. □

Lemma A.4. *Let $C/\overline{\mathbb{Q}}$ be a curve with field of moduli $\mathbb{Q}$ and such that $|\mathrm{Aut}(C)| = 2$. There exist infinitely many quadratic extensions $k/\mathbb{Q}$ such that C admits a model over k.*

Proof. For every $\sigma \in G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, let $\mu_\sigma : {}^\sigma C \xrightarrow{\simeq} C$ be an isomorphism, chosen in such a way that the system $\{\mu_\sigma\}_{\sigma \in G_{\mathbb{Q}}}$ is locally constant. For any $\psi \in \mathrm{Aut}(C)$ we have that

$$ {}^\sigma\psi = \mu_\sigma^{-1} \circ \psi \circ \mu_\sigma. \tag{11}$$

The equality is obvious when ψ is the identity. When ψ is the non-trivial automorphism of C, the equality follows from the fact that then ${}^\sigma\psi$ is the non-trivial automorphism of ${}^\sigma C$.

For $\sigma, \tau \in G_{\mathbb{Q}}$ define

$$c(\sigma, \tau) = \mu_\sigma \circ {}^{\sigma}\mu_\tau \circ \mu_{\sigma\tau}^{-1} \in \mathrm{Aut}(C).$$

A short computation using (11) shows that c is a two-cocycle in $Z^2\big(G_{\mathbb{Q}}, \mathrm{Aut}(C)\big)$, where the action of $G_{\mathbb{Q}}$ on $\mathrm{Aut}(C)$ is the trivial action. Therefore, the class of c can be identified with an element in $H^2(G_{\mathbb{Q}}, \{\pm 1\})$. Now $H^2(G_{\mathbb{Q}}, \{\pm 1\})$ is isomorphic to the 2-torsion of the Brauer group of $\mathbb{Q}$, which is generated by quaternion algebras. Any product of quaternion algebras is equivalent in the Brauer group to a quaternion algebra, so the class of c can be identified with a quaternion algebra B. Let k be any quadratic splitting field of B (there exist infinitely many such fields k). The restriction $\mathrm{Res}^k_{\mathbb{Q}}(c)$ is a coboundary, that is to say, there exists a function $\delta\colon G_k \to \{\pm 1\}$ such that

$$c(\sigma, \tau) = \delta(\sigma)\delta(\tau)\delta(\sigma\tau)^{-1} \text{ for all } \sigma, \tau \in G_k.$$

If we define $\tilde{\mu}_\sigma := \delta(\sigma)^{-1} \circ \mu_\sigma$ for $\sigma \in G_k$, the system $\{\tilde{\mu}_\sigma\}_{\sigma \in G_k}$ is a descent data for C over k and we see that C can be defined over k. □

Proposition A.5. *Let E_1, E_2, E_3 be elliptic curves over $\overline{\mathbb{Q}}$ with CM by K. Let φ be a principal indecomposable polarization on $A := E_1 \times E_2 \times E_3$ such that (A, φ) has field of moduli $\mathbb{Q}$. Then the class number of K is 1 or 3.*

Proof. By the results of [23] we have that (A, φ) is isomorphic to the canonically polarized Jacobian of some genus three curve $C/\overline{\mathbb{Q}}$. Since (A, φ) has field of moduli $\mathbb{Q}$, the curve C has field of moduli $\mathbb{Q}$ as well. By Proposition A.3 there exists a quadratic extension $k'/\mathbb{Q}$ with $k' \cap H_K = \mathbb{Q}$ such that C admits a model over k'. Put $k = k'K$ and suppose from now on that C is defined over k.

If $A = \mathrm{Jac}(C)$ we have that A is defined over k and $A_{\overline{\mathbb{Q}}} \sim E^3$, where E is an elliptic curve with CM by K. Denote by L the minimal extension of k such that $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathrm{End}(A_L)$. By [6, Theorem 2.14] the field $F = Hk$ is a subfield of L and $\mathrm{Gal}(F/k)$ has exponent dividing 3. Since $k \cap H_K = K$ we have that $\mathrm{Cl}(K) \simeq \mathrm{Gal}(H_K/K) \simeq \mathrm{Gal}(F/k)$ has exponent 3.

The argument in the proof of [6, Corollary 2.17] shows that if $v_3(|\mathrm{Gal}(L/k)|) > 1$ then $K = \mathbb{Q}(\sqrt{-3})$ (here v_3 stands for the valuation at 3). Suppose then that $v_3(|\mathrm{Gal}(L/k)|) \leqslant 1$. Since Hk/k is a subextension of L/k we see that $v_3(|\mathrm{Gal}(H_K/K)|) = v_3(|\mathrm{Gal}(Hk/k)|) \leqslant 1$. This completes the proof of the proposition. □

Remark A.6. Let A be an abelian threefold defined over a number field k such that $A_{\overline{\mathbb{Q}}} \sim E^3$, where $E/\overline{\mathbb{Q}}$ is an elliptic curve with CM by K. Denote by L the minimal extension of k such that $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathrm{End}(A_L)$. As explained in [8, §3.2] the group of components $\pi_0\big(\mathrm{ST}(A)\big)$ of the Sato–Tate group of A can be identified with $\mathrm{Gal}(L/k)$. The last paragraph of the proof of the previous proposition shows that if $v_3(|\pi_0\big(\mathrm{ST}(A)\big)|) > 1$, then $K = \mathbb{Q}(\sqrt{-3})$.

There are 4 maximal genus 3 Sato–Tate groups G with connected component of the identity $G^0 \simeq \mathrm{U}(1)_3$ and $v_3(|\pi_0(G)|) > 1$. These are $J_s\big(B(T,3)\big)$, $J\big(B(T,3)\big)$, $J\big(D(6,6)\big)$,

and $J\big(E(216)\big)$. Abelian threefolds realizing them are given in [8, §8]. Consistently with the observation of the previous paragraph, note that in all of these constructions K is taken to be $\mathbb{Q}(\sqrt{-3})$.

References

[1] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of Grundlehren der mathematischen Wissenschaften. Springer, 2004.

[2] Keith Conrad. Ideal classes and relative integers. 2016. https://kconrad.math.uconn.edu/blurbs/gradnumthy/relativeintandidealclasses.pdf

[3] Gary Cornell and Joseph H. Silverman, editors. *Arithmetic geometry*. Springer, 1986.

[4] Andreas-Stephan Elsenhans, Jürgen Klüners, and Florin Nicolae. Imaginary quadratic number fields with class groups of small exponent. *Acta Arith.* 193(3):217–233, 2020.

[5] Francesc Fité, Enric Florit and Xavier Guitart. Endomorphism algebras of geometrically split genus 2 Jacobians over Q. 2022. https://arxiv.org/abs/2212.11102

[6] Francesc Fité and Xavier Guitart. Fields of definition of elliptic k-curves and the realizability of all genus 2 Sato-Tate groups over a number field. *Trans. Amer. Math. Soc.* 370(7):4623–4659, 2018.

[7] Francesc Fité and Xavier Guitart. Endomorphism algebras of geometrically split abelian surfaces over $\mathbb{Q}$. *Algebra & Number Theory* 14(6):1399–1421, 2020.

[8] Francesc Fité, Kiran S. Kedlaya, and Andrew V. Sutherland. Sato-tate groups of abelian threefolds, 2021. https://arxiv.org/abs/2106.13759

[9] Alexandre Gélin, Everett W. Howe, and Christophe Ritzenthaler. Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$. In *Proceedings of the Thirteenth Algorithmic Number Theory Symposium*, volume 2 of Open Book Ser., pages 257–274. Math. Sci. Publ., 2019.

[10] Detlev W. Hoffmann. On positive definite Hermitian forms. *Manuscripta Math.* 71(4):399–429, 1991.

[11] W. L. Hoyt. On products and algebraic families of Jacobian varieties. *Ann. Math. (2)* 77:415–423, 1963.

[12] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, and John T. Tate. Abelian varieties isogenous to a power of an elliptic curve. *Compos. Math.* 154(5):934–959, 2018.

[13] Ernst Kani. Products of CM elliptic curves. *Collect. Math.* 62(3):297–339, 2011.

[14] Markus Kirschmer *Definite quadratic and hermitian forms with small class number*. Habilitation thesis, RWTH Aachen University, 2016.

[15] Markus Kirschmer, Fabien Narbonne, Christophe Ritzenthaler, and Damien Robert. Spanning the isogeny class of a power of an elliptic curve. *Math. Comp.* 91(333):401–449, 2021.

[16] Elisa Lorenzo García, Christophe Ritzenthaler and Fernando Rodríguez Villegas. An arithmetic intersection for squares of elliptic curves with complex multiplication. 2024. https://arxiv.org/abs/2412.08738

[17] Reynald Lercier, Christophe Ritzenthaler, Florent Rovetta, and Jeroen Sijsling. Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields. *LMS J. Comput. Math.* 17(suppl. A):128–147, 2014.

[18] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser, 1991.

[19] James S. Milne. *Abelian varieties*. Version v2.00, 2008. https://www.jmilne.org/math/

[20] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Oxford University Press, London, 1970.

[21] Fabien Narbonne. *Produits polarisés de courbes elliptiques à multiplication complexe et applications aux courbes de petit genre*. Thèse de doctorat. Sous la direction de Ritzenthaler, Christophe. Université de Rennes, 2022. http://www.theses.fr/2022REN1S049

[22] O. Timothy O'Meara. *Introduction to quadratic forms*. Classics in Mathematics, Springer, 2000. Reprint of the 1973 edition.

[23] Frans Oort and Kenji Ueno. Principally polarized abelian varieties of dimension two or three are Jacobian varieties. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 20:377–381, 1973.

[24] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, Springer, 1994.

[25] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate texts in mathematics, Springer, 2009.

[26] Mark Watkins. Class numbers of imaginary quadratic fields. *Math. Comp.* 73(246):907–938, 2004.