Isogeny graphs, modular polynomials, and applications

Chloe Martindale

April 24, 2017

Abstract

Contents

1 The Theory of Canonical Lifts and Other Preliminaries **3**
- 1.1 Principally polarised abelian varieties . . . 3
- 1.2 Lifting ordinary abelian varieties over $\mathbb{F}_q$ to ideals . . . 4
- 1.3 Canonical lifts of polarised ordinary abelian varieties with fixed Frobenius . . . 5
- 1.4 The theory of canonical lifts . . . 7
  - 1.4.1 Serre-Tate lifts of ordinary abelian varieties over finite fields 7
  - 1.4.2 Deligne lifts of ordinary abelian varieties over finite fields 8
  - 1.4.3 Howe lifts of polarised ordinary abelian varieties over finite fields . . . 10
  - 1.4.4 Proof of the Fixed Frobenius Lifting Theorem . . . 11
- 1.5 Hilbert modular forms . . . 14
- 1.6 A useful property of principally polarised ideals . . . 18

2 Hilbert modular polynomials **20**
- 2.1 Introduction and statement of the results . . . 20
- 2.2 Defining RM isomorphism invariants over the complex numbers . 24
- 2.3 Proof of Theorem 2.1.4 . . . 25
- 2.4 Algorithm to compute a set of Hilbert modular polynomials . . . 28
  - 2.4.1 The algorithm . . . 28
- 2.5 Computing the RM isomorphism invariant for a given genus 2 curve . . . 31
- 2.6 Defining RM isomorphism invariants over a finite field . . . 33
- 2.7 Complexity and simplifications for genus 2 . . . 35

3 The structure of μ-isogeny graphs **39**
- 3.1 The Volcano Theorem . . . 39
  - 3.1.1 All μ-isogenies are ascending, descending or horizontal . . 46
  - 3.1.2 Principally polarised ideals are invertible . . . 47
  - 3.1.3 The action of the Shimura class group . . . 50
  - 3.1.4 Counting horizontal μ-isogenies . . . 52
  - 3.1.5 A construction of ascending μ-isogenies . . . 54
  - 3.1.6 The size of the Shimura class group . . . 55
- 3.2 Example computation of a μ-isogeny graph . . . 57

4 A new algorithm for computing Igusa class polynomials 59
4.1 The algorithm 61
4.1.1 Finding a starting curve 63
4.1.2 Finding an isogenous curve 64
4.1.3 Enumerating curves with the same endomorphism ring . . 66
4.1.4 Computing the Igusa-Hilbert class polynomials 69

Chapter 1

The Theory of Canonical Lifts and Other Preliminaries

In most of this thesis we will study principally polarised ordinary abelian varieties over $\mathbb{F}_q$, where q is a prime power. In this chapter, we specialise results of Deligne and Howe that allow us to work with ideals and elements of CM-fields instead of with varieties over $\mathbb{F}_q$. The proofs of these results are based on the lifting theorems of Lubin, Serre and Tate. The main theorem of this chapter, Theorem 1.3.11, is an equivalence of categories, so we now proceed by defining these two categories.

1.1 Principally polarised abelian varieties

Definition 1.1.1. An *abelian variety* A/k is a complete algebraic variety over k with a group law $m : \mathrm{A} \times \mathrm{A} \to \mathrm{A}$ such that m and the inverse map are both morphisms of varieties.

Remark 1.1.2. If A is an abelian variety defined over $\mathbb{C}$ then $\mathrm{A}(\mathbb{C})$ is complex analytically isomorphic to a complex torus of dimension g.

Definition 1.1.3. An *isogeny* is a morphism of abelian varieties that is finite as a morphism of varieties and surjective. The *degree* of an isogeny is its degree as a morphism of varieties.

Definition 1.1.4. For an abelian variety A over a field k, we define the *Picard group* of A, written as $\mathrm{Pic}(\mathrm{A})$, is the group of isomorphism classes of invertible sheaves of A.

Proposition 1.1.5. For an abelian variety A over a field k and a line bundle Ł on A, the map

$$\begin{array}{rccc} \phi_{\mathcal{L}}: & \mathrm{A} & \longrightarrow & \mathrm{Pic}(\mathrm{A}) \\ & x & \mapsto & [T_x^*\mathcal{L} \otimes \mathcal{L}^{-1}], \end{array}$$

where $[\cdot]$ denotes the isomorphism class of $\cdot$ in Pic(A), is a homomorphism.

Proof. See [**?**, Chapter I, Corollary 4]. □

Definition 1.1.6. We define $\mathrm{Pic}^0(\mathrm{A})$ to be the subgroup of Pic(A) consisting of line bundles $\mathcal{L}$ such that the morphism $\phi_{\mathcal{L}}$ is identically 0.

Proposition 1.1.7. The group $\mathrm{Pic}^0(\mathrm{A})$ carries a canonical algebraic structure with which it is an abelian variety over k, and if $\mathcal{L}$ is an ample line bundle on A, then the homomorphism $\phi_{\mathcal{L}} : \mathrm{A} \to \mathrm{Pic}^0(\mathrm{A})$ is a morphism of abelian varieties.

Proof. See [**?**, Chapter III, Corollary 5]. □

Definition 1.1.8. For an abelian variety A over a field k, we define the *dual abelian variety* to be $\mathrm{A}^\vee = \mathrm{Pic}^0(\mathrm{A})$, and we define a *polarisation* to be a morphism

$$\xi : \mathrm{A} \longrightarrow \mathrm{A}^\vee$$

such that there exists an ample line bundle $\mathcal{L}$ of A for which $\xi = \phi_{\mathcal{L}}$. We define a *principal polarisation* to be a polarisation that is an isomorphism.

1.2 Lifting ordinary abelian varieties over $\mathbb{F}_q$ to ideals

Definition 1.2.1. For q a prime power, write $\mathbf{Ord}_{\mathbb{F}_q}$ for the category of ordinary abelian varieties over $\mathbb{F}_q$. For a Weil q-number π, and a CM-field K such that $K = \mathbb{Q}(\pi)$, write $\chi(\pi)$ for the characteristic polynomial of π over $\mathbb{Q}$. For $\mathrm{A} \in \mathbf{Ord}_{\mathbb{F}_q}$, write $\chi(\mathrm{Frob}_q(\mathrm{A}))$ for the characteristic polynomial of the q-power Frobenius endomorphism of A. Then we define $\mathbf{Ord}_\pi$ to be the full subcategory of $\mathbf{Ord}_{\mathbb{F}_q}$ with objects given by

$$\{\mathrm{A} \in \mathbf{Ord}_{\mathbb{F}_q} : \chi(\mathrm{Frob}_q(\mathrm{A})) = \chi(\pi)\}.$$

Definition 1.2.2. Given a prime power q, a Weil q-number π, and a CM-field K such that $K = \mathbb{Q}(\pi)$, we define $\mathbf{Id}_\pi$ to be the category with objects given by fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideals, where for any objects $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathbf{Id}_\pi$, the morphisms in $\mathbf{Id}_\pi$ from $\mathfrak{a}$ to $\mathfrak{b}$ are given by

$$\mathrm{Hom}(\mathfrak{a}, \mathfrak{b}) = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathfrak{b}\}.$$

We will see in Theorem 1.3.11 that there is an equivalence of categories

$$\mathbf{Ord}_\pi \leftrightarrow \mathbf{Id}_\pi,$$

and that this functor satisfies some useful properties.

1.3 Canonical lifts of polarised ordinary abelian varieties with fixed Frobenius

Definition 1.3.1. Write $\mathbf{Ord}_{\mathbb{F}_q}$ for the category of ordinary abelian varieties over $\mathbb{F}_q$ of dimension g for some fixed $g \in \mathbb{Z}_{\geq >0}$. We define the category $\mathbf{POrd}_{\mathbb{F}_q}$ to be the category whose objects are pairs (A, ξ) where $\mathrm{A} \in \mathbf{Ord}_{\mathbb{F}_q}$ and $\xi : \mathrm{A} \to \mathrm{A}^\vee$ is a principal polarisation of A. We define a morphism in $\mathbf{POrd}_{\mathbb{F}_q}$ to be a map $f : (\mathrm{A}, \xi) \to (\mathrm{A}', \xi')$ such that f induces an isomorphism of abelian varieties $f : \mathrm{A} \to \mathrm{A}'$ for which the following diagram commutes:

$$\begin{array}{ccc} \mathrm{A} & \xrightarrow{f} & \mathrm{A}' \\ {\scriptstyle\xi}\downarrow & & \downarrow{\scriptstyle\xi'} \\ \mathrm{A}^\vee & \xleftarrow[f^\vee]{} & (\mathrm{A}')^\vee. \end{array}$$

Definition 1.3.2. For $(\mathrm{A}, \xi), (\mathrm{A}', \xi') \in \mathbf{POrd}_{\mathbb{F}_q}$ and $\mu \in \mathrm{End}_{\mathbf{Ord}_{\mathbb{F}_q}}(\mathrm{A})$, a *$\mu$-isogeny*

$$f : (\mathrm{A}, \xi) \longrightarrow (\mathrm{A}', \xi')$$

is defined to be a morphism $f : \mathrm{A} \to \mathrm{A}'$ in $\mathbf{Ord}_{\mathbb{F}_q}$ such that the diagram

$$\begin{array}{ccccc} \mathrm{A} & \xleftarrow{\mu} & \mathrm{A} & \xrightarrow{f} & \mathrm{A}' \\ & {\scriptstyle\xi}\searrow & & & \downarrow{\scriptstyle\xi'} \\ & & \mathrm{A}^\vee & \xleftarrow[f^\vee]{} & \mathrm{A}'^\vee \end{array}$$

commutes.

Remark 1.3.3. Note that the morphisms in $\mathbf{POrd}_{\mathbb{F}_q}$ are 1-isogenies.

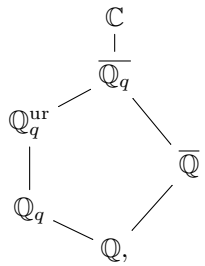
Definition 1.3.4. For q a prime power, a Weil q-number π, and a CM-field K such that $K = \mathbb{Q}(\pi)$, write $\chi(\pi)$ for the characteristic polynomial of π over $\mathbb{Q}$, and for $(\mathrm{A}, \xi) \in \mathbf{POrd}_{\mathbb{F}_q}$, write $\chi(\mathrm{Frob}_q(\mathrm{A}))$ for the characteristic polynomial of the q-power Frobenius endomorphism of A. Then we define $\mathbf{POrd}_\pi$ to be the full subcategory of $\mathbf{POrd}_{\mathbb{F}_q}$ with objects given by

$$\{(\mathrm{A}, \xi) \in \mathbf{POrd}_{\mathbb{F}_q} : \chi(\mathrm{Frob}_q(\mathrm{A})) = \chi(\pi)\}.$$

We now define, in several steps, the notion of a polarisation on objects in $\mathbf{Id}_\pi$ that will be functorially compatible with the notion of polarisation on objects in $\mathbf{Ord}_\pi$. Fix a prime power q, a Weil q-number π, and a CM-field K such that $K = \mathbb{Q}(\pi)$. We first show how to associate a CM-type of K to π, following Howe in [How95, Notation 4.6].

Let k be an algebraic closure of $\mathbb{F}_q$ and write $\mathbb{Q}_q^{\mathrm{ur}} = W(k)$, where $W(k)$ denotes the Witt vectors of k. Now fix one embedding $j : \mathbb{Q}_q^{\mathrm{ur}} \hookrightarrow \mathbb{C}$, and

identify $\mathbb{Q}_q^{\mathrm{ur}}$ with its image under j so that $\mathbb{Q}_q^{\mathrm{ur}} \subseteq \mathbb{C}$. Now, write $\overline{\mathbb{Q}_q}$ and $\overline{\mathbb{Q}}$ for the algebraic closure of $\mathbb{Q}_q^{\mathrm{ur}}$ and $\mathbb{Q}$ inside $\mathbb{C}$ respectively. We then obtain the following diagram of inclusions (some of which may depend on j):



so that in particular the q-adic valuation on $\mathbb{Q}_q^{\mathrm{ur}}$ extends uniquely via j to a q-adic valuation v_j on $\mathbb{C} \supseteq \overline{\mathbb{Q}_q} \supseteq \overline{\mathbb{Q}}$.

Definition 1.3.5. (c.f. [How95, Notation 4.6])
For a rational prime power q, fix $j : \mathbb{Q}_q^{\mathrm{ur}} \hookrightarrow \mathbb{C}$ as above and define v_j to be the q-adic valuation on $\overline{\mathbb{Q}} \subseteq \mathbb{C}$ obtained from j. Then given a CM-field K and an algebraic integer π such that $K = \mathbb{Q}(\pi)$ and $\pi\overline{\pi} = q$, we define the (π, j)*–CM-type of* K to be

$$\Phi_{\pi,j} := \{\phi : K \hookrightarrow \mathbb{C} : v_j(\phi(\pi)) > 0\}.$$

Definition 1.3.6. With notation as in Definition 1.3.5, for any $x \in K$, we say that x is $\Phi_{\pi,j}$–non-positive-imaginary if, for every $\phi \in \Phi_{\pi,j}$, we have that $\phi(x)/i \in \mathbb{R}_{\leq 0}$.

Definition 1.3.7. For an object $\mathfrak{a} \in \mathbf{Id}_\pi$, we define the *dual* of $\mathfrak{a}$ to be the fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideal

$$\mathfrak{a}^\vee = \{\alpha \in K : \mathrm{tr}(\alpha\bar{\mathfrak{a}}) \subseteq \mathbb{Z}\}.$$

For a morphism $\beta \in \mathrm{Hom}_{\mathbf{Id}_\pi}(\mathfrak{a}, \mathfrak{a}^\vee)$, we define β to be a *polarisation* if β is $\Phi_{\pi,j}$–non-positive-imaginary. If in addition $\beta\mathfrak{a} = \mathfrak{a}^\vee$, then we say that β is *principal*. For a morphism $\alpha \in \mathrm{Hom}_{\mathbf{Id}_\pi}(\mathfrak{a}, \mathfrak{b})$, we define the *dual* of α to be

$$\alpha^\vee = \overline{\alpha} \in \mathrm{Hom}_{\mathbf{Id}_\pi}(\mathfrak{b}^\vee, \mathfrak{a}^\vee),$$

where $\bar{\cdot}$ denotes complex conjugation.

Remark 1.3.8. Note that for any totally positive element μ of $\mathrm{End}(\mathfrak{a})$, if β is a polarisation of $\mathfrak{a}$ then $\mu\beta$ is also a polarisation of $\mathfrak{a}$.

Definition 1.3.9. Fix a prime power q, a Weil q-number π, and a CM-field K such that $K = \mathbb{Q}(\pi)$. We define the category $\mathbf{PId}_\pi$ to be the category with objects given by pairs $(\mathfrak{a}, \beta)$, where $\mathfrak{a} \in \mathbf{Id}_\pi$ and $\beta \in \mathrm{Hom}(\mathfrak{a}, \mathfrak{a}^\vee)$ is a principal polarisation of $\mathfrak{a}$. We define a morphism $(\mathfrak{a}, \beta) \to (\mathfrak{a}', \beta') \in \mathbf{PId}_\pi$ to be an isomorphism $\alpha \in \mathrm{Hom}(\mathfrak{a}, \mathfrak{a}')$ in $\mathbf{Id}_\pi$ such that

$$\beta = \overline{\alpha}\beta'\alpha.$$

Definition 1.3.10. For $(\mathfrak{a}, \beta), (\mathfrak{a}', \beta') \in \mathbf{PId}_\pi$ and $\mu \in \mathrm{End}(\mathfrak{a})$, a μ-isogeny

$$f : (\mathfrak{a}, \beta) \to (\mathfrak{a}', \beta')$$

is defined to be a morphism $\alpha \in \mathrm{Hom}(\mathfrak{a}, \mathfrak{a}')$ such that

$$\beta\mu = \overline{\alpha}\beta'\alpha.$$

Theorem 1.3.11. *(Fixed Frobenius Lifting Theorem)*
Fix a prime power q, a Weil q-number π, and a CM-field K such that $K = \mathbb{Q}(\pi)$. Then there exists an equivalence of categories

$$\mathbf{Ord}_\pi \leftrightarrow \mathbf{Id}_\pi$$

that preserves both the notion of polarisation and of μ-isogeny.

The remainder of this chapter is dedicated to defining the functor which defines this equivalence, and to showing how Theorem 1.3.11 follows from the work of Deligne and Howe in [Del69] and [How95] via the lifting theorems of Serre, Tate and Lubin.

1.4 The theory of canonical lifts

In order to write down the functor of Theorem 1.3.11, we require the notion of a 'Serre-Tate lift' of an ordinary abelian variety A over a field k of positive characteristic, and of a morphism of ordinary abelian varieties over k. This was first studied by Lubin, Serre, and Tate in a seminar, skeleton notes of which can be found at [LST64]. A simpler proof of their main lifting theorem was later found by Drinfeld and written down by Katz in [Kat, Chapter 1]. The machinery required to use this theorem to lift ordinary abelian varieties over $\mathbb{F}_q$ to abelian schemes over $\mathbb{Q}_q^{\mathrm{ur}}$ was written down by Messing in [Mes90]; the version of the lifting theorems that we state here are as stated by Messing.

1.4.1 Serre-Tate lifts of ordinary abelian varieties over finite fields

In this section we show how to lift an ordinary abelian varieties over a finite field k to an abelian schemes over the Witt vectors $W(k)$ of k; we first recall the definition of an abelian scheme.

Definition 1.4.1. For a scheme S, an *abelian scheme* over S is defined to be a proper smooth group S–scheme of which all fibres are geometrically connected.

Proposition 1.4.2. It is equivalent to define an abelian scheme to be a smooth group scheme over S of which all fibres are abelian varieties. In particular, if k is a field and A is an abelian $\mathrm{Spec}(k)$-scheme then A is an abelian variety.

Proof. See [Dol14]. □

Definition 1.4.3. Let R be a commutative ring and let S be a projective abelian scheme over R. Then we write $\mathrm{End}_{R\text{-gr}}(\mathrm{S})$ for the ring of endomorphisms of S in the category of R-group schemes.

Fix a perfect field k of characteristic $p > 0$, and write $W(k)$ for the ring of Witt vectors of k.

Theorem 1.4.4. *Let* A *be an ordinary abelian variety defined over* k*. Then, up to unique isomorphism, there is a projective abelian scheme* $\mathrm{B} \to W(k)$ *such that* $\mathrm{B} \times_{W(k)} k = \mathrm{A}$ *and the map* $\mathrm{End}_{W(k)\text{-gr}}(\mathrm{B}) \to \mathrm{End}_{k\text{-gr}}(\mathrm{A})$ *is bijective.*

Proof. See [Mes90, V.3.3]. □

Definition 1.4.5. For an ordinary abelian variety A defined over k, we define the the projective abelian $W(k)$-scheme satisfying the conditions of Theorem 1.4.4 to be the *Serre-Tate lift* of A.

Theorem 1.4.6. *Let* A *and* A' *be ordinary abelian varieties over* k *and let* B *and* B' *be the Serre-Tate lifts of* A *and* A' *respectively. Then the map*

$$\phi : \mathrm{Hom}(\mathrm{B}, \mathrm{B}') \longrightarrow \mathrm{Hom}(\mathrm{A}, \mathrm{A}')$$

is bijective.

Proof. See [Mes90, V.3.4]. □

Definition 1.4.7. Fix A, A', B, B' and ϕ as in Theorem 1.4.6. Then for $f \in \mathrm{Hom}(\mathrm{A}, \mathrm{A}')$, we define the *Serre-Tate lift* of f to be $\phi^{-1} f \in \mathrm{Hom}(\mathrm{B}, \mathrm{B}')$.

1.4.2 Deligne lifts of ordinary abelian varieties over finite fields

Following the work of Drinfeld, Lubin, Katz, Messing, Serre, and Tate giving Theorem 1.4.4 and Theorem 1.4.6, Deligne showed how to lift ordinary abelian varieties over finite fields to abelian varieties over $\mathbb{C}$, for which he defined the following category:

Definition 1.4.8. (c.f. [How95, Definition 4.1])
For a prime power q, we define the category $\mathbf{Del}_q$ to be the category whose objects are pairs (Λ, F), where the Λ are finitely generated free $\mathbb{Z}$-modules, and for a given Λ, the F are endomorphisms of Λ such that

- the endomorphism $F \otimes \mathbb{Q}$ of $\Lambda \otimes \mathbb{Q}$ is semi-simple, and its eigenvalues in $\mathbb{C}$ have magnitude $q^{1/2}$,
- at least half of the roots of the characteristic polynomial of F in $\overline{\mathbb{Q}}_q$, counting multiplicities, are p-adic units, and
- there is an endomorphism V of Λ such that $F \circ V = q$.

The morphisms

$$(\Lambda, F) \longrightarrow (\Lambda', F')$$

of $\mathbf{Del}_q$ are given by homomorphisms $\varphi : \Lambda \longrightarrow \Lambda'$ of $\mathbb{Z}$-modules such that $\varphi \circ F = F' \circ \varphi$.

This allows us to state Deligne's lifting theorem:

Theorem 1.4.9. *(Deligne's lifting theorem)*
For a prime power q, fix an embedding $j : \mathbb{Q}_q^{\mathrm{ur}} \hookrightarrow \mathbb{C}$. Let $\mathbf{Ord}_{\mathbb{F}_q}$ be the category of ordinary abelian varieties A over $\mathbb{F}_q$, and for an object A in $\mathbf{Ord}_{\mathbb{F}_q}$, let $\mathrm{B} \to \mathbb{Q}_q^{\mathrm{ur}}$ be the Serre-Tate lift of $\mathrm{A} \times \overline{\mathbb{F}_q}$. Define

$$T : \mathrm{A} \mapsto H_1(\mathrm{B} \times_j \mathbb{C}, \mathbb{Z}).$$

Let $\mathrm{Frob}_q(\mathrm{A})$ be the q-power Frobenius endomorphism on A, let $\mathrm{Frob}_q(\mathrm{B})$ be its Serre-Tate lift, and let $\overline{\mathrm{Frob}_q(\mathrm{B})}$ be the endomorphism induced by $\mathrm{Frob}_q(\mathrm{B}) \times_j \mathbb{C}$ on $T(\mathrm{A})$. Then the functor defined by

$$\begin{array}{ccc} \mathbf{Ord}_{\mathbb{F}_q} & \longrightarrow & \mathbf{Del}_q \\ \mathrm{A} & \mapsto & (T(\mathrm{A}), \overline{\mathrm{Frob}_q(\mathrm{B})}) \end{array}$$

is an equivalence of categories.

Proof. See [Del69, Théorème 7]. □

We will in fact only use a special case of Deligne's lifting theorem, stated in Corollary 1.4.11.

Definition 1.4.10. For a prime power q, a non-negative integer g, an algebraic integer π, and a CM-field K of degree g over $\mathbb{Q}$ such that $K = \mathbb{Q}(\pi)$, where $q = \pi\overline{\pi}$, we define the category $\mathbf{Mod}_\pi$ to be the category of $\mathbb{Z}[\pi, \overline{\pi}]$-modules that are free of rank $2g$ over $\mathbb{Z}$.

Corollary 1.4.11. For a prime power q, an algebraic integer π, and a CM-field K such that $K = \mathbb{Q}(\pi)$ and $q = \pi\overline{\pi}$, define $\mathbf{Ord}_\pi$ as in Definition 1.2.1 and $\mathbf{Mod}_\pi$ as in Definition 1.4.10. Then the functor of Theorem 1.4.9 defines an equivalence of categories

$$\begin{array}{ccc} \mathbf{Ord}_\pi & \longrightarrow & \mathbf{Mod}_\pi \\ \mathrm{A} & \mapsto & T(\mathrm{A}). \end{array}$$

Proof. First view $\mathbf{Mod}_\pi$ as a subcategory of $\mathbf{Del}_q$ by viewing a $\mathbb{Z}[\pi, \overline{\pi}]$-module M as a pair (M, F) where F is the action of π. Note that the Verschiebung V is the action of $\overline{\pi}$, and that $\mathbf{Mod}_\pi$ is exactly the full subcategory of pairs (Λ, F) for which the characteristic of the Frobenius F is exactly that characteristic polynomial of π over $\mathbb{Q}$. The result then follows from Theorem 1.4.9. □

1.4.3 Howe lifts of polarised ordinary abelian varieties over finite fields

Write $\mathbf{POrd}_{\mathbb{F}_q}$ for the category of principally polarised ordinary abelian varieties over $\mathbb{F}_q$, as defined in Definition 1.3.1. In [How95], Howe gave a notion of polarisation on the objects of $\mathbf{Del}_q$ which is compatible with the notion of polarisation in $\mathbf{Ord}_{\mathbb{F}_q}$ under the functor given in Theorem 1.4.9; we state in Theorem 1.4.19 the special case of Howe's lifting theorem, [How95, Proposition 4.9], that we need to prove Theorem 1.3.11. We first define polarisations of objects in $\mathbf{Mod}_\pi$, following Howe.

Definition 1.4.12. For an algebraic integer π such that π generates a CM-field over $\mathbb{Q}$ and $\pi\overline{\pi} = q$ is a rational prime power, if $\Lambda \in \mathbf{Mod}_\pi$ then we define the *dual* of Λ to be

$$\Lambda^\vee = \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z})$$

viewed as a $\mathbb{Z}[\pi, \overline{\pi}]$-module via

$$\begin{array}{ccc} \mathbb{Z}[\pi,\overline{\pi}] \times \Lambda^\vee & \longrightarrow & \Lambda^\vee \\ (r, \lambda \mapsto f(\lambda)) & \mapsto & (\lambda \mapsto f(\overline{r}\lambda)). \end{array}$$

Then in particular, $\Lambda^\vee \in \mathbf{Mod}_\pi$.

Definition 1.4.13. If R is a ring with an involution

$$\begin{array}{ccc} R & \longrightarrow & R \\ r & \mapsto & \overline{r}, \end{array}$$

M and N are R-modules, and f is a R-bilinear form

$$f : M \times M \longrightarrow N,$$

then we define f to be *R–semi-balanced* if for every $r \in R$ and $\ell, m \in M$, we have that

$$f(r\ell, m) = f(\ell, \overline{r}m).$$

If M is an R-module and N is an abelian group, then we define a R bilinear form

$$f : M \times M \longrightarrow N$$

to be *R–sesquilinear* if for every $r \in R$ and $\ell, m \in M$, we have that

$$f(r\ell, m) = rf(\ell, m) = f(\ell, \overline{r}m).$$

Definition 1.4.14. (c.f. [How95, p. 2370])
For an algebraic integer π such that π generates a CM-field over $\mathbb{Q}$ and $\pi\overline{\pi} = q$ is a rational prime power, if $\Lambda \in \mathbf{Mod}_\pi$ and $\zeta \in \mathrm{Hom}_{\mathbf{Mod}_\pi}(\Lambda, \Lambda^\vee)$ then we define the *$\mathbb{Z}$-bilinear form associated to ζ* to be

$$\begin{array}{rccc} b: & \Lambda \times \Lambda & \longrightarrow & \mathbb{Z} \\ & (s,t) & \mapsto & \zeta(s)t. \end{array}$$

One can check that this is a non-degenerate $\mathbb{Z}[\pi, \overline{\pi}]$–semi-balanced form.

Proposition 1.4.15. For an order $\mathcal{O}$ in a number field K, given a non-degenerate $\mathcal{O}$–semi-balanced form $b : \Lambda \times \Lambda \to \mathbb{Z}$, there exists a unique non-degenerate K-sesquilinear form $S : (\Lambda \otimes \mathbb{Q}) \times (\Lambda \otimes \mathbb{Q}) \to K$ such that $b \otimes \mathbb{Q} = \mathrm{tr}_{K/\mathbb{Q}} \circ S$.

Proof. See [Knu91, Theorem I.7.4.1, p.44]. □

Definition 1.4.16. For $\Lambda \in \mathbf{Mod}_\pi$ and $\zeta \in \mathrm{Hom}_{\mathbf{Mod}_\pi}(\Lambda, \Lambda^\vee)$, let $b : \Lambda \times \Lambda \to \mathbb{Z}$ be the $\mathbb{Z}$-bilinear form associated to ζ. We define the *K-sesquilinear form associated to* Λ to be the unique non-degenerate K-sesquilinear form $S : (\Lambda \otimes \mathbb{Q}) \times (\Lambda \otimes \mathbb{Q}) \to K$ such that $b \otimes \mathbb{Q} = \mathrm{tr}_{K/\mathbb{Q}} \circ S$.

Remark 1.4.17. For every $\Lambda \in \mathbf{Mod}_\pi$, given a non-degenerate $\mathbb{Z}[\pi, \overline{\pi}]$-semi-balanced form $b : \Lambda \times \Lambda \to \mathbb{Z}$ and a non-degenerate K-sesquilinear form $S : (\Lambda \otimes \mathbb{Q}) \times (\Lambda \otimes \mathbb{Q}) \to K$ such that $b \otimes \mathbb{Q} = \mathrm{tr}_{K/\mathbb{Q}} \circ S$, there is a unique morphism $\zeta \in \mathrm{Hom}(\Lambda, \Lambda^\vee)$ for which the associated $\mathbb{Z}$-bilinear form is b. For more details, see [How95, p. 2370].

Definition 1.4.18. (c.f. [How95, Definition 4.8])
Fix a Weil q-number π and a CM-field K such that $K = \mathbb{Q}(\pi)$, and fix an embedding $j : \mathbb{Q}_q^{\mathrm{ur}} \hookrightarrow \mathbb{C}$. Recall the definition of the CM-type $\Phi_{\pi,j}$ of K from Definition 1.3.5, and recall the definition of $\Phi_{\pi,j}$–non-positive-imaginary from Definition 1.3.6. For $\Lambda \in \mathbf{Mod}_\pi$, we define a *$j$-polarisation of* Λ to be a morphism

$$\zeta : \Lambda \longrightarrow \Lambda^\vee$$

such that the sesquilinear form S associated to ζ is skew-Hermitian and for every $\lambda \in \Lambda$, we have that $S(\lambda, \lambda)$ is $\Phi_{\pi,j}$–non-positive.

The following theorem, a special case of Howe's lifting theorem in [How95, Proposition 4.9], shows that this definition of polarisation is what we should use if we wish to study ordinary abelian varieties over finite fields.

Theorem 1.4.19. *For an abelian variety* $\mathrm{A} \in \mathbf{Ord}_\pi$ *with dual abelian variety* $\mathrm{A}^\vee \in \mathbf{Ord}_\pi$ *and an isogeny* $\xi : \mathrm{A} \to \mathrm{A}^\vee \in \mathbf{Ord}_\pi$*, let* Λ*,* $\Lambda^\vee \in \mathbf{Mod}_\pi$ *and* $\alpha \in \mathrm{Hom}(\Lambda, \Lambda^\vee)$ *be the images under the functor of Corollary 1.4.11 of* A*,* $\mathrm{A}^\vee$ *and* ξ *respectively. Let* $j : \mathbb{Q}_q^{\mathrm{ur}} \hookrightarrow \mathbb{C}$ *be the embedding on which the functor of Corollary 1.4.11 depends. Then* α *is a* j*-polarisation if and only if* ξ *is a polarisation.*

Proof. See [How95, Proposition 4.9]. See Corollary 1.4.26 below for clarification on the first step of the proof. □

1.4.4 Proof of the Fixed Frobenius Lifting Theorem

The Fixed Frobenius Lifting Theorem, Theorem 1.3.11, is a consequence of Howe's lifting theorem Theorem 1.4.19. We only need to show that there is a functor defining an equivalence of categories between $\mathbf{Mod}_\pi$ of $\mathbb{Z}[\pi, \overline{\pi}]$-modules and the category $\mathbf{Id}_\pi$ of fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideals that preserves the notions of polarisation and of μ-isogeny.

Definition 1.4.20. We define a *μ-isogeny* of j-polarised objects in $\mathbf{Mod}_\pi$ to be a morphism that is equivalent under the functor of Theorem 1.4.9 to a μ-isogeny of polarised ordinary abelian varieties in $\mathbf{Ord}_\pi$.

Proof of Theorem 1.3.11. Using Theorem 1.4.19, it only remains to show that the categories $\mathbf{Mod}_\pi$ and $\mathbf{Id}_\pi$ are equivalent, and that the functor defining this equivalence also preserves the notion of polarisation and of μ-isogeny. For $\Lambda \in \mathbf{Mod}_\pi$ with j-polarisation ζ, choose an isomorphism $\varphi : \Lambda \otimes \mathbb{Q} \to K$. Then $\varphi(\Lambda)$ and $\varphi(\Lambda^\vee)$ are fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideals, and $\zeta : \Lambda \to \Lambda^\vee$ defines a morphism $\varphi(\zeta) : \varphi(\Lambda) \to \varphi(\Lambda^\vee)$. Write β_ζ for the element of K such that

$$\begin{array}{rccc} \varphi(\zeta): & \varphi(\Lambda) & \longrightarrow & \varphi(\Lambda^\vee) \\ & x & \mapsto & \beta_\zeta x. \end{array}$$

The functor

$$\begin{array}{rccc} F: & \mathbf{Mod}_\pi & \longrightarrow & \mathbf{Id}_\pi \\ & \Lambda & \mapsto & \varphi(\Lambda) \end{array}$$

is clearly an equivalence of categories. We claim further that:

1. β_ζ is a polarisation of $\varphi(\Lambda)$.
2. F maps μ-isogenies to μ-isogenies.

To prove (1), we first show that under F, the unique sesquilinear form S associated to ζ becomes

$$\begin{array}{rccc} S: & K \times K & \longrightarrow & K \\ & (a, b) & \mapsto & \beta_\zeta a\overline{b}. \end{array}$$

To see this, consider that for every $a \in \varphi(\Lambda)$, we have that $\beta_\zeta a \in \varphi(\Lambda^\vee) = \mathrm{Hom}(\varphi(\Lambda), \mathbb{Z})$, and hence

$$\mathrm{tr}_{K/\mathbb{Q}}(S(a, \cdot)) = (\zeta a)(\cdot).$$

Therefore it suffices to show that $S(a, \cdot) = \beta_\zeta a\overline{\cdot}$. But

$$\begin{array}{ccc} K \times K & \longrightarrow & K \\ (a, b) & \mapsto & \beta_\zeta a\overline{b} \end{array}$$

is non-degenerate and K-sesquilinear, hence by Proposition 1.4.15, this is exactly S. Then in particular, we see that

$$\varphi(\Lambda)^\vee = \mathrm{Hom}(\varphi(\Lambda), \mathbb{Z}) \subseteq \{\alpha \in K : \mathrm{tr}(\alpha\overline{\varphi(\Lambda)}) \subseteq \mathbb{Z}\}.$$

The other inclusion is clear, so we get that

$$\varphi(\Lambda)^\vee = \{\alpha \in K : \mathrm{tr}(\alpha\overline{\varphi(\Lambda)}) \subseteq \mathbb{Z}\},$$

and hence β_ζ is a polarisation of $\varphi(\Lambda)$. For (2), we now only need to show that for every Λ, $\Lambda' \in \mathbf{Mod}_\pi$ with principal j-polarisations ζ and ζ' respectively, if there exists a μ-isogeny

$$f : (\Lambda, \zeta) \longrightarrow (\Lambda', \zeta'),$$

then there exists $\alpha \in K$ such that the maps on modules $f : \Lambda \to \Lambda'$ and $f^\vee : \Lambda'^\vee \to \Lambda^\vee$ defined by f map under F to α and $\overline{\alpha}$. But this follows from the fact that for $(\mathfrak{a}, \zeta) \in \mathbf{PId}_\pi$, we have

$$\mathfrak{a}^\vee = \{\alpha \in K : \mathrm{tr}(\alpha\overline{\mathfrak{a}}) \subseteq \mathbb{Z}\}.$$

□

Definition 1.4.21. For a projective abelian scheme $\mathrm{A} \to S$, we define its *dual abelian scheme* $\mathrm{A}^\vee$ to be the projective abelian S-scheme

$$\mathrm{A}^\vee := \mathbf{Pic}^0_{\mathrm{A}/S}.$$

We now define polarisations of abelian schemes, following [MFK94, Chapter 6, Section 2].

Definition 1.4.22. For a projective abelian scheme $\mathrm{A} \to S$, define the maps

$$\mu : \mathrm{A} \times_S \mathrm{A} \to \mathrm{A}, \quad p_1 : \mathrm{A} \times_S \mathrm{A} \to \mathrm{A}, \quad \text{and } p_2 : \mathrm{A} \times_S \mathrm{A} \to \mathrm{A}$$

to be the group law on A, projection onto the first coordinate, and projection onto the second coordinate respectively. Then for any invertible sheaf $\mathcal{L}$ on A, define the invertible sheaf

$$\mathcal{F}_\mathcal{L} := \mu^*(\mathcal{L}) \otimes p_1^*(\mathcal{L})^{-1} \otimes p_2^*(\mathcal{L})^{-1}$$

on $\mathrm{A} \times_S \mathrm{A}$. Now regarding $\mathrm{A} \times_S \mathrm{A}$ as a scheme over A via p_1, the class of $\mathcal{F}_\mathcal{L}$ in $\mathrm{Pic}(\mathrm{A} \times_S \mathrm{A})/\mathrm{Pic}(\mathrm{A})$ defines a morphism

$$\phi_\mathcal{L} : \mathrm{A} \longrightarrow \mathrm{Pic}(\mathrm{A}/S)$$

by representability of $\mathrm{Pic}_{\mathrm{A}/S}$. Furthermore, by Corollary 6.4 and the preamble to Chapter 6, Section 2 in [MFK94], we have that $\phi_\mathcal{L}$ is in fact a homomorphism

$$\phi_\mathcal{L} : \mathrm{A} \longrightarrow \mathrm{A}^\vee.$$

Remark 1.4.23. If $\mathrm{A} \to k$ is an abelian scheme over a field k, that is, an abelian variety, and Ł is an ample line bundle of A then the morphism $\phi_\mathcal{L}$ defined in Definition 1.4.22 is the same morphism that we defined in Proposition 1.1.5. For a proof, see [**?**, Theorem, p.125].

Definition 1.4.24. For a projective abelian scheme $\mathrm{A} \to S$, we define a *polarisation* of A to be a homomorphism

$$\xi : \mathrm{A} \longrightarrow \mathrm{A}^\vee$$

such that for each geometric point $\overline{s}$ of S, there exists an ample invertible sheaf $\mathcal{L}_{\overline{s}}$ on $\mathrm{A}_{\overline{s}}$ (the fibre at $\overline{s}$) such that $\phi_{\mathcal{L}_{\overline{s}}} = \xi_{\overline{s}}$, where $\phi_{\mathcal{L}_{\overline{s}}}$ is as defined in Definition 1.4.22. If a polarisation ξ is an isomorphism, then we say that it is *principal*.

Theorem 1.4.25. *For a field k, algebraic over $\mathbb{F}_p$, and for an ordinary abelian variety A defined over k with dual abelian variety $\mathrm{A}^\vee$, let $\xi : \mathrm{A} \longrightarrow \mathrm{A}^\vee$ be a polarisation of A, let $\mathrm{B} \to W(\overline{\mathbb{F}}_p)$ be the Serre-Tate lift of $\mathrm{A} \times \overline{\mathbb{F}}_p$, and let ψ be the Serre-Tate lift of the morphism $\xi \times \overline{\mathbb{F}_p}$. Then we have the following:*

1. *B is projective.*
2. *The dual abelian scheme of B is the Serre-Tate lift of $\mathrm{A}^\vee \times \overline{\mathbb{F}}_p$.*
3. *ψ defines a polarisation on the generic point of B.*

Proof. Noting that $W(\overline{\mathbb{F}_p})$ is the ring of integers of $\mathbb{Q}_p^{\mathrm{ur}}$, (1) follows immediately from [Ray70, Théorème XI.1.4]. (2) is in the proof of [Mes90, Chapter V, Theorem 3.3] (this theorem was already stated as Theorem 1.4.4). (3) is proven in [FC90, p.6 point (b)]. □

Corollary 1.4.26. For A, B, and ξ as in Theorem 1.4.25 and an embedding $j : \mathbb{Q}_p^{\mathrm{ur}} \hookrightarrow \mathbb{C}$, define

$$\mathrm{A}_{\mathbb{C}} := (\mathrm{B} \times \mathbb{Q}_q^{\mathrm{ur}}) \times_j \mathbb{C} \quad \text{and} \quad (\mathrm{A}^\vee)_{\mathbb{C}} := (\mathrm{B}^\vee \times \mathbb{Q}_q^{\mathrm{ur}}) \times_j \mathbb{C}.$$

Then

1. $(\mathrm{A}^\vee)_{\mathbb{C}} = (\mathrm{A}_{\mathbb{C}})^\vee$.
2. $\mathrm{End}(\mathrm{A}_{\mathbb{C}}) = \mathrm{End}(\mathrm{A})$ and $\mathrm{End}(\mathrm{A}_{\mathbb{C}}^\vee) = \mathrm{End}(\mathrm{A}^\vee)$.
3. There is a canonical isogeny $\xi_{\mathbb{C}}$ lifting ξ which defines a polarisation of $\mathrm{A}_{\mathbb{C}}$.

Proof. (1) follows from part (2) in Theorem 1.4.25 and the definition of the dual abelian scheme (see Definition 1.4.21). (2) follows from the definition of Serre-Tate lift. For (3), let ψ be the Serre-Tate lift of ξ and define $\xi_{\mathbb{C}} = (\psi \times \mathbb{Q}_p^{\mathrm{ur}}) \times_j \mathbb{C}$, which by (3) in Theorem 1.4.25 defines a polarisation on $\mathrm{A}_{\mathbb{C}}$. □

1.5 Hilbert modular forms

Definition 1.5.1. Let K_0 be a totally real number field of degree g over $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_0}$. Let $\mathcal{N}$ be an invertible $\mathcal{O}_{K_0}$-ideal. Then the matrix group $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{N})$ is defined by

$$\{A \in \mathrm{SL}_2(K_0) : \forall x \in \mathcal{O}_{K_0} \oplus \mathcal{N},\ Ax \in \mathcal{O}_{K_0} \oplus \mathcal{N}\}.$$

This can be written explicitly as

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(K_0) : a, d \in \mathcal{O}_{K_0},\ b \in \mathcal{N},\ c \in \mathcal{N}^{-1} \right\}.$$

We look now at the case in which the abelian varieties we are considering are defined over $\mathbb{C}$ and have *maximal real multiplication*, that is, the real part of the endomorphism ring is maximal.

Definition 1.5.2. Let K_0 be a totally real number field of degree g over $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_0}$, and define $\mathbf{Ord}_{k,g}$ to be the category of abelian varieties over k of dimension g. We define the objects of the category $\mathbf{POrd}_{k,K_0}$ by triples (A, ξ, ι), where $\mathrm{A} \in \mathbf{Ord}_{k,g}$, $\xi : \mathrm{A} \to \mathrm{A}^\vee$ is a principal polarisation of A, and $\iota : \mathcal{O}_{K_0} \hookrightarrow \mathrm{End}(\mathrm{A})$ is an embedding that is stable under the Rosati involution. A morphism in $\mathbf{POrd}_{k,K_0}$ between two objects (A, ξ, ι) and $(\mathrm{A}', \xi', \iota') \in \mathbf{POrd}_{k,K_0}$ is given by an isomorphism

$$f : \mathrm{A} \longrightarrow \mathrm{A}'$$

in $\mathbf{Ord}_{k,g}$ that makes the diagram

$$\begin{array}{ccc} \mathrm{A} & \xrightarrow{f} & \mathrm{A}' \\ {\scriptstyle\xi}\downarrow & & \downarrow{\scriptstyle\xi'} \\ \mathrm{A}^\vee & \xleftarrow[f^\vee]{} & \mathrm{A}'^\vee \end{array}$$

commute, and furthermore the map induced by f on endomorphism algebras makes the diagram

$$\begin{array}{ccc} \mathrm{End}(\mathrm{A}) \otimes \mathbb{Q} & \xrightarrow{f} & \mathrm{End}(\mathrm{A}') \otimes \mathbb{Q} \\ {\scriptstyle\iota}\uparrow & \nearrow_{\iota'} & \\ K_0 & & \end{array}$$

commute.

Definition 1.5.3. For $(\mathrm{A}, \xi, \iota), (\mathrm{A}', \xi', \iota') \in \mathbf{POrd}_{k,K_0}$ and $\mu \in \mathrm{End}(\mathrm{A})$, we define a *$\mu$-isogeny* $f : (\mathrm{A}, \xi, \iota) \to (\mathrm{A}', \xi', \iota')$ to be a morphism $f : \mathrm{A} \to \mathrm{A}'$ in $\mathbf{Ord}_{k,g}$ such that the diagram

$$\begin{array}{ccccc} \mathrm{A} & \xleftarrow{\mu} & \mathrm{A} & \xrightarrow{f} & \mathrm{A}' \\ & \searrow^{\xi} & & & \downarrow{\scriptstyle\xi'} \\ & & \mathrm{A}^\vee & \xleftarrow[f^\vee]{} & \mathrm{A}'^\vee \end{array}$$

commutes and the map induced by f on endomorphism algebras makes the diagram

$$\begin{array}{ccc} \mathrm{End}(\mathrm{A}) \otimes \mathbb{Q} & \xrightarrow{f} & \mathrm{End}(\mathrm{A}') \otimes \mathbb{Q} \\ {\scriptstyle\iota}\uparrow & \nearrow_{\iota'} & \\ K_0 & & \end{array}$$

commute.

Theorem 1.5.4. *For a prime power q, a Weil q-number π, and a CM-field $K = \mathbb{Q}(\pi)$ of degree g over $\mathbb{Q}$ with maximal totally real subfield K_0, define $\mathbf{Id}_{\pi,K_0}$ to be the full subcategory of the category $\mathbf{Id}_\pi$ of Definition 1.2.2 with objects given by*

$$\{\mathfrak{a} \in \mathbf{Id}_\pi : \mathcal{O}_{K_0} \subseteq \mathrm{End}(\mathfrak{a})\}.$$

Then the fully faithful functor

$$\begin{array}{rccc} F_\pi : & \mathbf{Id}_{\pi,K_0} & \to & \mathbf{Ord}_{\mathbb{C},K_0} \\ & \mathfrak{a} & \mapsto & \mathbb{C}^g/\Phi_{\pi,j}(\mathfrak{a}) \end{array}$$

preserves the notions of polarisation and of μ-isogeny, where $j : \mathbb{Q}_q^{\mathrm{ur}} \hookrightarrow \mathbb{C}$ is am embedding and $\Phi_{\pi,j}$ is the CM-type of K that we defined in **??**. *Furthermore, for every principally polarised complex abelian variety $(\mathrm{A}, \xi) \in \mathbf{POrd}_{\mathbb{C},K_0}$, there exists a prime power q, a Weil q-number $\pi \in \mathrm{End}(\mathrm{A}) \otimes \mathbb{Q}$, and $(\mathfrak{a}, \beta) \in \mathbf{PId}_{\pi,K_0}$ such that $\mathrm{A} = F_\pi(\mathfrak{a})$ and $\xi = F_\pi(\beta)$.*

Proof. Define $\mathbf{Ord}_{\pi,K_0}$ to be the full subcategory of $\mathbf{Ord}_\pi$ such that for every $\mathrm{A} \in \mathbf{Ord}_\pi$, we have that $\mathcal{O}_{K_0} \subseteq \mathrm{End}(\mathrm{A})$. Fix an embedding $j : \mathbb{Q}_q^{ur} \hookrightarrow \mathbb{C}$, where $q = \pi\overline{\pi}$, and let B be the Serre-Tate lift of $\mathrm{A} \times \overline{\mathbb{F}_q}$. Then write $\mathrm{A}_\mathbb{C} := (\mathrm{B} \times \mathbb{Q}_q^{\mathrm{ur}}) \times_j \mathbb{C}$, and write $\xi_\mathbb{C}$ for the polarisation of $\mathrm{A}_\mathbb{C}$ lifting ξ that was given in Corollary 1.4.26. Write F (resp. V) for the Serre-Tate lift of the Frobenius (resp. Verschiebung) morphism of $\mathrm{A} \times \overline{\mathbb{F}_q}$, and define the embedding ι_π by

$$\begin{array}{rccc} \iota_\pi : & \mathcal{O}_{K_0} & \hookrightarrow & \mathrm{End}(\mathrm{A}_\mathbb{C}) \\ & \pi + \overline{\pi} & \mapsto & F \times_j \mathbb{C} + V \times_j \mathbb{C}. \end{array}$$

Now define Ψ to be the fully faithful functor

$$\begin{array}{rccc} \Psi : & \mathbf{Ord}_{\pi,K_0} & \longrightarrow & \mathbf{Ord}_{\mathbb{C},K_0} \\ & \mathrm{A} & \mapsto & (\mathrm{A}_\mathbb{C}, \iota_\pi) \end{array}.$$

This sends a polarisation ξ of A to the polarisation $\xi_\mathbb{C}$ of $\mathrm{A}_\mathbb{C}$ that we defined in Corollary 1.4.26 as the choice is canonical. So suppose now that $\mathrm{A} \in \mathbf{Ord}_{\mathbb{C},K_0}$. As all complex abelian varieties are ordinary, we know that there exists a CM-field K with maximal totally real subfield for which $\mathrm{End}(\mathrm{A}) \otimes \mathbb{Q} = K$, and hence that there exists an algebraic integer $\pi \in K$ such that $H_1(\mathrm{A}(\mathbb{C}), \mathbb{Z}) \in \mathbf{Mod}_\pi$. The result now follows from Theorem 1.3.11. □

We will rely heavily on the 'moduli interpretation' in the complex setting, which is given in the following lemma.

Lemma 1.5.5. Let K_0 be a totally real number field of degree g over $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_0}$. Write $K_0 \otimes \mathbb{H}$ for the set of elements of $K_0 \otimes \mathbb{C}$ with totally positive imaginary part, and write $\mathcal{O}_{K_0}^\vee$ for the trace dual of $\mathcal{O}_{K_0}$. Then there is a correspondence

$$\begin{array}{c} \left\{(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{C},K_0} : \exists \phi : H_1(\mathrm{A}(\mathbb{C}), \mathbb{Z}) \tilde{\to} \mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee\right\} \\ \updownarrow \\ \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee) \backslash (K_0 \otimes \mathbb{H}) \end{array}$$

where $\tau \in K_0 \otimes \mathbb{H}$ is given by $\phi^{-1}(1,0)/\phi^{-1}(0,1)$, and the action of $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$ on $F \otimes \mathbb{H}$ is given by Möbius transformations.

Proof. See [vdG88, Chapter IX, Section 1]. □

Definition 1.5.6. Let κ be an integer, and let τ be in $K_0 \otimes \mathbb{H}$, i.e., an element of $K_0 \otimes \mathbb{C}$ with totally positive imaginary part. Let the the group of 2×2 matrices with entries in K_0 and whose elements have totally positive determinant be denoted by $\mathrm{GL}_2(K_0)^+$. Then the *weight function* w_κ is defined by

$$\begin{array}{rccc} w_\kappa: & \mathrm{GL}_2(K_0)^+ \times K_0 \otimes \mathbb{H} & \longrightarrow & \mathbb{C} \\ & (M,\tau) & \mapsto & \left(\mathrm{N}_{K_0/\mathbb{Q}}(\det(M))^{-1/2}\mathrm{N}_{(K_0\otimes\mathbb{C})/\mathbb{C}}(c\tau+d)\right)^\kappa, \end{array}$$

where we choose the positive square root.

Definition 1.5.7. Let $\mathrm{GL}_2(K_0)^+$ and $K_0 \otimes \mathbb{H}$ be as in Definition 1.5.6. Let M be any matrix in $\mathrm{GL}_2(K_0)^+$, and let $f : K_0 \otimes \mathbb{H} \to \mathbb{C}$ be a holomorphic map. Then we define $f|_{[M]_\kappa}$ by

$$\begin{array}{rccc} f|_{[M]_\kappa}: & K_0 \otimes \mathbb{H} & \to & \mathbb{C} \\ & \tau & \mapsto & w_\kappa(M,\tau)^{-1} f(M\tau). \end{array}$$

It is straightforward to check that for $M, N \in \mathrm{GL}_2(K_0)^+$, we have that

$$(f|_{[M]_\kappa})|_{[N]_\kappa} = f|_{[MN]_\kappa}.$$

Definition 1.5.8. Let $g \geq 2$ and let κ be a non-negative integer. Let $\mathrm{GL}_2(K_0)^+$ and $K_0 \otimes \mathbb{H}$ be as in Definition 1.5.6. Let Γ be a congruence subgroup of $\mathrm{GL}_2(K_0)^+$. We say that $f : K_0 \otimes \mathbb{H} \to \mathbb{C}$ is a *Hilbert modular form* of weight κ for Γ if and only if it is holomorphic and for all $M \in \Gamma$ and $\tau \in K_0 \otimes \mathbb{H}$, we have that

$$f|_{[M]_\kappa}(\tau) = f(\tau).$$

From this point on, if f is a Hilbert modular form of weight κ, then for $M \in \mathrm{GL}_2(K_0)^+$ we will write $f|_M$ for $f|_{[M]_\kappa}$.

Definition 1.5.9. With notation as in Definition 1.5.8, if $\varphi = f/g$ is the quotient of Hilbert modular forms for Γ of equal weight, then we say that φ is a *Hilbert modular function* for Γ.

Definition 1.5.10. Define σ to be a generator of $\mathrm{Gal}((K_0 \otimes \mathbb{C})/\mathbb{C})$. Then for $f \in \mathcal{M}_{K_0,k}$, if for every $\tau \in K_0 \otimes \mathbb{H}$ we have

$$f(\tau) = f(\sigma(\tau)),$$

we say that f is *symmetric*.

Definition 1.5.11. Let $\mathcal{O}_{K_0}^\vee$ be the trace dual of $\mathcal{O}_{K_0}$. We define $\mathcal{M}_{K_0,\kappa}$ to be the $\mathbb{C}$-algebra of Hilbert modular forms for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$ of weight κ, and we define $\mathcal{M}_{K_0} = \oplus_\kappa \mathcal{M}_{K_0,\kappa}$ to be the graded ring of all Hilbert modular forms for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$.

Theorem 1.5.12. *(Baily-Borel Theorem)*
Let $\mathcal{M}_{K_0}$ be the graded ring of Hilbert modular forms for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$. Then the normal complex analytic space of $\mathrm{Proj}(\mathcal{M}_{K_0})$ is a compactification of V.

Proof. See [vdG88, II.7.1]. □

Definition 1.5.13. We define the *Hilbert modular variety* $\overline{V}$ to be the normal complex analytic space of $\mathrm{Proj}(\mathcal{M}_{K_0})$. We will also refer to this as the *Baily-Borel compactification of V*.

Proposition 1.5.14. (Rapoport)
$\mathcal{M}_{K_0,\kappa}(\mathbb{Z})$ is a finitely generated $\mathbb{Z}$-module.

Proof. See [Rap78, Proposition 6.6]. □

Lemma 1.5.15. (Rapoport)

$$\mathcal{M}_{K_0}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C} = \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee) \backslash (K_0 \otimes \mathbb{H}).$$

Proof. See the proof of [Rap78, Lemma 6.12]. □

Proposition 1.5.16. Let K_0 have discriminant 5, 8, 13 or 17. Then $\mathcal{M}_{K_0}(\mathbb{Z})$ is a finitely generated $\mathbb{Z}$-algebra, and the q-expansions of a choice of generators are known.

Proof. For discriminant 5 see [Mul85] or [May07], for discriminant 8 see [Mul83], and for discriminants 13 and 17 see [May07]. □

1.6 A useful property of principally polarised ideals

As we have seen in Theorem 1.3.11, we can study principally polarised ordinary abelian varieties over finite fields by studying principally polarised ideals. Recall that we defined $\mathbf{PId}_\pi$ to be the category of principally polarised $\mathbb{Z}[\pi, \overline{\pi}]$-ideals, where π is a Weil q-number, and that $\mathbf{PId}_{\pi,K_0}$ was the full category of $\mathbf{PId}_\pi$ in which the objects have endomorphism ring containing $\mathcal{O}_{K_0}$. This corresponds to studying principally polarised ordinary abelian varieties over $\mathbb{F}_q$ with Frobenius π and with real multiplication by $\mathcal{O}_{K_0}$, which are a main topic of interest throughout this thesis. In this section we prove a very useful property of objects $(\mathfrak{a}, \beta) \in \mathbf{PId}_{\pi,K_0}$ that we will use throughout this thesis, namely that for every such object, there exists $\tau \in K$ and $\beta' \in K$ such that

$$(\mathfrak{a}, \beta) \cong (\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee, \beta').$$

Lemma 1.6.1. Suppose that $(\mathfrak{a}, \beta) \in \mathbf{PId}_{\pi,K_0}$ is a principally polarised fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideal that is stable under complex conjugation with maximal real multiplication by $\mathcal{O}_{K_0}$. Then there exists $\tau \in K$ for which

$$\mathfrak{a} = \tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee,$$

where $\mathcal{O}_{K_0}^\vee$ denotes the trace dual of $\mathcal{O}_{K_0}$.

Proof. As $\mathcal{O}_{K_0}$ is a Dedekind domain, every ideal is generated as a $\mathbb{Z}$-module by at most 2 elements, so that by [Bass63, Proposition 1.5], every finitely generated projective $\mathcal{O}_{K_0}$-module is the direct sum of ideals of $\mathcal{O}_{K_0}$. By assumption we have that $\mathcal{O}_{K_0} \subset \mathrm{End}(\mathfrak{a}) \subseteq \mathcal{O}_K$, where $K = \mathbb{Q}(\pi)$ is a totally imaginary quadratic extension of K_0, so that $\mathfrak{a}$ is a finitely generated projective $\mathcal{O}_{K_0}$-module. In particular, there exist $x, y \in K$ and a fractional $\mathcal{O}_{K_0}$-ideal $\mathfrak{b}$ such that

$$\mathfrak{a} = x\mathcal{O}_{K_0} + y\mathfrak{b}.$$

Now, from the polarisation β of $\mathfrak{a}$, we have a non-degenerate alternating $\mathbb{Z}$-bilinear form defined by

$$\begin{array}{rccc} E: & \mathfrak{a} \times \mathfrak{a} & \longrightarrow & \mathbb{Z} \\ & (u, v) & \mapsto & \mathrm{tr}_{K/\mathbb{Q}}(\beta \overline{u} v), \end{array}$$

which factors via the non-degenerate alternating $\mathcal{O}_{K_0}$-bilinear form

$$\begin{array}{rccc} S: & \mathfrak{a} \times \mathfrak{a} & \longrightarrow & \mathcal{O}_{K_0}^{\vee} \\ & (u, v) & \mapsto & \mathrm{tr}_{K/K_0}(\beta \overline{u} v) \end{array}$$

by definition of the trace dual $\mathcal{O}_{K_0}^{\vee}$. The matrix of $S \otimes \mathbb{Q}$ with respect to the K_0-basis $\langle x, y \rangle$ is then given by

$$\begin{pmatrix} 0 & c \\ -c & 0 \end{pmatrix},$$

where $c = \mathrm{tr}_{K/K_0}(\beta \overline{x} y)$. Choose $\mathbb{Z}$-bases $\langle \omega_1, \ldots, \omega_g \rangle$ and $\langle b_1, \ldots, b_g \rangle$ for $\mathcal{O}_{K_0}$ and $\mathfrak{b}$ respectively. We can then compute the matrix of E with respect to the $\mathbb{Z}$-basis

$$\langle x\omega_1, \ldots, x\omega_g, yb_1, \ldots, yb_g \rangle,$$

to be

$$\begin{pmatrix} 0 & M \\ -M & 0 \end{pmatrix},$$

where

$$M = (\mathrm{tr}_{K_0/\mathbb{Q}}(c\omega_i b_j))_{i,j=1,\ldots,g}.$$

In turn, we get that M is the matrix of the form

$$\begin{array}{rccc} F: & \mathcal{O}_{K_0} \times \mathfrak{b} & \longrightarrow & \mathbb{Z} \\ & (u, v) & \mapsto & \mathrm{tr}_{K_0/\mathbb{Q}}(cuv) \end{array}$$

with respect to the $\mathbb{Z}$-basis $\langle \omega_1, \ldots, \omega_g, b_1, \ldots, b_g \rangle$. In particular, as E is non-degenerate, so is F, giving us that

$$c\mathfrak{b} = \mathcal{O}_{K_0}^{\vee}.$$

Hence, multiplication by $y^{-1}c^{-1}$ defines an isomorphism

$$(\mathfrak{a}, \beta) \tilde{\to} (xy^{-1}c^{-1}\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^{\vee}, yc\overline{yc}\beta).$$

□

Chapter 2

Hilbert modular polynomials

2.1 Introduction and statement of the results

The modular polynomial for elliptic curves of prime level p is an irreducible polynomial $\Phi_p(X,Y) \in \mathbb{Z}[X,Y]$ which, for every pair of p-isogenous elliptic curves E and E', satisfies

$$\Phi_p(j(E), j(E')) = 0,$$

where $j(E)$ is the j-invariant of the elliptic curve E. Examples of these modular polynomials can be found in the Handbook of Hyperelliptic Curves and Cryptography, [HEHCC, Section 17.2.3]. One of the reasons that modular polynomials interest us is that given the j-invariant of an elliptic curve E over a field k, we can find the j-invariants of all those elliptic curves that are p-isogenous to it by computing the roots of $\Phi_p(j(E), Y) \in k[Y]$. In this chapter, we describe an analogue of the modular polynomial for principally polarised abelian varieties of dimension g with real multiplication, which we call a *set of Hilbert modular polynomials*. This is a Hilbert modular function analogue of Dupont's work with Siegel modular functions in [Dup06]. The advantage of working in this setting is that the coefficients of the polynomials are much more manageable, making it possible to compute them for higher prime levels than previously. Furthermore, Algorithm 2.4.1 computes these polynomials, and is implemented in MAGMA, and the content of this chapter gives a proof that the output of the algorithm is exactly what we expect.

The modular polynomial for elliptic curves of level p parametrises p-isogenies of elliptic curves (for p prime) and is defined using the j-invariant. To generalise the modular polynomial to a Hilbert modular setting, we first fix a totally real number field K_0 of degree g over $\mathbb{Q}$, and we write $\mathcal{O}_{K_0}$ for its maximal order. We then need to replace j by an 'isomorphism invariant' for objects $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{C},K_0}$, the category of principally polarised complex abelian

g-folds (A, ξ) with an appropriate embedding $\iota : \mathcal{O}_{K_0} \hookrightarrow \mathrm{End}(\mathrm{A})$ (see Definition 1.5.2 for the formal definition). Let $\overline{V}$ be the Hilbert modular variety for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^{\vee})$, as defined in Definition 1.5.13, where $\mathcal{O}_{K_0}^{\vee}$ is the trace dual of $\mathcal{O}_{K_0}$. We will see in Section 2.2 that for some $d \leq g+1$, there exist d rational functions

$$J_1, \ldots, J_d : \overline{V} \longrightarrow \mathbb{C}$$

such that the function field of $\overline{V}$ is $\mathbb{C}(J_1, \ldots, J_d)$, and for such $J_1, \ldots, J_d$, there exists a Zariski-open affine subvariety U of $\overline{V}$ such that the rational map

$$(J_1, \ldots, J_d) : U \longrightarrow \mathbb{A}^d_{\mathbb{C}}$$

is an injective morphism.

Definition 2.1.1. For $d \leq g+1$, a d-tuple of Hilbert modular functions $(J_1, \ldots, J_d) \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))^{\times d}$ such that

$$\mathbb{C}(\overline{V}) = \mathbb{C}(J_1, \ldots, J_d)$$

is a choice of *RM isomorphism invariant* for K_0.

Remark 2.1.2. Fixing U as above, for every $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{C}, K_0}$ which corresponds as in Lemma 1.5.5 to a point in U, the d-tuple

$$(J_1, \ldots, J_d)(\mathrm{A}, \xi, \iota)$$

determines (A, ξ, ι) up to isomorphism. That is, RM isomorphism invariants are only isomorphism invariants in the traditional sense on U.

Definition 2.1.3. For a totally positive prime element μ of $\mathcal{O}_{K_0}$, and for $\tau, \tau' \in K_0 \otimes \mathbb{H}$, we say that *there exists a μ-isogeny*

$$\tau \to \tau'$$

if there exists a μ-isogeny

$$(\mathrm{A}, \xi, \iota) \longrightarrow (\mathrm{A}', \xi', \iota',)$$

where the isomorphism classes of (A, ξ, ι) and $(\mathrm{A}', \xi', \iota') \in \mathbf{POrd}_{\mathbb{C}, K_0}$ correspond as in Lemma 1.5.5 to the equivalence classes of τ and τ' in $\overline{V}$ respectively. Note that by Theorem 1.5.4 and Lemma 1.6.1 τ and τ' satisfy

$$H_1(\mathrm{A}(\mathbb{C}), \mathbb{Z}) = \tau \mathcal{O}_{K_0} + \mathcal{O}_{K_0}^{\vee} \quad \text{and} \quad H_1(\mathrm{A}'(\mathbb{C}), \mathbb{Z}) = \tau' \mathcal{O}_{K_0} + \mathcal{O}_{K_0}^{\vee}.$$

Our higher dimensional analogue of the modular polynomial will parametrise μ-isogenies of objects in $\mathbf{POrd}_{\mathbb{C}, K_0}$, and will be defined using the isomorphism invariants of Section 2.2. The first main theorem of this chapter, given below, gives this higher dimensional analogue of the modular polynomial for elliptic curves.

Theorem 2.1.4. *For a totally real number field K_0 of degree g over $\mathbb{Q}$, and a totally positive prime element μ of $\mathcal{O}_{K_0}$ (the ring of integers of K_0), let $\overline{V}$ be the Hilbert modular variety for K_0 (as defined in Definition 1.5.13), and fix a choice of RM isomorphism invariants $(J_1, \ldots, J_d)$ for K_0, as defined in Definition 2.1.1. Then Algorithm 2.4.1 below outputs a polynomial*

$$G_\mu(X_1, \ldots, X_d, Y) \in \mathbb{Z}[X_1, \ldots, X_d, Y]$$

that has degree $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)+1$ *in Y, and for $i = 2, \ldots, d$, outputs polynomials*

$$H_{\mu,i}(X_1, \ldots, X_d, Y, Z_i) \in \mathbb{Z}[X_1, \ldots, X_d, Y, Z_i]$$

that are linear in Z_i. Furthermore, for any choice of Zariski-open subvariety U of $\overline{V}$ such that the map

$$(J_1, \ldots, J_d) : U \to \mathbb{A}^d_{\mathbb{C}}$$

is injective, as in Theorem 2.2.1. for every

$$[\tau], [\tau'] \in U - \{x \in U : \Delta_{G_\mu(J_1(x),\ldots,J_d(x),Y)} = 0\},$$

there exists a μ-isogeny

$$\tau \to \tau'$$

if and only if

$$G(J_1(\tau), \ldots, J_d(\tau), J_1(\tau')) = 0,$$

and for $i = 2, \ldots, d$,

$$H_{\mu,i}(J_1(\tau), \ldots, J_d(\tau), J_1(\tau'), J_i(\tau')) = 0.$$

Definition 2.1.5. For a totally positive prime element $\mu \in K_0$, we define a *set of Hilbert modular polynomials of level μ* to be a set of polynomials

$$\left\{ \begin{array}{c} G_\mu(X_1, \ldots, X_d, Y) \in \mathbb{Z}[X_1, \ldots, X_d, Y], \\ H_{\mu,i}(X_1, \ldots, X_d, Y, Z_i) \in \mathbb{Z}[X_1, \ldots, X_d, Y, Z_i] \end{array} \right\}_{i=2,\ldots,d}$$

such that $G_\mu(X_1, \ldots, X_d, Y)$ and $H_{\mu,i}(X_1, \ldots, X_d, Y, Z_i)$ satisfy the conclusions of Theorem 2.1.4.

Let $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ be the modular polynomial for elliptic curves of level ℓ, and write $\overline{\Phi_\ell(X, Y)} \in \mathbb{F}_q[X, Y]$ for its reduction modulo q. For every pair of elliptic curves E and E' defined over $\mathbb{F}_q$, we have that E and E' are ℓ-isogenous if and only if

$$\overline{\Phi_\ell(j(E), j(E'))} \equiv 0.$$

The second main theorem of this chapter, Theorem 2.1.9, gives a genus 2 analogue of $\overline{\Phi_\ell(X, Y)}$. Being able to work with Hilbert modular polynomials mod q allows us to speed up the algorithm that computes the polynomials over $\mathbb{C}$ by using the Chinese remainder theorem, as well as being interesting in their own right, for example in order to generalise Schoof's algorithm for point counting, which we look at in Chapter 5.

Definition 2.1.6. Recall from Definition 1.5.2 the definition of $\mathbf{POrd}_{\mathbb{F}_q,K_0}$, the category of principally polarised abelian varieties over $\mathbb{F}_q$ with maximal real multiplication by K_0, and from Definition 1.5.3 the definition of a μ-isogeny between objects of $\mathbf{POrd}_{\mathbb{F}_q,K_0}$. Define

$$F_\pi : \mathbf{Ord}_{\pi,K_0} \longrightarrow \mathbf{Id}_{\pi,K_0}$$

to be the functor of Theorem 1.3.11. Then we say that $(\mathrm{A},\xi,\iota) \in \mathbf{POrd}_{\mathbb{F}_q,K_0}$ *lifts to* $\tau \in K_0 \otimes \mathbb{H}$ if there exists a Weil q-number $\pi \in \mathrm{End}(\mathrm{A}) \otimes \mathbb{Q}$ such that $\iota(\mathrm{Frob}_q) = \pi$, where Frob_q is the q-power Frobenius on A, and

$$(F_\pi(\mathrm{A}), F_\pi(\xi)) \cong (\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee, \beta'),$$

for some principal polarisation β' of $\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee \in \mathbf{Id}_{\pi,K_0}$.

Definition 2.1.7. For a totally real number field K_0 of degree g over $\mathbb{Q}$, and a prime power $q \in \mathbb{Z}$, we say that q is K_0-*friendly* if there exists a totally imaginary degree 2 extension of K_0 which is generated by a Weil q-number.

Definition 2.1.8. We will see in Lemma 2.2.3 that J_3 is algebraic over $\mathbb{Q}(J_1, J_2)$. Write $m(X) \in \mathbb{Q}(J_1, J_2)[X]$ for the minimal polynomial of J_3 in $\mathbb{Q}(J_1, J_2)[X]$.

Theorem 2.1.9. *Let $g = 2$, and fix (J_1, J_2, J_3) as in Theorem 2.1.4. For all but finitely many K_0-friendly prime powers q, if $\tau \in K_0 \otimes \mathbb{H}$ is a lift of some $(\mathrm{A},\xi,\iota) \in \mathbf{POrd}_{\mathbb{F}_q,K_0}$ and the equivalence class $[\tau]$ of τ in $\overline{V}$ is in U, then the pair*

$$(J_1(\tau), J_2(\tau)) \ mod\ q$$

determines (A,ξ) up to isomorphism. Furthermore, defining μ, U, G_μ and $H_{\mu,2}$, as in Theorem 2.1.4, if

$$[\tau], [\tau'] \in U - \{x \in U : \Delta_{G_\mu(J_1(x),J_2(x),Y)} = 0\},$$

and τ and τ' are lifts of (A,ξ,ι) and $(\mathrm{A}',\xi',\iota') \in \mathbf{POrd}_{\mathbb{F}_q,K_0}$, then there exists a μ-isogeny

$$(\mathrm{A},\xi,\iota) \longrightarrow (\mathrm{A}',\xi',\iota')$$

or

$$(\mathrm{A},\xi,\iota) \longrightarrow (\mathrm{A}',\xi',-\iota')$$

if and only if

$$G_\mu(\overline{J_1(\tau)}, \overline{J_2(\tau)}, \overline{J_3(\tau)}, \overline{J_1(\tau')}) \equiv 0 \ mod\ q,$$
$$H_{\mu,2}(\overline{J_1(\tau)}, \overline{J_2(\tau)}, \overline{J_3(\tau)}, \overline{J_1(\tau')}, \overline{J_2(\tau')}) \equiv 0 \ mod\ q,$$

and

$$m(J_3(\tau)) \equiv 0 \ mod\ q,$$

where $\bar{\cdot}$ denotes reduction mod q.

We will discuss isomorphism invariants of abelian 2-folds defined over finite fields in Section 2.6; we will see that Theorem 2.1.9 follows from this discussion and Theorem 2.1.4.

2.2 Defining RM isomorphism invariants over the complex numbers

As before, let K_0 be a totally real number field of degree g over $\mathbb{Q}$, and let $\overline{V}$ be the Hilbert modular variety for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$, as defined in Definition 1.5.13. The aim of this section is to prove Theorem 2.2.1:

Theorem 2.2.1. *Write $\mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))$ for the $\mathbb{Q}$-algebra of quotients of Hilbert modular forms in $\mathcal{M}_{K_0}(\mathbb{Z})$ of equal weight. For some $d \leq g+1$, there exist rational functions*

$$J_1, \ldots, J_d \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))$$

such that the function field of $\overline{V}$, denoted $\mathbb{C}(\overline{V})$, is $\mathbb{C}(J_1, \ldots, J_d)$, and for such $J_1, \ldots, J_d$, there exists a Zariski-open affine subvariety U of $\overline{V}$ such that the map

$$(J_1, \ldots, J_d) : U \longrightarrow \mathbb{A}^d_{\mathbb{C}}$$

is a well-defined injective morphism.

Example 2.2.2. If $g = 1$, so that $K_0 = \mathbb{Q}$, then we have that

$$\mathrm{SL}_2(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee) \backslash K_0 \otimes \mathbb{H} = \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}.$$

The j-invariant for elliptic curves defines an isomorphism

$$j : \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H} \longrightarrow \mathbb{A}^1_{\mathbb{C}}.$$

Hence setting

$$V = \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}, \quad \overline{V} = \mathbb{P}^1_{\mathbb{C}}, \quad U = V, \text{ and } \quad J_1 = j$$

gives us $\mathbb{C}(\overline{V}) = \mathbb{C}(J_1)$ and an injective morphism $J_1 : U \to \mathbb{A}^1_{\mathbb{C}}$.

Before proving Theorem 2.2.1, we first prove the following lemma.

Lemma 2.2.3. Let $\mathbb{C}(\overline{V})$ denote the function field of $\overline{V}$. Then there exist rational functions $J_1, \ldots, J_{g+1} : \overline{V} \longrightarrow \mathbb{P}^1(\mathbb{C})$ such that

$$\mathbb{C}(\overline{V}) = \mathbb{C}(J_1, \ldots, J_{g+1}).$$

Proof. The transcendence degree of the function field $\mathbb{C}(\overline{V})$ over $\mathbb{C}$ is g, so there exist g algebraically independent rational functions $J_1, \ldots, J_g$ in $\mathbb{C}(\overline{V})$. By Proposition 1.5.14 and Lemma 1.5.15, we have that $\mathbb{C}(\overline{V})$ is a finite separable field extension of $\mathbb{C}(J_1, \ldots, J_g)$ and hence is generated by one element, which we denote by J_{g+1}. □

Proof of Theorem 2.2.1. By Lemma 2.2.3, we can fix $J_1, \ldots, J_{g+1} \in \mathbb{C}(\overline{V})$ such that

$$\mathbb{C}(\overline{V}) = \mathbb{C}(J_1, \ldots, J_{g+1})$$

as $\mathbb{C}$-algebras. Write W for the image of $(J_1, \ldots, J_{g+1})$ in $\mathbb{A}^{g+1}_{\mathbb{C}}$. Then by [Har77, Corollary I.4.5], there are non-empty Zariski-open subsets $U \subseteq \overline{V}$ and $U' \subseteq W$ such that U is isomorphic to U'. By the Baily-Borel Theorem, Definition 1.5.13, we have also that $\mathbb{C}(\overline{V}) = \mathbb{C}(\mathcal{M}_{K_0})$, where $\mathcal{M}_{K_0}$ is the graded ring of Hilbert modular forms for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}^{\vee}_{K_0})$, so that $J_1, \ldots, J_{g+1}$ are also Hilbert modular functions for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}^{\vee}_{K_0})$. Then, we have by Lemma 1.5.15 that

$$\mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z})) \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{C}(\mathcal{M}_{K_0}).$$

In particular, we can choose $J_1, \ldots, J_d$ to be in $\mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))$. □

For completeness, we recall here the definition of RM isomorphism invariants from the previous section.

Definition 2.1.1. *For $d \leq g+1$, a d-tuple of Hilbert modular functions*

$$(J_1, \ldots, J_d) \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))^{\times d}$$

such that

$$\mathbb{C}(\overline{V}) = \mathbb{C}(J_1, \ldots, J_d)$$

is a choice of RM isomorphism invariant *for K_0.*

From this point on, we fix an RM isomorphism invariant $(J_1, \ldots, J_d)$, and a non-empty Zariski-open subvariety U of the Hilbert modular variety $\overline{V}$ such that

$$(J_1, \ldots, J_d) : U \longrightarrow \mathbb{A}^d_{\mathbb{C}}$$

defines an injective morphism.

2.3 Proof of Theorem 2.1.4

As before, in what follows, K_0 is a totally real number field of degree g over $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_0}$. As in Definition 2.1.1, we write $\overline{V}$ for the Hilbert modular variety, as in Definition 2.1.1, we fix a choice of RM isomorphism invariant $(J_1, \ldots, J_d) \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z}))$, and as in Theorem 2.2.1, we write U for a Zariski-open subvariety of $\overline{V}$ for which

$$(J_1, \ldots, J_d) : U \longrightarrow \mathbb{A}^d_{\mathbb{C}}$$

is an injective morphism.

Definition 2.3.1. For $i = 1, \ldots, g+1$, we define f_i and g_i to be elements of $\mathcal{M}_{K_0}(\mathbb{Z})$ of weight k_i such that

$$J_i = f_i / g_i.$$

Definition 2.3.2. Define $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}^{\vee}_{K_0})$ as in Definition 1.5.1. Then we define

$$\Gamma^0(\mu) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}^{\vee}_{K_0}) : b \in \mu \mathcal{O}^{\vee}_{K_0} \right\}.$$

Definition 2.3.3. Denote by $\mathcal{C}$ a choice of coset representatives for the quotient of groups $\Gamma^0(\mu)\backslash \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$, and for any $x \in K_0$ define

$$\underline{x} := \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}.$$

We then define the polynomials

$$\Phi_\mu(Y) := \prod_{M \in \mathcal{C}} \left(g_1|_{\underline{\mu^{-1}}M} Y - f_1|_{\underline{\mu^{-1}}M} \right)$$

and for each $i = 2, \ldots, g+1$,

$$\Psi_{\mu,i}(Y, Z_i) := \sum_{M \in \mathcal{C}} \left\{ \left(g_i|_{\underline{\mu^{-1}}M} Z_i - f_i|_{\underline{\mu^{-1}}M} \right) \prod_{\substack{M' \in \mathcal{C} \\ M' \neq M}} \left(g_1|_{\underline{\mu^{-1}}M'} Y - f_1|_{\underline{\mu^{-1}}M'} \right) \right\}.$$

Remark 2.3.4. We have that

$$\Phi_\mu(Y) \in \mathcal{M}_{K_0}(\mathbb{Z})[Y] \quad \text{and} \quad \Psi_{\mu,i}(Y, Z_i) \in \mathcal{M}_{K_0}(\mathbb{Z})[Y, Z_i].$$

Recall that for any $M \in \mathcal{C} (= \Gamma^0(\mu)\backslash \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee))$ and any $N \in \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$, and for every $f \in \mathcal{M}_{K_0}$, we have that

$$(f|_{\underline{\mu^{-1}}M})|_N(\tau) = f|_{\underline{\mu^{-1}}MN}(\tau).$$

In particular, acting by $|_N$ on the coefficients of $\Phi_\mu(Y)$ (and $\Psi_{\mu,i}(Y, Z_i)$) just permutes the factors (or terms) of the defining product (or sum), leaving $\Phi_\mu(Y)$ (and $\Psi_{\mu,i}(Y, Z_i)$) unchanged, hence the coefficients are modular forms for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$.

Proposition 2.3.5. Fix notation as in Definitions 2.1.3-2.3.3. Then for any $\tau, \tau' \in K_0 \otimes \mathbb{H}$ such that the classes $[\tau]$ and $[\tau']$ of τ and τ' in $\overline{V}$ are in U, there exists a μ-isogeny $\tau \to \tau'$ if and only if for every $i = 2, \ldots, d$, evaluating $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$ at $(Y, Z_2, \ldots, Z_d) = (J_1([\tau']), \ldots, J_d([\tau']))$, and then evaluating the resulting modular forms at $[\tau]$, gives

$$\left(\Phi_\mu(J_1([\tau']))\right)([\tau]) = 0 \quad \text{and} \quad \left(\Psi_{\mu,i}(J_1([\tau']), J_i([\tau']))\right)([\tau]) = 0.$$

We prove this by means of the following lemma.

Lemma 2.3.6. Define $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$ as in Definition 1.5.1, fix a totally positive element $\mu \in K_0$, and define $\Gamma^0(\mu)$ as in Proposition 2.3.5. For $\mathcal{C}$ a set of coset representatives for $\Gamma^0(\mu)\backslash \mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$, for any $\tau \in K_0 \otimes \mathbb{H}$, we have that

$$\left\{ [\mu^{-1} M \tau] : M \in \mathcal{C} \right\} = \left\{ [\tau'] : \exists\ \mu\text{-isogeny } \tau \to \tau' \right\},$$

where $[\cdot]$ denotes the class of $\cdot$ in $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)\backslash K_0 \otimes \mathbb{H}$.

Proof. We first show that there is a μ-isogeny $\tau \to \mu^{-1}\tau$, that is, that there is a surjective morphism

$$f : \mathbb{C}^g/(\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee) \longrightarrow \mathbb{C}^g/(\mu^{-1}\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee$$

that defines a μ-isogeny. Note that $f : x \mapsto x$ is a surjective morphism in this case and defines a μ-isogeny

$$\left(\mathbb{C}^g/(\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee), \xi, \iota\right) \longrightarrow \left(\mathbb{C}^g/(\mu^{-1}\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee), \mu\xi, \iota\right).$$

So there is a μ-isogeny $\tau \to \mu^{-1}\tau$, and it is then easy to see that

$$\left\{[\mu^{-1}M\tau] : M \in \mathcal{C}\right\} \subseteq \left\{[\tau'] : \exists\ \mu\text{-isogeny } \tau \to \tau'\right\}.$$

Now let $\tau' \in K_0 \otimes \mathbb{H}$ be such that there is a μ-isogeny $\tau \to \tau'$. By definition of μ-isogeny there exists

$$\alpha \in \{x \in K_0^* : x(\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee) \subseteq \tau'\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee\}$$

such that the following diagram is exact and commutative:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & \longrightarrow & \operatorname{coker}(\alpha) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee & \xrightarrow{\alpha} & \tau'\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee & \longrightarrow & \operatorname{coker}(\alpha) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \alpha^\vee\beta'} & & \downarrow & & \\
0 & \longrightarrow & \tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee & \xrightarrow{\beta} & \mathcal{O}_{K_0} + \overline{\tau}^{-1}\mathcal{O}_{K_0}^\vee & \longrightarrow & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \operatorname{coker}(\mu) & \longrightarrow & \operatorname{coker}(\alpha^\vee) & \longrightarrow & 0. & &
\end{array}$$

In particular, by the Snake Lemma we get an exact sequence

$$0 \longrightarrow \operatorname{coker}(\alpha) \longrightarrow \frac{\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee}{\mu\tau\mathcal{O}_{K_0} + \mu\mathcal{O}_{K_0}^\vee} \longrightarrow \operatorname{coker}(\overline{\alpha}) \to 0.$$

Also, as $\mathcal{O}_{K_0}$ is a Dedekind domain, the trace dual $\mathcal{O}_{K_0}^\vee$ is an invertible $\mathcal{O}_{K_0}$-ideal, so in particular, as additive groups, we have an isomorphism

$$\frac{\mathcal{O}_{K_0}}{\mu\mathcal{O}_{K_0}} \times \frac{\mathcal{O}_{K_0}}{\mu\mathcal{O}_{K_0}} \cong \frac{\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee}{\mu\tau\mathcal{O}_{K_0} + \mu\mathcal{O}_{K_0}^\vee},$$

so that the exact sequence gives us an isomorphism of additive groups

$$\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0} \cong \frac{\tau'\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee}{\alpha(\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee)} \cong \frac{\alpha^{-1}\mu\tau'\mathcal{O}_{K_0} + \alpha^{-1}\mu\mathcal{O}_{K_0}^\vee}{\mu(\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee)}.$$

In particular, we get that

$$\alpha^{-1}\mu\tau'\mathcal{O}_{K_0} + \alpha^{-1}\mu\mathcal{O}_{K_0}^{\vee} = \tau\mathcal{O}_{K_0} + \mu\mathcal{O}_{K_0}^{\vee}.$$

This shows that $\alpha \in (\mathcal{O}_{K_0}^{\vee})^*$ and

$$[\mu\tau'] = [\alpha\tau] = [\tau].$$

□

Proof of Proposition 2.3.5. The theorem now follows from Lemma 2.3.6. □

Lemma 2.3.7. Let $\mathcal{M}_{K_0}$ be as in Definition 1.5.11. For every $i = 1, \ldots, d$, define k_i as in Definition 2.3.1, and define $\mathcal{C}$ as in Definition 2.3.3. Define $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$ as in Definition 2.3.3. Then there exist modular forms $y_0, \ldots, y_{|\mathcal{C}|-1} \in \mathcal{M}_{K_0}$ of weight $|\mathcal{C}|k_1$, and for $i = 2, \ldots, d$, there exist modular forms $z_{i,0}, z'_{i,0}, \ldots, z_{i,|\mathcal{C}|-1}, z'_{i,|\mathcal{C}|-1} \in \mathcal{M}_{K_0}$ of weight $(|\mathcal{C}| - 1)k_1 + k_i$ such that

$$\Phi_\mu(Y) = \sum_{n=0}^{|\mathcal{C}|} y_n Y^n$$

and

$$\Psi_{\mu,i}(Y, Z_i) = \sum_{n=0}^{|\mathcal{C}|-1} (z_{i,n} Z_i - z'_{i,n}) Y^n.$$

Proof. This follows from the explicit formulae in Definition 2.3.3. □

Proof of Theorem 2.1.4. Theorem 2.1.4 now follows from Proposition 2.3.5 and Lemma 2.3.7. □

2.4 Algorithm to compute a set of Hilbert modular polynomials

The main theorem of this chapter, Theorem 2.1.4, proves that Algorithm 2.4.1 runs and that the output is correct. In this section, we will first prove Theorem 2.1.4, and then give Algorithm 2.4.1.

2.4.1 The algorithm

Given the coefficients of the q-expansions of $J_1, \ldots J_d$ up to a high enough precision to determine them completely, using Lemma 2.7.2 and the formulae for $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$ given in Definition 2.3.3 we can write out explicit formulae for the q-expansions of the constant coefficients (with respect to Y and Z_i) of $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$. Then, fix the $\mathbb{Z}$-algebra generators of $\mathcal{M}_{K_0}$ to be $\gamma_1, \ldots, \gamma_s$ of weights $\kappa_1, \ldots, \kappa_s$ respectively, and assume that we also know the coefficients of the q-expansions of $\gamma_1, \ldots, \gamma_s$. It is then just linear

algebra to determine the integers $h_1, \ldots, h_s$ and the rational numbers $b_{\underline{h}}$, where $\underline{h} = (h_1, \ldots, h_s)$, such that for each coefficient $f \in \mathcal{M}_{K_0}$ of $\Phi_\mu(Y)$ or $\Psi_{\mu,i}(Y, Z_i)$, we have that

$$f = \sum_{\left\{\underline{h} \in (\mathbb{Z}_{\geq 0})^{\times(s)} : \sum_{j=1}^{s} h_j \kappa_j = k\right\}} b_{\underline{h}} \prod_{j}^{s+1} \gamma_j^{h_j}.$$

The following algorithm computes a Hilbert set of modular polynomials in the sense of Definition 2.1.5.

Algorithm 2.4.1.
INPUT: A totally real number field K_0 of degree g over $\mathbb{Q}$, the q-expansions of generators $\gamma_1, \ldots, \gamma_s$ of the $\mathbb{Z}$-module $\mathcal{M}_{K_0}(\mathbb{Z})$, RM isomorphism invariants $J_1, \ldots, J_d$ for K_0 as defined in Definition 2.1.1 written in terms of $\gamma_1, \ldots, \gamma_s$, and a totally positive element $\mu \in K_0$ that generates a prime ideal.
OUTPUT: Polynomials

$$G_\mu(X_1, \ldots, X_d, Y) \in \mathbb{Z}[X_1, \ldots, X_d, Y]$$
$$H_{\mu,i}(X_1, \ldots, X_d, Y, Z_i) \in \mathbb{Z}[X_1, \ldots, X_d, Y, Z_i],$$

for $i = 2, \ldots, d$, satisfying the conclusions of Theorem 2.1.4.

1. Compute the q-expansions of the coefficients of $\Phi_\mu(Y)$ and $\Psi_{i,\mu}(Y, Z_i)$ using Definition 2.3.3, up to precision P. For details on how to compute the required precision, see the MAGMA code, which can be found at `https://pub.math.leidenuniv.nl/~martindalecr/Code`.

2. Write each coefficient of $\Phi_\mu(Y)$ and $\Psi_{\mu,i}(Y, Z_i)$ as elements of $\mathbb{Z}[\gamma_1, \ldots, \gamma_s]$ using linear algebra on the q-expansions (here it is necessary to have chosen the precision of the q-expansions to be sufficiently large).

3. (a) Write $h_1 = g_1^{|\mathcal{C}|}$, where $g_1 \in \mathcal{M}_{K_0}$ is the denominator of J_1, and $\mathcal{C}$ is as defined in Definition 2.3.3.
   (b) For $i = 2, \ldots, d$, write $h_i = g_1^{|\mathcal{C}|-1} g_i$, where $g_i \in \mathcal{M}_{K_0}$ is the denominator of J_i.

4. (a) Define
$$\mathbf{r}^{\Phi_\mu} = \left\{ (r_1, \ldots, r_d) \in \mathbb{Z}^d : \sum_{i=1}^{d} r_i k_i = |\mathcal{C}| k_1 \right\},$$
   where for each i, the integer k_i is the weight of g_i.
   (b) For $i = 2, \ldots, d$, define
$$\mathbf{r}^{\Psi_{\mu,i}} = \left\{ (r_1, \ldots, r_d) \in \mathbb{Z}^d : \sum_{i=1}^{d} r_i k_i = (|\mathcal{C}| - 1) k_1 + k_i \right\}.$$

5. (a) Write $\ell = \mathrm{Norm}_{K_0/\mathbb{Q}}$. Using linear algebra, for every $n = 0, \ldots, \ell+1$ and every $(r_1, \ldots, r_d) \in \mathbf{r}^{\Phi_\mu}$, compute the rational numbers $a_{n,r_1,\ldots,r_d}$ such that

$$\Phi_\mu(Y)/h_1 = \sum_{n=0}^{\ell+1} \left(\sum_{(r_1,\ldots,r_d)\in\mathbf{r}^{\Phi_\mu}} a_{n,r_1,\ldots,r_d} \prod_{i=1}^{d} J_i^{r_i} \right) Y^n.$$

(b) For $i = 2, \ldots, d$, using linear algebra, for every $n = 0, \ldots, \ell$ and every $(r_1, \ldots, r_d) \in \mathbf{r}^{\Psi_{\mu,i}}$, compute the rational numbers $b_{n,r_1,\ldots,r_d}$ and $c_{n,r_1,\ldots,r_d}$ such that

$$\Psi_{\mu,i}/h_i =$$

$$\sum_{n=0}^{\ell} \left(\sum_{(r_1,\ldots,r_d)\in\mathbf{r}^{\Psi_{\mu,i}}} \left(b_{n,r_1,\ldots,r_d} + c_{n,r_1,\ldots,r_d} Z_i\right) \prod_{j=1}^{d} J_j^{r_j} \right) Y^n.$$

6. (a) Define the $\mathbb{Q}$-valued polynomial

$$G'_\mu(X_1, \ldots, X_d, Y) = \sum_{n=0}^{\ell+1} \left(\sum_{(r_1,\ldots,r_d)\in\mathbf{r}^{\Phi}} a_{n,r_1,\ldots,r_d} \prod_{i=1}^{d} X_i^{r_i} \right) Y^n,$$

write s for the common denominator of the coefficients of G'_μ, and set

$$G_\mu(X_1, \ldots, X_d, Y) = sG'_\mu(X_1, \ldots, X_d, Y).$$

(b) For every $i = 2, \ldots, d$, define the $\mathbb{Q}$-valued polynomial

$$H'_{\mu,i}(X_1, \ldots, X_d, Y, Z_i) =$$
$$\sum_{n=0}^{\ell} \left(\sum_{(r_1,\ldots,r_d)\in\mathbf{r}^{\Psi_{\mu,i}}} \left(b_{n,r_1,\ldots,r_d} + c_{n,r_1,\ldots,r_d} Z_i\right) \prod_{j=1}^{d} X_j^{r_j} \right) Y^n,$$

write t_i for the common denominator of the coefficients of $H'_{\mu,i}$, and set

$$H_{\mu,i}(X_1, \ldots, X_d, Y, Z_i) = t_i H'_{\mu,i}(X_1, \ldots, X_d, Y, Z_i).$$

We have implemented this in MAGMA for $K_0 = \mathbb{Q}(\sqrt{5})$ and $K_0 = \mathbb{Q}(\sqrt{2})$, and the code can be found at `http://pub.math.leidenuniv.nl/~martindalecr/Code`.

2.5 Computing the RM isomorphism invariant for a given genus 2 curve

In Definition 2.1.1, we defined an RM isomorphism invariant for elements of $\mathbf{POrd}_{\mathbb{C},K_0}$. It is however not immediately clear how to compute these, which we now address, at least in the genus 2 case. We have a computational advantage in genus 2, which is that there exist Igusa invariants to determine a curve up to isomorphism.

Definition 2.5.1. For a curve C of genus 2 over a field k with $\mathrm{char}(k) \neq 2$, there exists an affine model of C given by $y^2 = f(x)$, where f is a separable polynomial of degree 6. Denote by c the leading coefficient of f, fix an ordering $x_1, \ldots, x_6$ of the roots of f in its splitting field, and denote by (ij) the difference $x_i - x_j$. Then we define the *Igusa-Clebsch invariants* of C to be

$$\begin{aligned} I_2 &= c^2 \sum (12)^2(34)^2(56)^2, \\ I_4 &= c^4 \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2, \\ I_6 &= c^6 \sum (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2, \\ I_{10} &= c^{10} \prod (12)^2, \end{aligned}$$

where each sum and product runs over the distinct expressions obtained by applying a permutation to the index set $\{1, \ldots, 6\}$.

These invariants are integral whenever f is integral. The Igusa-Clebsch invariants are 'invariants for the Siegel moduli space'. Before making this more precise, we recall some facts about the Siegel moduli space.

Definition 2.5.2. We define

$$\mathrm{Sym}_2(\mathbb{C}) = \left\{ \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_3 \end{pmatrix} \in \mathrm{Mat}_{2\times 2}(\mathbb{C}) \right\},$$

and for $\tau \in \mathrm{Sym}_2(\mathbb{C})$, we define $\Im(\tau) > 0$ to mean that τ is positive definite.

Definition 2.5.3. The *Siegel upper half space* is defined to be

$$\mathbb{H}_2 = \left\{ \tau = \begin{pmatrix} \tau_1 & \tau_2 \\ \tau_2 & \tau_4 \end{pmatrix} \in \mathrm{Sym}_2(\mathbb{C}) : \mathrm{Im}(\tau) > 0 \right\},$$

and the symplectic group

$$\mathrm{Sp}_2(\mathbb{Z}) = \left\{ \gamma \in \mathrm{GL}_4(\mathbb{Z}) : g \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} g^{\mathrm{tr}} = \begin{pmatrix} 0 & I_2 \\ -I_2 & 0 \end{pmatrix} \right\}$$

acts on $\mathbb{H}_2$ via

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \tau = (A\tau + B)(C\tau + D)^{-1}.$$

In [Igu60], Igusa defined three Siegel modular functions

$$i_1, i_2, i_3 : \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2 \longrightarrow \mathbb{C}$$

that generate the ring of rational functions of the coarse moduli space for hyperelliptic curves of genus 2. Furthermore, if C is a curve of genus 2, and $\tau \in \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2$ is the point in the moduli space corresponding to C, then

$$i_1(\tau) = (I_4 I_6 / I_{10})(C), \tag{2.1}$$

$$i_2(\tau) = (I_2^3 I_4 / I_{10})(C), \tag{2.2}$$

$$i_3(\tau) = (I_2^2 I_6 / I_{10})(C). \tag{2.3}$$

Now, the forgetful functor

$$\begin{array}{ccc} \mathbf{POrd}_{\mathbb{C},K_0} & \longrightarrow & \mathbf{POrd}_{\mathbb{C}} \\ (\mathrm{A}, \xi, \iota) & \mapsto & (\mathrm{A}, \xi) \end{array}$$

induces a map

$$\phi : \mathrm{SL}_2(\mathcal{O}_{K_0})\backslash K_0 \otimes \mathbb{H} \to \mathrm{Sp}_2(\mathbb{Z})\backslash\mathbb{H}_2,$$

which is generically 2-1. We will refer to this as the *modular map*. The image of the graded ring of Hilbert modular forms $\mathcal{M}_{K_0}$ under this map is called the *Humbert surface for* K_0, and is denoted as $\mathcal{H}_{K_0}$. That is, the modular map ϕ induces a degree 2 quotient map

$$\phi : \mathcal{M}_{K_0} \longrightarrow \mathcal{H}_{K_0}.$$

In particular, as there exist 2 algebraically independant Siegel modular functions j_1 and j_2 in $\mathbb{C}(\mathcal{H}_{K_0})$, which generically will be in $\mathbb{C}(i_1, i_2, i_3)$, we get 2 algebraically independent Hilbert modular functions

$$J_1 = \phi^* j_1 \quad J_2 = \phi^* j_2 \tag{2.4}$$

in $\mathbb{C}(\mathcal{M}_{K_0})$, written as pullbacks of the Igusa invariants. Furthermore, by construction, we get that J_1 and J_2 are *symmetric*, that is, that if σ is the generator of $\mathrm{Gal}(K_0/\mathbb{Q})$, then for all $\tau \in K_0 \otimes \mathbb{H}$, we have that

$$J_1(\sigma(\tau)) = J_1(\tau) \quad J_2(\sigma(\tau)) = J_2(\tau).$$

Recall now from Lemma 2.2.3 that if $\overline{V}$ is the Hilbert modular variety, then there exists $J_3 \in \mathbb{C}(\overline{V})$ such that

$$\mathbb{C}(\overline{V}) = \mathbb{C}(J_1, J_2)(J_3).$$

Hence, if we write $m(X) \in \mathbb{C}(J_1, J_2)[X]$ for the minimal polynomial of J_3, then $m(X)$ is the pullback along ϕ of a polynomial in $\mathbb{C}(i_1, i_2, i_3)[X]$.

The subtlety of how to choose the root of $m(X)$ in practise is addressed in Algorithm 2.7.3, Step 2.

Example 2.5.4. Gundlach [Gun63] and Müller [Mul85] computed formulae for a choice of isomorphism invariants J_1, J_2, and J_3 for $K_0 = \mathbb{Q}(\sqrt{5})$, and gave the functions from which J_1, J_2, and J_3^2 (here $m(X)$ is quadratic) are pulled back along ϕ:

$$J_1 = \phi^* \left(\frac{2^{-6}3^{-3}i_1^2 i_2^2 + 2^{-3}3^2 i_1 i_2^2 - 2^{-4}3^{-3} i_1 i_3^3 + 2^{-5}3^2 i_2 i_3^2}{i_1^2 i_2^2 + 2^2 3^5 i_1 i_2^2} \right), \tag{2.5}$$

$$J_2 = \phi^* \left(\frac{2^9 i_1^3 i_2^2 + 2^{11} 3^5 i_1^2 i_2^2}{i_1^2 i_2^2 + 2^2 i_1 i_3^3 - 2 \cdot 3^5 i_2 i_3^2} \right), \tag{2.6}$$

$$\begin{aligned} J_3^2 = {} & 5^5 - 2^{-1}5^3 J_1 J_2 + 2^{-4} J_2 + 2^{-1}3^2 5^2 J_2^2 J_1^3 - 2^{-3} J_1^2 J_2^2 - 2 \cdot 3^3 J_2^3 J_1^5 \\ & + 2^{-4} J_2^3 J_1^4 \end{aligned} \tag{2.7}$$

Remark 2.5.5. For each choice of K_0, we have to recalculate RM isomorphism invariants J_1, J_2, and J_3. In [LNY15, Theorem 2.2], Lauter, Naehrig, and Yang give a method to calculate a choice of Siegel modular functions j_1 and j_2 as in (2.4), but the minimal polynomial of J_3 in $\mathbb{C}(J_1, J_2)$ is not known in general.

2.6 Defining RM isomorphism invariants over a finite field

Note that we defined Igusa-Clebsch invariants in Definition 2.5.1 for genus 2 curves over any field with characteristic different from 2. Indeed, two genus 2 curves over a finite field $\mathbb{F}_q$ for q odd are isomorphic over $\overline{\mathbb{F}_q}$ if and only if they have the same Igusa invariants. We would like to also be able to define RM isomorphism invariants over $\mathbb{F}_q$, which we do via the Igusa invariants. For this we use the canonical lifts of Chapter 1.

Definition 2.6.1. We say that $(\mathrm{B}, \zeta, \iota) \in \mathbf{POrd}_{\mathbb{Q}_q^{\mathrm{ur}}, K_0}$ is the *canonical lift* of $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{F}_q, K_0}$ if, writing Frob_q for the q-power Frobenius of A and $\pi = \iota(\mathrm{Frob}_q)$, there exists $(\mathfrak{a}, \beta) \in \mathbf{PId}_{\pi, K_0}$ such that

- (A, ξ) corresponds to $(\mathfrak{a}, \beta)$ under the functor of Theorem 1.3.11, and
- $(\mathfrak{a}, \beta)$ maps to (B, ζ) under the functor of Theorem 1.5.4.

We will show in Proposition 2.6.5 that given a genus 2 curve $C/\mathbb{F}_q$, the canonical lift of its Jacobian is the Jacobian of some naïve lift of C to $\mathbb{Q}_q^{\mathrm{ur}}$. This will allow us in Corollary 2.6.7 to use the Igusa invariants to define RM isomorphism invariants over $\mathbb{F}_q$.

Definition 2.6.2. Denote by $\mathbb{Z}_q^{\mathrm{ur}}$ the ring of Witt vectors of $\overline{\mathbb{F}_q}$, and let $C/\mathbb{Q}_q^{\mathrm{ur}}$ be a geometrically irreducible curve with minimal regular model $\mathcal{C}/\mathbb{Z}_q^{\mathrm{ur}}$. Write P for the open subfunctor of $\mathrm{Pic}_{\mathcal{C}/\mathbb{Z}_q^{\mathrm{ur}}}$ given by line bundles of total degree 0, and E for the schematic closure in P of the unit section $\mathrm{Spec}(\mathbb{Q}_q^{\mathrm{ur}}) \to P \times_{\mathbb{Q}_q^{\mathrm{ur}}} \mathbb{Q}_q^{\mathrm{ur}}$. We define the *quasi-Jacobian* of $\mathcal{C}$ to be P/E.

Remark 2.6.3. If $\mathcal{C}$ is smooth over $\mathbb{Z}_q^{\mathrm{ur}}$, then the quasi-Jacobian of $\mathcal{C}$ is just the Jacobian of $\mathcal{C}$.

Theorem 2.6.4. *Let $C/\mathbb{Q}_q^{\mathrm{ur}}$ be a geometrically irreducible curve with Jacobian $J/\mathbb{Q}_q^{\mathrm{ur}}$, and let $\mathcal{C}/\mathbb{Z}_q^{\mathrm{ur}}$ be the minimal regular model of C. Then the quasi-Jacobian of $\mathcal{C}$ is the Nëron model of J.*

Proof. See [BLR90, Chapter 9, Theorem 4]. □

Proposition 2.6.5. Let C be a genus 2 curve over $\mathbb{F}_q$ for which the Jacobian $\mathrm{Jac}(C) = (\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{F}_q, K_0}$, and let $(\mathrm{B}, \zeta, \iota) \in \mathbf{POrd}_{\mathbb{Q}_q^{\mathrm{ur}}, K_0}$ be the canonical lift of (A, ξ, ι). By Torelli's Theorem, up to isomorphism there exists a unique curve $D/\mathbb{Q}_q^{\mathrm{ur}}$ with Jacobian $(\mathrm{B}, \zeta, \iota)$. Define $\mathcal{C}/\mathbb{Z}_q^{\mathrm{ur}}$ to be the minimal regular model of D, and $C'/\mathbb{F}_q$ to be the reduction of $\mathcal{C}$ mod q. Then

$$C' \times_{\mathbb{F}_q} \overline{\mathbb{F}_q} = C \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}.$$

Proof. Denote by $\mathcal{J}/\mathbb{Z}_q^{\mathrm{ur}}$ the canonical lift of $\mathrm{Jac}(C)$ to $\mathbb{Z}_q^{\mathrm{ur}}$. Then $\mathcal{J}$ is the Néron model of J and hence by Theorem 2.6.4 and the universal property of the Néron map, we have that $\mathcal{J}$ is the quasi-Jacobian of $\mathcal{C}$. In particular, this implies that

$$\mathrm{Jac}(C') \times_{\mathbb{F}_q} \overline{\mathbb{F}_q} = \mathcal{J} \times_{\overline{\mathbb{F}_q}} \overline{\mathbb{F}_q} = \mathrm{Jac}(C) \times_{\mathbb{F}_q} \overline{\mathbb{F}_q},$$

and hence by the Torelli theorem, we have that

$$C' \times_{\mathbb{F}_q} \overline{\mathbb{F}_q} = C \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}.$$

□

Proposition 2.6.6. Let $C/\mathbb{Q}_p^{\mathrm{ur}}$ be a genus 2 curve defined by an affine equation

$$y^2 = P(x),$$

with $P(x) \in \mathbb{Q}_p^{\mathrm{ur}}[x]$ separable. Then C has good reduction if and only if after a suitable change of variables we can define C by

$$y^2 = P_0(x) \in \mathbb{Z}_q^{\mathrm{ur}}[x]$$

such that the reduction of P_0 mod q to give a polynomial in $\mathbb{F}_q[x]$ is separable of degree 5 or 6.

Proof. See [Liu02, Example 10.1.26]. □

Corollary 2.6.7. Let (J_1, J_2, J_3) be a choice of RM isomorphism invariants for K_0 such that J_1 and J_2 are symmetric Hilbert modular functions. For $(\mathrm{A}, \xi, \iota), (\mathrm{A}', \xi', \iota') \in \mathbf{POrd}_{\mathbb{F}_q, K_0}$, write $(\mathrm{B}, \zeta, \iota)$ and $(\mathrm{B}', \zeta', \iota') \in \mathbf{POrd}_{\mathbb{Q}_q^{\mathrm{ur}}, K_0}$ for the canonical lifts of (A, ξ, ι) and $(\mathrm{A}', \xi', \iota')$ respectively. Then (A, ξ) and (A', ξ') are isomorphic over $\overline{\mathbb{F}_q}$ as elements of $\mathbf{POrd}_{\mathbb{F}_q}$ if and only if

$$(J_1, J_2)(\mathrm{B}, \zeta) \equiv (J_1, J_2)(\mathrm{B}', \zeta') \bmod q.$$

Proof. Let $D/\mathbb{Q}_q^{\mathrm{ur}}$ and $D'/\mathbb{Q}_q^{\mathrm{ur}}$ be the genus 2 curves with Jacobians (B, ζ) and (B', ζ') respectively. Then by Proposition 2.6.5 both D and D' have good reduction at q, and hence by Proposition 2.6.6, both D and D' have a hyperelliptic model. Let C and C' be the genus 2 curves over $\mathbb{F}_q$ defined by the hyperelliptic models given by reducing D and D' mod q respectively. Then by Proposition 2.6.5, the Jacobians of $C \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ and $C' \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ are given by $(\mathrm{A}, \xi) \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ and $(\mathrm{A}', \xi') \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ respectively. Recall that the Igusa invariants (i_1, i_2, i_3) were defined in terms of the coefficients of an affine hyperelliptic model, hence, we have that (A, ξ) and (A', ξ') are isomorphic over $\overline{\mathbb{F}_q}$ if and only if

$$(i_1, i_2, i_3)(D) \equiv (i_1, i_2, i_3)(D') \bmod q.$$

Furthermore, recall from Equation (2.4) that the Igusa invariants (i_1, i_2, i_3) determine (J_1, J_2) and vice versa. □

Definition 2.6.8. Let q be a prime power, and suppose that (A, ξ, ι) is the Jacobian of a genus 2 curve C defined over $\mathbb{F}_q$. Fix a choice (J_1, J_2, J_3) of RM isomorphism invariants for K_0, and let U be the Zariski-open subvariety of the Hilbert modular variety $\overline{V}$ on which the rational map

$$(J_1, J_2, J_3) : \overline{V} \dashrightarrow \mathbb{C}^{\times 3}$$

is an injective morphism. Write $(\mathrm{B}, \zeta, \iota)$ for the canonical lift of (A, ξ, ι) to $\mathbb{Q}_q^{\mathrm{ur}}$, and suppose that $(\mathrm{B}, \zeta, \iota) \in U$. Then we define the *$\mathbb{F}_q$-RM isomorphism invariant* of (A, ξ, ι) to be

$$(J_1(\mathrm{B}, \zeta, \iota), J_2(\mathrm{B}, \zeta, \iota), J_3(\mathrm{B}, \zeta, \iota)) \bmod q.$$

In particular, given explicit formulae for Equation (2.4), we can compute the the $\mathbb{F}_q$-RM isomorphism invariants of a genus 2 curve C easily via the relations

$$\begin{aligned} J_1((\mathrm{B}, \zeta, \iota)) &\equiv (\phi^* j_1)(C) \bmod q \\ J_2((\mathrm{B}, \zeta, \iota)) &\equiv (\phi^* j_2)(C) \bmod q \\ m(X)((\mathrm{B}, \zeta, \iota)) &\equiv (\phi^* m(X))(C) \bmod q, \end{aligned}$$

up to the choice of root of $m(X)$ for J_3.

Remark 2.6.9. Suppose that $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{F}_q, K_0}$. The $\mathbb{F}_q$-RM isomorphism invariant of $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{F}_q, K_0}$ determines (A, ξ) up to isomorphism, but not (A, ξ, ι). However, one of the roots of $m(X)$ gives the correct invariant, and in practise we can check this.

2.7 Complexity and simplifications for genus 2

Lemma 2.7.2 gives one simplification of the formulae for genus 2, which in particular implies that $\mathcal{O}_{K_0}$ and $\mathcal{O}_{K_0}^\vee$ are isomorphic as $\mathcal{O}_{K_0}$-modules. This means that we may define the Hilbert modular variety as a compactification of

$\mathrm{SL}_2(\mathcal{O}_{K_0})\backslash(K_0\otimes\mathbb{H})$ or $\mathrm{SL}_2(\mathcal{O}_{K_0})\backslash(K_0\otimes\mathbb{H}^-)$ instead of $\mathrm{SL}(\mathcal{O}_{K_0}\oplus\mathcal{O}_{K_0}^\vee)\backslash(K_0\otimes\mathbb{H})$. When we do this, in Lemma 2.3.6, we must replace the matrix group $\Gamma^0(\mu)$ with the matrix group $\Gamma^0(\mu)'$, which we now define.

Definition 2.7.1. For a totally real number field K_0 of degree 2 over $\mathbb{Q}$, with ring of integers $\mathcal{O}_{K_0}$, and a totally positive element $\mu \in K_0$, we define

$$\Gamma^0(\mu)' = \left\{ \begin{pmatrix} a & \mu b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathcal{O}_{K_0}) : a, b, c, d \in \mathcal{O}_{K_0} \right\}.$$

Lemma 2.7.2. For a totally real number field K_0 of degree 2 over $\mathbb{Q}$ with ring of integers $\mathcal{O}_{K_0}$, and a totally positive element $\mu \in \mathcal{O}_{K_0}$ that generates a prime ideal, the set

$$\mathcal{C} = \left\{ \begin{pmatrix} 1 & \omega \\ 0 & 1 \end{pmatrix} : \omega \in \mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0} \right\} \bigcup \left\{ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

is a choice of coset representatives for the quotient of groups $\Gamma^0(\mu)'\backslash\mathrm{SL}_2(\mathcal{O}_{K_0})$.

Proof. The matrix group $\mathrm{SL}_2(\mathcal{O}_{K_0})$ acts on $\mathbb{P}^1(\mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0})$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot (x : y) = (ax + by : cx + dy).$$

Then in particular, the stabilizer of $(0 : 1)$ is given by $\Gamma^0(\mu)'$, and hence by the orbit-stabilizer theorem, there exists a natural bijection from $\mathcal{C}$ to $\Gamma^0(\mu)'\backslash\mathrm{SL}_2(\mathcal{O}_{K_0})$. □

We can currently only implement this algorithm in genus 2, and only for small quadratic fields K_0, due to the fact that we do not know explicit q-expansions for the RM invariants $J_1, \ldots, J_{g+1}$ in any other case. Hence, we restrict now to the genus 2 case.
Algorithm 2.4.1 is extremely slow and uses a lot of memory, and so we give here some practical improvements on the computation time and memory usage. First of all, we do not compute the third modular polynomial $H_{\mu,3}(X_1, X_2, X_3, Y, Z_3)$; Algorithm 2.7.3 shows that, given $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{C},K_0}$, we can compute every abelian surface μ-isogenous to it without using $H_{\mu,3}$.

Algorithm 2.7.3.
INPUT: The first 2 Hilbert modular polynomials $G_\mu(X_1, X_2, X_3, Y)$ and $H_{\mu,2}(X_1, X_2, X_3, Y, Z_2)$, as defined in Definition 2.1.5, the RM isomorphism invariants $(j_1, j_2, j_3) \in \mathbb{C}^3$ of some $(\mathrm{A}, \xi, \iota) \in \mathbf{POrd}_{\mathbb{C},K_0}$, as defined in Definition 2.1.1, and the minimal polynomial $m(X) \in \mathbb{C}(J_1, J_2)[X]$ of J_3, as in Section 2.5.
OUTPUT: The RM isomorphism invariants of each $(\mathrm{A}', \xi', \iota') \in \mathbf{POrd}_{\mathbb{C},K_0}$ that is μ-isogenous to (A, ξ, ι).

1. Set L to be the list of the $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) + 1$ roots of $G_\mu(j_1, j_2, j_3, Y)$.
2. For every $j_1' \in L$:

(a) set j_2' to be the unique element of $\mathbb{C}$ for which $H_{\mu,2}(j_1, j_2, j_3, j_1', j_2') = 0$,

(b) set L_0 to be the list of the roots of $m(X)$ evaluated at $(J_1, J_2) = (j_1', j_2')$.

(c) for every $l \in L_0$, check if $G_\mu(j_1', j_2', l, j_1) = 0$. If true, set $j_3' = l$.

(d) add (j_1', j_2', j_3') to list L'

3. Return L'.

The second major improvement is to use the Chinese Remainder Theorem. From Theorem 2.1.9, we see that for all but finitely many primes p, if we replace $\mathbb{Q}$ by $\mathbb{F}_p$ in Algorithm 2.4.1, then the algorithm outputs at least G_μ and $H_{\mu,2}$ mod p. One advantage of working over a finite field in place of $\mathbb{Q}$ is that while the algorithm is running over $\mathbb{Q}$, the coefficients of the q-expansions blow up, using up memory space and slowing down computations, so that Algorithm 2.7.4 is significantly faster than Algorithm 2.4.1.

Algorithm 2.7.4.
INPUT:

1. A totally real number field K_0 of degree 2 over $\mathbb{Q}$.

2. The q-expansions of generators $\gamma_1, \ldots, \gamma_s$ of the $\mathbb{Z}$-module $\mathcal{M}_{K_0}(\mathbb{Z})$.

3. RM isomorphism invariants J_1, J_2, J_3 for K_0 as defined in Definition 2.1.1, written in terms of $\gamma_1, \ldots, \gamma_s$.

4. A totally positive element $\mu \in K_0$ that generates a prime ideal.

5. An upper bound B on the coefficients of the Hilbert modular polynomials $G_\mu(X_1, X_2, X_3, Y)$ and $H_{\mu,2}(X_1, X_2, X_3, Y, Z_2)$.

6. An integer p_0 such that for every prime $p > p_0$, the RM isomorphism invariants of Definition 2.6.8 are well-defined for $\mathbb{F}_p$.

OUTPUT: The first 2 polynomials

$$G_\mu(X_1, X_2, X_3, Y) \in \mathbb{Z}[X_1, X_2, X_3, Y], \text{ and}$$
$$H_{\mu,2}(X_1, X_2, X_3, Y, Z_2) \in \mathbb{Z}[X_1, X_2, X_3, Y, Z_2]$$

of Definition 2.1.5.

1. Create a list L of primes in the following way:

(a) Set $i = 0$.

(b) Set $p_{i+1} = \min\{n \in \mathbb{Z}_{>p_i} : n \text{ prime}, n \equiv 1 \bmod \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)\}$.

(c) If $\prod_{j=1}^{i+1} p_j < B$ then set $i = i + 1$ and go to (b). Else return

$$L = \{p_1, \ldots, p_{i+1}\}.$$

2. Compute $G_\mu(X_1, X_2, X_3, Y)$ and $H_{\mu,2}(X_1, X_2, X_3, Y, Z_2)$ mod p for every $p \in L$ by following Algorithm 2.4.1, with $\mathbb{Q}$ replaced by $\mathbb{F}_p$. (This can be done in parallel).

3. Use the Chinese Remainder Theorem to compute G_μ and $H_{\mu,2}$.

Remark 2.7.5. The condition that the primes in the list should be 1 mod $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)$ is there to simplify, and therefore speed up, the computation. This speed up occurs because $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)^{\text{th}}$ roots of unity appear in the q-expansions of the coefficients of $\Phi_\mu(Y)$ and $\Psi_{\mu,2}(Y, Z_2)$; this can be seen by writing out the explicit formulae for the q-expansions using Definition 2.3.3. Restricting to finite fields $\mathbb{F}_p$ for which these roots of unity are in the field means that the computations do not have be done in a field extension.

The disadvantage of Algorithm 2.7.4 is that the output is currently not provable, since we do not yet know how to compute the input variables B or p_0. However, the speed up is quite significant: for $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) = 11$, Algorithm 2.4.1 took 1 week and Algorithm 2.7.4 took 90 minutes. With this in mind, in order to be able to compute more polynomials, we are forced to settle for guessing B and p_0 and checking the output by looking at the behaviour of the polynomials, for example by attempting to run Algorithm 2.7.3. Even with these improvements, there is still a long way to go before this algorithm is practical; Table 2.1 gives the timings for the computations that we have done so far.

$\mathrm{Disc}(K_0)$	8	5	5	5	5	5
$\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)$	2	4	5	9	11	19
Time	2 secs	63 secs	90 secs	$\sim$ 4 mins	$\sim$ 90 mins	$\sim$ 3 days

Table 2.1: Timings for computation of Hilbert modular polynomials G_μ and $H_{\mu,2}$

Chapter 3

The structure of μ-isogeny graphs

The main theorem of this chapter, the Volcano Theorem, Theorem 3.1.9, gives the complete structure of the graph of μ-isogenies of principally polarised abelian varieties over a finite field of dimension g with real multiplication by a given maximal order. We defined μ-isogenies in Definition 1.3.4; the definition is recalled below. This is a generalisation of David Kohel's structure theorem for $g = 1$ in [Koh96], and Ionica and Thomé's work on genus 2 curves with maximal real multiplication by a given field with narrow class number 1 in their preprint [IT14]. In parallel to the work in this thesis, Brooks, Jetchev, and Wesolowski recently accounced some overlapping results, proven using different methods, in their preprint [BJW16].

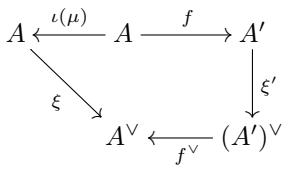
3.1 The Volcano Theorem

Let q be a prime power, let π be a Weil q-number, and let K be a CM-field of degree $2g$ over $\mathbb{Q}$ such that $K = \mathbb{Q}(\pi)$. Recall from Definition 1.3.4 that $\mathbf{POrd}_{\pi,K_0}$ denotes the category of principally polarised ordinary abelian varieties (A, ξ) over $\mathbb{F}_q$ such that the characteristic polynomial of the q-power Frobenius equals the minimal polynomial of π, together with an embedding $\mathcal{O}_{K_0} \hookrightarrow \mathrm{End}(\mathrm{A})$. The only morphisms in this category were isomorphisms.

Recall also from Definition 1.3.2 that for a totally positive element $\mu \in \mathcal{O}_{K_0}$ for which $\mu\mathcal{O}_{K_0}$ is a prime ideal, and for $(\mathrm{A}, \xi), (\mathrm{A}', \xi') \in \mathbf{POrd}_{\pi,K_0}$ with $\iota : \mathcal{O}_{K_0} \hookrightarrow \mathrm{End}(\mathrm{A})$, we define a μ-isogeny

$$f : (\mathrm{A}, \xi) \longrightarrow (\mathrm{A}', \xi')$$

to be a morphism $\mathrm{A} \to \mathrm{A}'$ of abelian varieties such that the diagram



commutes.

We also fix a totally positive element $\mu \in \mathcal{O}_{K_0}$ such that $\mu\mathcal{O}_{K_0}$ is a prime ideal.

Definition 3.1.1. Assume that the only roots of unity in $\mathcal{O}_K$ are $\{\pm 1\}$. The *μ-isogeny graph for the Weil q-number π* is a weighted undirected graph for which:

1. The vertices are the isomorphism classes of objects in $\mathbf{POrd}_{\pi,K_0}$,
2. There is an edge between V and V' if and only if there exists a μ-isogeny from V to V'.
3. If a μ-isogeny is f satisfies $f^\vee = \pm f$, then the edge corresponding to this isogeny has weight $\frac{1}{2}$.
4. All other edges have weight 1 and this will not be notated.

Remark 3.1.2. In fact, given that the only roots of unity in $\mathcal{O}_K$ are $\{\pm 1\}$, if there exists a μ-isogeny f between V and V', then the set of μ-isogenies between V and V' is exactly

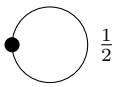
$$\{f, -f, f^\vee, -f^\vee\}.$$

That is, the weight of an edge between V and V' in a μ-isogeny graph denotes the total number of μ-isogenies between V and V' divided by 4.

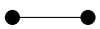
Definition 3.1.3. We define the graphs I, R_1, R_2, and for $n \in \mathbb{Z}_{\geq 0}$, the graph C_n in the following way:

- The graph I is a single vertex with no edges.

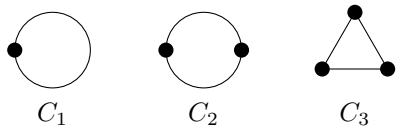
- The graph R_1 is a single vertex with one edge of weight $\frac{1}{2}$.



- The graph R_2 is a pair of vertices joined by a single edge of weight 1.



- For $n \in \mathbb{Z}_{\geq 1}$, the graph C_n is a cycle of length n where every edge has weight 1.



Definition 3.1.4. For a connected graph G, and vertices V and $V' \in G$, we define the *distance from V to V'*, notated $D(V, V')$, to be the length of the shortest path in G connecting V and V'. If G' is a subgraph of G, for any vertex $V \in G$, we define the *distance from V to G'* to be

$$D(V, G') = \min\{D(V, V') : V' \in G'\}.$$

Definition 3.1.5. Let G be a connected graph and let G' be a subgraph of G. Suppose that E is an edge in G connecting V and V', and write $D(V, G') = d$. If $D(V', G') = d-1$, then we say that E *ascends from* V, and if $D(V', G') = d+1$, then we say that E *descends from* V.

Definition 3.1.6. For $v \in \mathbb{Z}_{\geq 1}$, $d, n \in \mathbb{Z}_{\geq 0}$, and $\Gamma \in \{I, R_1, R_2, C_n\}$, the (Γ, v, d)-*volcano* is a weighted undirected connected graph G given as follows:

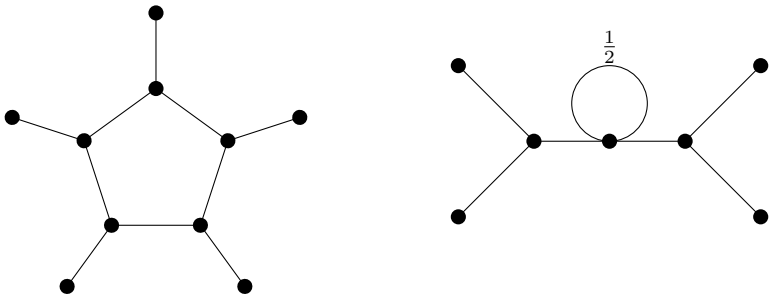
1. If $d = 0$, define $G = \Gamma$.
2. If $d > 0$, define the tree $T(v, v', d)$ of root r to be the tree with
   - v' edges descending from r,
   - 1 edge ascending from every vertex V such that $D(V, r) > 0$,
   - $v - 1$ edges descending from every vertex V such that $D(V, r) < d$,

   and no other edges. Let G be obtained from Γ by, for each vertex V of Γ, glueing a copy of $T(v, v'd)$ at $V = r$, where

$$v' = \begin{cases} v & \Gamma = I \\ v-1 & \Gamma = R_n \\ v-2 & \Gamma = C_n. \end{cases}$$

This definition was chosen in such a way that every vertex has v edges, counted with weights, except for those at distance d from Γ.

Example 3.1.7. Here is a $(C_5, 3, 1)$-volcano and an $(R_1, 3, 2)$-volcano.



Definition 3.1.8. Let $\mathcal{O}$ be an order in $\mathcal{O}_K$ which contains $\mathcal{O}_{K_0}$ and such that $\overline{\mathcal{O}} = \mathcal{O}$, where $^-$ denotes complex conjugation. The *Shimura class group* of $\mathcal{O}$ is defined to be

$$\mathrm{SCl}(\mathcal{O}) = \frac{\{(\mathfrak{a}, \lambda) : \mathfrak{a} \text{ an invertible } \mathcal{O}\text{-ideal, } \mathrm{End}(\mathfrak{a}) = \mathcal{O},\ \lambda \in K_0^+,\ \mathfrak{a}\overline{\mathfrak{a}} = \lambda\mathcal{O}\}}{\{(v\mathcal{O}, v\overline{v})) : v \in K^\times,\ v\overline{v} \in K_0^+\}},$$

where K_0^+ denotes the group of totally positive elements of $K_0^\times$.

The purpose of this section will be to prove the Volcano Theorem, below, which is our analogue to the results for elliptic curves first given by David Kohel in [Koh96].

Theorem 3.1.9 (Volcano Theorem)**.** *Let K be a CM-field of degree $2g$, generated over $\mathbb{Q}$ by a Weil q-number π, and with maximal totally real subfield K_0. Suppose further that the only roots of unity in $\mathcal{O}_K$ are $\{\pm 1\}$. Let μ be a totally positive element of $\mathcal{O}_{K_0}$ such that $\mu\mathcal{O}_{K_0}$ is a prime ideal. Define*

$$v = \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) + 1$$

and

$$d = \max\{n \in \mathbb{Z} : (\mathbb{Z}[\pi, \overline{\pi}] : \mathcal{O}_K) \subseteq \mu^n \mathcal{O}_K\}.$$

If $\mu\mathcal{O}_K$ splits in $\mathcal{O}_K$ as $\mu\mathcal{O}_K = \mathfrak{m}\overline{\mathfrak{m}}$, then define n to be the order of $(\mathfrak{m}, \mu)$ in $\mathrm{SCl}(\mathcal{O}_K)$. Now define

$$\Gamma = \begin{cases} I & \text{if } \mu\mathcal{O}_K \text{ is inert,} \\ C_n & \text{if } \mu\mathcal{O}_K \text{ is split,} \\ R_n & \text{if } \mu\mathcal{O}_K \text{ is ramified.} \end{cases}$$

Then every connected component of the μ-isogeny graph for Weil q-number π is a (Γ, v, d)-volcano.

Our first goal will be to understand how μ-isogenous abelian varieties can differ. As isogenies preserve the endomorphism algebra, looking at the endomorphism rings of μ-isogenous abelian varieties is a natural place to begin - in fact the endomorphism ring of any abelian variety in our μ-isogeny graph will be an order in $\mathcal{O}_K$ that contains $\mathcal{O}_{K_0}[\pi, \overline{\pi}]$, by assumption. ?put this in subsection

Lemma 3.1.10. There is a bijection of sets

$$\begin{array}{ccc} \{\text{Ideals of } \mathcal{O}_{K_0}\} & \leftrightarrow & \left\{ \begin{array}{c} \text{Orders } \mathcal{O} \text{ in } \mathcal{O}_K \\ \text{s.t. } \mathcal{O} = \overline{\mathcal{O}} \\ \text{and } \mathcal{O}_{K_0} \subseteq \mathcal{O} \end{array} \right\} \\ \mathfrak{f} & \mapsto & \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K \\ (\mathcal{O} : \mathcal{O}_K) \cap \mathcal{O}_{K_0} & \leftarrow\!\shortmid & \mathcal{O}. \end{array}$$

Proof. We first show that for an ideal $\mathfrak{f}$ of $\mathcal{O}_{K_0}$, we have that

$$(\mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K : \mathcal{O}_K) = \mathfrak{f}\mathcal{O}_K. \tag{3.1}$$

As $\mathfrak{f}\mathcal{O}_K \subseteq \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K$, clearly

$$\mathfrak{f}\mathcal{O}_K = (\mathfrak{f}\mathcal{O}_K : \mathcal{O}_K) \subseteq (\mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K : \mathcal{O}_K).$$

So suppose for a contradiction that there exists $\alpha \in \mathcal{O}_{K_0} - \mathfrak{f}$ such that

$$\alpha\mathcal{O}_K \subseteq \mathcal{O}_{K_0} + \mathfrak{f}\mathcal{O}_K.$$

Recall that K is a totally imaginary quadratic extension of K_0, so that we can choose a totally imaginary element $\varphi \in K$ such that

$$\mathcal{O}_K = \mathcal{O}_{K_0} + \varphi\mathcal{O}_{K_0}.$$

In particular, this implies that

$$\alpha\varphi \in \mathcal{O}_{K_0} + \varphi\mathfrak{f},$$

and hence $\alpha \in \mathfrak{f}$. So (3.1) holds. Now suppose that $\mathcal{O}$ is an order in $\mathcal{O}_K$ such that $\mathcal{O} = \overline{\mathcal{O}}$ and $\mathcal{O}_{K_0} \subseteq \mathcal{O}$. Define $\mathfrak{f}_\mathcal{O} = (\mathcal{O} : \mathcal{O}_K)$. Then $\mathfrak{f}_\mathcal{O}$ is an $\mathcal{O}_K$-ideal, and $\mathcal{O}_K$ is a Dedekind domain, so by [Bass63], there exist $a, b \in \mathcal{O}_K$ such that

$$\mathfrak{f}_\mathcal{O} = a\mathcal{O}_K + b\mathcal{O}_K.$$

In particular, we have that

$$\overline{a}\mathcal{O}_K + \overline{b}\mathcal{O}_K = \overline{\mathfrak{f}_\mathcal{O}} = \mathfrak{f}_\mathcal{O} = a\mathcal{O}_K + b\mathcal{O}_K,$$

which **add details** implies that

$$(\mathfrak{f}_\mathcal{O} \cap \mathcal{O}_{K_0})\mathcal{O}_K = \mathfrak{f}_\mathcal{O}.$$

□

Recall that orders are classified by their conductors; before giving the proof of the Volcano theorem we give some useful definitions.

Definition 3.1.11. Let $\mathcal{O} \subseteq \mathcal{O}_K$ be an order in K. We define the *conductor ideal* of $\mathcal{O}$ to be

$$\mathfrak{f}_\mathcal{O} = (\mathcal{O} : \mathcal{O}_K) = \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\}.$$

For $\mu \in \mathcal{O}_K$, we define the *conductor of $\mathcal{O}$ locally at μ* to be $\mu^k\mathcal{O}_K$, where

$$k = \max_{n \in \mathbb{Z}}\{\mathfrak{f}_\mathcal{O} \subseteq \mu^n\mathcal{O}_K\}.$$

We define the *non-μ-part of the conductor* to be $\mu^{-k}\mathfrak{f}_\mathcal{O}$.

Definition 3.1.12. Suppose that we have a μ-isogeny $\phi \in \mathbf{PId}_{\pi,K_0}$ given by

$$\phi : (\mathrm{A}, \xi) \longrightarrow (\mathrm{A}', \xi').$$

Write $\mathcal{O} = \mathrm{End}(\mathrm{A})$ and $\mathcal{O}' = \mathrm{End}(\mathrm{A}')$. If

(a) $\mu\mathfrak{f}_{\mathcal{O}} = \mathfrak{f}_{\mathcal{O}'}$, then we say that ϕ is *ascending*,

(b) $\mu\mathfrak{f}_{\mathcal{O}'} = \mathfrak{f}_{\mathcal{O}}$, then we say that ϕ is *descending*, and

(c) $\mathfrak{f}_{\mathcal{O}} = \mathfrak{f}_{\mathcal{O}'}$, then we say that ϕ is *horizontal*.

Proposition 3.1.14. *All μ-isogenies are ascending, descending, or horizontal.*

We will prove this in Section 3.1.1. In particular, in any given μ-isogeny graph G, for every non-empty connected component C there exists an ideal $\mathfrak{f}_C \in \mathcal{O}_K$ such that for every vertex $(\mathrm{A}, \xi) \in C$, the non-μ-part of the conductor of $\mathrm{End}(\mathrm{A})$ is $\mathfrak{f}_C$.

Definition 3.1.13. Given a non-empty connected component C of a μ-isogeny graph, we choose a vertex $(\mathrm{A}, \xi) \in C$, and we define the *conductor of C* to be the non-μ-part of the conductor of $\mathrm{End}(\mathrm{A})$, and we denote this by $\mathfrak{f}_C$.

We now give the proof of Theorem 3.1.9. We first prove that the subgraph of a connected component C containing the vertices with endomorphism ring of conductor $\mathfrak{f}_C$ has the form Γ. We then show that from all the other vertices there are no horizontal μ-isogenies and there is a unique ascending μ-isogeny, and recall from Lemma 2.3.6 that there are exactly $\mathrm{Norm}_{K_0/\mathbb{Q}}(\mu)+1$ edges from every vertex that does not have minimal endomorphism ring, so that the result follows from induction.

Proof of Theorem 3.1.9. For a connected component C of a μ-isogeny graph G, let G_C be the subgraph of G given by the connected components of G with conductor $\mathfrak{f}_C$. We first partition G_C by endomorphism ring and look at the action of the Shimura class group on these subsets. More precisely, suppose that we have a non-empty connected component C of a μ-isogeny graph G. Write $\mu^d\mathcal{O}_K$ for the conductor of $\mathcal{O}_{K_0}[\pi, \overline{\pi}]$ locally at μ (this is equivalent to the formula given for d in the Volcano Theorem). By Proposition 3.1.14, we can partition the set of vertices of G_C as

$$\bigsqcup_{i=0}^{d} V(\mu^i \mathfrak{f}_C),$$

where for any ideal I in $\mathcal{O}_K$, we define

$$V(I) = \{(\mathrm{A}, \xi) \in \mathbf{POrd}_{\pi, K_0} : \mathfrak{f}_{\mathrm{End}(\mathrm{A})} = I\}_{/\cong}. \tag{3.2}$$

Proposition 3.1.18. *Let $\mathcal{O}$ be an order in $\mathcal{O}_K$ containing $\mathcal{O}_{K_0}[\pi, \overline{\pi}]$ that is stable under complex conjugation. Then the Shimura Class Group $\mathrm{SCl}(\mathcal{O})$ of $\mathcal{O}$ acts faithfully and transitively on $V(\mathfrak{f}_{\mathcal{O}})$.*

For the proof, see Section 3.1.3.

Proposition 3.1.19. *Let* $(\mathrm{A},\xi) \in V(\mu^i \mathfrak{f}_C)$. *If* $i > 0$, *then there are no horizontal* μ*-isogenies from* (A,ξ). *If* $i = 0$, *then there are exactly* m *horizontal* μ*-isogenies from* (A,ξ), *where*

$$m = \begin{cases} 0 & \mu \text{ is inert in } K \\ 1 & \mu \text{ is ramified in } K \\ 2 & \mu \text{ splits in } K. \end{cases}$$

Furthermore, if there exists a horizontal μ*-isogeny* f *from* (A,ξ), *then there exists* $[(\mathfrak{m},\mu)] \in \mathrm{SCl}(\mathcal{O})$ *such that* f *is isomorphic to a* μ*-isogeny of the form*

$$(\mathrm{A},\xi) \longrightarrow (\mathfrak{m},\mu)\cdot(\mathrm{A},\xi).$$

For the proof, see Section 3.1.4. Now writing $\max_{G_C}$ for the subgraph of the μ-isogeny graph G_C consisting of the vertices in $V(\mathfrak{f}_C)$ and the edges between them, Proposition 3.1.18 and Proposition 3.1.19 tell us that

(a) if μ is inert in K then there no edges in $\max_{G_C}$,

(b) if μ is ramified in K and there is no non-trivial element $[(\mathfrak{m},\mu)] \in \mathrm{SCl}(\mathcal{O}_K)$, then $\max_{G_C}$ is the disjoint union of loops of weight $\frac{1}{2}$,

(c) if μ is ramified in K and there is a non-trivial element $[(\mathfrak{m},\mu)] \in \mathrm{SCl}(\mathcal{O}_K)$, then $\max_{G_C}$ is the disjoint union of pairs of vertices joined by a single edge, and

(d) if μ splits in K as $\mathfrak{m}\overline{\mathfrak{m}}$, then $\max_{G_C}$ is the disjoint union of cycles of length n, where n is the order of $[(\mathfrak{m},\mu)]$ in $\mathrm{SCl}(\mathcal{O})$.

That is, every connected component of $\max_{G_C}$ has exactly the form Γ. Hence, if $d = 0$, then we are done, so assume now that $d > 0$. (Recall that d was the exponent of the conductor $\mu^d\mathcal{O}_K$ of $\mathcal{O}_{K_0}[\pi,\overline{\pi}]$ locally at μ). We first need that every non-empty connected component C' of G_C contains vertices in $V(\mathfrak{f}_C)$, which is an immediate corollary of the following proposition:

Proposition 3.1.21. *If* $i \in \mathbb{Z}_{>0}$ *and* $(\mathrm{A},\xi) \in V(\mu^i\mathfrak{f}_C)$, *then there exists an ascending* μ*-isogeny from* (A,ξ).

For the proof, see Section 3.1.5. Defining

$$v = \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) + 1$$

and

$$v' = \begin{cases} v & \Gamma = I, \\ v-1 & \Gamma = R_n, \\ v-2 & \Gamma = C_n, \end{cases} \tag{3.3}$$

it now suffices to show that each $r \in V(\mathfrak{f}_C)$ is the root of a tree $T(v,v',d)$, where $T(v,v',d)$ is as defined in Definition 3.1.6, and $V(\mathfrak{f}_C) \cap T(v,v'd) = r$. Recall that in Lemma 2.3.6 we proved that there are exactly v non-isomorphic μ-isogenies from each $(\mathrm{A},\xi,\iota) \in \mathbf{PId}_{\mathbb{C},K_0}$. In particular, by Theorem 1.5.4,

from each vertex in $G_C - V(\mu^d \mathfrak{f}_C)$ there are exactly v edges. Hence there are v' descending μ-isogenies from each vertex in $V(\mathfrak{f}_C)$ and there are v edges going away from every vertex in $V(\mu^i \mathfrak{f}_C)$ for $0 < i < d$. It remains only to show that if $i > 0$ then there is a unique ascending μ-isogeny from each vertex in $V(\mu^i \mathfrak{f}_C)$ (recall that there are no horizontal μ-isogenies from these vertices). We show this by induction; first we show that there is a unique ascending μ-isogeny from each vertex in $V(\mu \mathfrak{f}_C)$. From (3.3) we know that there are exactly

$$v' \# V(\mathfrak{f}_C)$$

descending μ-isogenies from $V(\mathfrak{f}_C)$, hence by considering duals, there are exactly $v' \# V(\mathfrak{f}_C)$ ascending μ-isogenies from $V(\mu \mathfrak{f}_C)$.

Proposition 3.1.22.

$$\# V(\mu \mathfrak{f}_C) = v' \# V(\mathfrak{f}_C)$$

and for $i \geq 1$,

$$\# V(\mu^{i+1} \mathfrak{f}_C) = v \# V(\mu^i \mathfrak{f}_C).$$

For the proof, see Section 3.1.6. Hence, there are exactly $\# V(\mu \mathfrak{f}_C)$ ascending μ-isogenies from $V(\mu \mathfrak{f}_C)$, and by Proposition 3.1.21, we know that from each vertex in $V(\mu \mathfrak{f}_C)$ there is at least one ascending μ-isogeny. Therefore, there is a unique ascending μ-isogeny from each vertex in $V(\mu \mathfrak{f}_C)$. The inductive step is the same. □

The rest of this section is dedicated to proving the remaining propositions. For these propositions we will use the Fixed Frobenius Lifting Theorem (Theorem 1.3.11) to work instead in the category $\mathbf{PId}_{\pi, K_0}$ of principally polarised fractional $\mathcal{O}_{K_0}[\pi, \overline{\pi}]$-ideals that we defined in Definition 1.3.9. Recall that the Fixed Frobenius Lifting Theorem gave us an equivalence of categories

$$\mathbf{Ord}_{\pi, K_0} \leftrightarrow \mathbf{Id}_{\pi, K_0}$$

that preserves both the notion of polarisation and of μ-isogeny.

3.1.1 All μ-isogenies are ascending, descending or horizontal

For a totally positive prime element $\mu \in \mathcal{O}_{K_0}$, define ascending, descending, and horizontal μ-isogenies as in Definition 3.1.12. Then:

Proposition 3.1.14. All μ-isogenies are ascending, descending, or horizontal.

Proof. We prove this is the category $\mathbf{Id}_{\pi, K_0}$. It suffices to show that if $(\mathfrak{a}, \beta)$ and $(\mathfrak{a}', \beta') \in \mathbf{PId}_{\pi, K_0}$ are μ-isogenous, with $\mathcal{O} = (\mathfrak{a} : \mathfrak{a})$ and $\mathcal{O}' = (\mathfrak{a}' : \mathfrak{a}')$, then

$$\mathfrak{f}_{\mathcal{O}} = \mu \mathfrak{f}_{\mathcal{O}'}, \quad \mathfrak{f}_{\mathcal{O}'} = \mu \mathfrak{f}_{\mathcal{O}}, \quad \text{or } \mathfrak{f}_{\mathcal{O}} = \mathfrak{f}_{\mathcal{O}'}.$$

So let

$$\alpha \in (\mathfrak{a}' : \mathfrak{a}) = \{x \in K : x\mathfrak{a} \subseteq \mathfrak{a}'\}$$

be a μ-isogeny. Then

$$\alpha\mathfrak{a} \subseteq \mathfrak{a}' \tag{3.4}$$

and

$$\overline{\alpha} \in (\mathfrak{a}^\vee : (\mathfrak{a}')^\vee) = (\beta\mathfrak{a} : \beta'\mathfrak{a}'),$$

which implies that $\overline{\alpha}\beta'\mathfrak{a}' \subseteq \beta\mathfrak{a}$. Also, as α is a μ-isogeny, we have that $\beta^{-1}\alpha\beta'\overline{\alpha} = \mu$, hence

$$\mu\mathfrak{a}' \subseteq \alpha\mathfrak{a}. \tag{3.5}$$

Therefore,

$$\begin{aligned}
\mu\mathcal{O}' &= (\mu\mathfrak{a}' : \mathfrak{a}') && \text{as } \mathrm{End}(\mathfrak{a}') = (\mathfrak{a}' : \mathfrak{a}') \\
&\subseteq (\alpha\mathfrak{a} : \mathfrak{a}') && \text{by (3.5)} \\
&\subseteq (\alpha\mathfrak{a} : \alpha\mathfrak{a}) && \text{by (3.4)} \\
&= \mathcal{O} && \text{as } \mathrm{End}(\mathfrak{a}) = (\mathfrak{a} : \mathfrak{a}) \\
&\subseteq (\alpha^{-1}\mathfrak{a}' : \mathfrak{a}) && \text{by (3.4)} \\
&\subseteq (\alpha^{-1}\mathfrak{a}' : \alpha^{-1}\mu\mathfrak{a}') && \text{by (3.5)} \\
&= \mu^{-1}\mathcal{O}' && \text{as } \mathrm{End}(\mathfrak{a}') = (\mathfrak{a}' : \mathfrak{a}').
\end{aligned}$$

In particular,

$$\mu\mathfrak{f}_{\mathcal{O}'} \subseteq \mathfrak{f}_{\mathcal{O}} \subseteq \mu^{-1}\mathfrak{f}_{\mathcal{O}'}.$$

□

3.1.2 Principally polarised ideals are invertible

We will use repeatedly for the rest of the chapter the surprising result that objects of $\mathbf{PId}_{\pi,K_0}$ are invertible, which we now prove:

Proposition 3.1.15. If $(\mathfrak{a}, \beta) \in \mathbf{PId}_{\pi,K_0}$, then $\mathfrak{a}$ is an invertible $\mathrm{End}(\mathfrak{a})$-ideal.

Recall from Lemma 1.6.1 that for $(\mathfrak{a}, \beta) \in \mathbf{PId}_{\pi,K_0}$ there exist $\tau, \beta \in K$ such that

$$(\mathfrak{a}, \beta) \cong (\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee, \beta'),$$

where $\mathcal{O}_{K_0}^\vee$ is the trace dual of $\mathcal{O}_{K_0}$. Before proving Proposition 3.1.15 we first prove the following technical lemma:

Lemma 3.1.16. Suppose that $\mathfrak{a} = \tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee$ is a fractional $\mathbb{Z}[\pi, \overline{\pi}]$-ideal, so that in particular $\tau \in K$, and hence there exist $A, B, C \in K_0$ such that

$$A\tau^2 + B\tau + C = 0. \tag{3.6}$$

Define the fractional $\mathcal{O}_{K_0}$-ideal $\mathfrak{d}$ by

$$\mathfrak{d} = A\mathcal{O}_{K_0}^\vee + B\mathcal{O}_{K_0} + C(\mathcal{O}_{K_0}^\vee)^{-1}. \tag{3.7}$$

Then

$$\mathrm{End}(\mathfrak{a}) = A\tau\mathfrak{d}^{-1} + \mathcal{O}_{K_0}.$$

Proof. For every $x \in \mathrm{End}(\mathfrak{a})$, as $\mathrm{End}(\mathfrak{a}) \subseteq \mathcal{O}_K$, we know that there exist $a, b \in K_0$ such that

$$x = a\tau + b.$$

Then for every $a, b \in K_0$, we have that $a\tau + b \in \mathrm{End}(\mathfrak{a})$ if and only if

$$(a\tau + b)(\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee) \subseteq \tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee.$$

That is, if and only if for every $\alpha \in \mathcal{O}_{K_0}$ and every $\beta \in \mathcal{O}_{K_0}^\vee$, we have that

$$(a\tau + b)\tau\alpha = \tau^2\alpha a + \tau\alpha b = -A^{-1}(B\tau + C)\alpha a + \tau\alpha b \in \tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee \tag{3.8}$$

and

$$(a\tau + b)\beta = \beta\tau a + \beta b \in \tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee. \tag{3.9}$$

Now, we have (3.8) for every $\alpha \in \mathcal{O}_{K_0}$ if and only if

$$\left(b - \frac{B}{A}a\right)\mathcal{O}_{K_0} \subseteq \mathcal{O}_{K_0} \tag{3.10}$$

and

$$a\frac{C}{A}\mathcal{O}_{K_0} \subseteq \mathcal{O}_{K_0}^\vee. \tag{3.11}$$

Similarly, we have (3.9) for every $\beta \in \mathcal{O}_{K_0}^\vee$ if and only if

$$a\mathcal{O}_{K_0}^\vee \subseteq \mathcal{O}_{K_0} \tag{3.12}$$

and

$$b \in \mathcal{O}_{K_0}. \tag{3.13}$$

So that $a\tau + b \in \mathrm{End}(\mathfrak{a})$ if and only if (3.10)-(3.13) hold. Now, (3.13) and (3.10) hold if and only if $b \in \mathcal{O}_{K_0}$ and

$$\frac{B}{A}a\mathcal{O}_{K_0} \subseteq \mathcal{O}_{K_0}. \tag{3.14}$$

Also, we know that $\mathcal{O}_{K_0}$ is a Dedekind domain and $\mathcal{O}_{K_0}^\vee$ is a fractional $\mathcal{O}_{K_0}$-ideal, so that in paritcular it is an invertible $\mathcal{O}_{K_0}$-ideal, and hence (3.11) holds if and only if

$$a\frac{C}{A}(\mathcal{O}_{K_0}^\vee)^{-1} \subseteq \mathcal{O}_{K_0}. \tag{3.15}$$

We now have that $a\tau + b \in \mathrm{End}(\mathfrak{a})$ if and only if (3.12), (3.14), (3.15), and (3.13) hold. But (3.12), (3.14), and (3.15) hold if and only if

$$a \in \left(\mathcal{O}_{K_0} : \mathcal{O}_{K_0}^\vee + \frac{B}{A}\mathcal{O}_{K_0} + \frac{C}{A}(\mathcal{O}_{K_0}^\vee)^{-1}\right) = A\mathfrak{d}^{-1}.$$

Hence

$$\mathrm{End}(\mathfrak{a}) = A\tau\mathfrak{d}^{-1} + \mathcal{O}_{K_0}.$$

□

Proof of Proposition 3.1.15. By Lemma 1.6.1, there exists $\alpha \in K^\times$ such that

$$\alpha\mathfrak{a} = \tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee. \tag{3.16}$$

Choose $A, B, C \in K_0$ such that

$$A\tau^2 + B\tau + C = 0$$

and define

$$\mathfrak{d} = A\mathcal{O}_{K_0}^\vee + B\mathcal{O}_{K_0} + C(\mathcal{O}_{K_0}^\vee)^{-1}.$$

We claim that there exists a totally positive element a of K_0 such that

$$\mathfrak{a}^{-1} = aA\mathfrak{d}^{-1}\overline{\mathfrak{a}}(\mathcal{O}_{K_0}^\vee)^{-1}.$$

To see this, first note that:

(a) As $\mathcal{O}_{K_0}$ is a Dedekind domain and $\mathcal{O}_{K_0}^\vee$ and both $\mathfrak{d}$ are fractional $\mathcal{O}_{K_0}$-ideals, then (i) $\mathcal{O}_{K_0}^\vee$ is an invertible $\mathcal{O}_{K_0}$-ideal, and (ii) $\mathfrak{d}$ is an invertible $\mathcal{O}_{K_0}$-ideal.

(b) We have that $\mathrm{tr}_{K/K_0}(\tau) = -B/A$ and $\mathrm{N}_{K/K_0}(\tau) = -C/A$.

Then

$$\begin{aligned}
&\mathfrak{a}(\alpha\overline{\alpha}A\overline{\mathfrak{a}}\mathfrak{d}^{-1}(\mathcal{O}_{K_0}^\vee)^{-1}) \\
&= (\tau\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee)(\overline{\tau}\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee)A\mathfrak{d}^{-1}(\mathcal{O}_{K_0}^\vee)^{-1} && \text{by 3.16} \\
&= (\tau\overline{\tau}(\mathcal{O}_{K_0}^\vee)^{-1} + \tau\mathcal{O}_{K_0} + \overline{\tau}\mathcal{O}_{K_0} + \mathcal{O}_{K_0}^\vee)A\mathfrak{d}^{-1} && \text{by (ai)} \\
&= (C(\mathcal{O}_{K_0}^\vee)^{-1} + B\mathcal{O}_{K_0} + A\mathcal{O}_{K_0}^\vee + A\tau\mathcal{O}_{K_0})\mathfrak{d}^{-1} && \text{by (b)} \\
&= A\tau\mathfrak{d}^{-1} + \mathcal{O}_{K_0} && \text{by (aii)} \\
&= \mathrm{End}(\mathfrak{a}). && \text{by Lemma 3.1.16}
\end{aligned}$$

Hence $\mathfrak{a}$ is an invertible $\mathrm{End}(\mathfrak{a})$-ideal, with

$$\mathfrak{a}^{-1} = \alpha\overline{\alpha}A\overline{\mathfrak{a}}\mathfrak{d}^{-1}(\mathcal{O}_{K_0}^\vee)^{-1}.$$

□

One nice corollary of this is the following formula for the trace dual of a principally polarised ideal:

Corollary 3.1.17. Let $(\mathfrak{a}, \beta) \in \mathbf{PId}_{\pi,K_0}$ with $\mathrm{End}(\mathfrak{a}) = \mathcal{O}$. Then

$$\mathfrak{a}^\vee = \overline{\mathfrak{a}}^{-1}\mathcal{O}^\vee. \tag{3.17}$$

Proof. Note first that

$$\begin{aligned}
\mathfrak{a}^\vee &= \{x \in K : \mathrm{tr}_{K/\mathbb{Q}}(\overline{x}\mathfrak{a}) \subseteq \mathbb{Z}\} \\
&= \{x \in K : \mathrm{tr}_{K/\mathbb{Q}}(x\overline{\mathfrak{a}}) \subseteq \mathbb{Z}\}.
\end{aligned}$$

For any $x \in \overline{\mathfrak{a}}^{-1}\mathcal{O}^\vee$, we have that

$$x\overline{\mathfrak{a}} \in \overline{\mathfrak{a}}^{-1}\overline{\mathfrak{a}}\mathcal{O}^\vee = \mathcal{O}^\vee,$$

so that in particular $\mathrm{tr}_{K/\mathbb{Q}}(x\overline{\mathfrak{a}}) \subseteq \mathrm{tr}_{K/\mathbb{Q}}(\mathcal{O}^\vee) \subseteq \mathbb{Z}$. Hence

$$\overline{\mathfrak{a}}^{-1}\mathcal{O}^\vee \subseteq \mathfrak{a}^\vee.$$

For the other inclusion, observe that

$$\overline{\mathfrak{a}}\mathfrak{a}^\vee = \{xy : x \in K,\, y \in \overline{\mathfrak{a}},\, \mathrm{tr}_{K/\mathbb{Q}}(x\overline{\mathfrak{a}}\mathcal{O}) \subseteq \mathbb{Z}\},$$

as $\mathfrak{a}$ is a fractional $\mathcal{O}$-ideal. In particular, for all $x \in \mathfrak{a}^\vee$ and $y \in \overline{\mathfrak{a}}$, we have that $xy \in \mathcal{O}^\vee$, so that $\overline{\mathfrak{a}}\mathfrak{a}^\vee \subseteq \mathcal{O}^\vee$. Then as $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal, we have that

$$\mathfrak{a}^\vee \subseteq \overline{\mathfrak{a}}^{-1}\mathcal{O}^\vee.$$

□

3.1.3 The action of the Shimura class group

Let μ be a totally positive prime element of $\mathcal{O}_{K_0}$ and let G be the μ-isogeny graph for Weil q-number π. Let C be a connected component of G and let $\mathfrak{f}_C$ be the conductor of C, as defined in Definition 3.1.13. Recall from Equation (3.2) that we defined

$$V(\mu^i\mathfrak{f}_C) = \{(\mathrm{A}, \xi) \in \mathbf{POrd}_{\pi,K_0} : \mathfrak{f}_{\mathrm{End(A)}} = \mu^i\mathfrak{f}_C\}_{/\cong}.$$

Proposition 3.1.18. For any order $\mathcal{O}$ in $\mathcal{O}_K$ containing $\mathcal{O}_{K_0}[\pi, \overline{\pi}]$ that is stable under complex conjugation, the Shimura Class Group $\mathrm{SCl}(\mathcal{O})$ of $\mathcal{O}$ acts faithfully and transitively on $V(\mathfrak{f}_\mathcal{O})$. (We define a transitive action to have at most one orbit).

Proof. We prove this in the category $\mathbf{Id}_{\pi,K_0}$. We show that $\mathrm{SCl}(\mathcal{O})$ acts on

$$S_\mathcal{O} = \{(\mathfrak{a}, \beta) \in \mathbf{PId}_{\pi,K_0} : \mathrm{End}(\mathfrak{a}) = \mathcal{O}\}_{/\cong}$$

via

$$[(\mathfrak{c}, \lambda)] \cdot [(\mathfrak{a}, \beta)] = [(\mathfrak{c}^{-1}\mathfrak{a}, \lambda\beta)],$$

and that this action is faithful and transitive. We first show that for any $[(\mathfrak{c}, \lambda)] \in \mathrm{SCl}(\mathcal{O})$ and $[(\mathfrak{a}, \beta)] \in S_\mathcal{O}$, we have that $[(\mathfrak{c}^{-1}\mathfrak{a}, \lambda\beta)] \in S_\mathcal{O}$. Recall from Proposition 3.1.15 that $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal, and that $\mathfrak{c}$ is an invertible $\mathcal{O}$-ideal by definition. In particular, we have that

$$(\mathfrak{c}^{-1}\mathfrak{a})^{-1}(\mathfrak{c}^{-1}\mathfrak{a}) = \mathfrak{c}\mathfrak{c}^{-1}\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O},$$

which implies that $\mathfrak{c}^{-1}\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal. Now, as λ is totally positive, we know that $\lambda\beta$ is a polarisation of $\mathfrak{a}$ by Remark 1.3.8, and

$$\begin{aligned}
(\mathfrak{c}^{-1}\mathfrak{a})^\vee &= (\overline{\mathfrak{c}^{-1}\mathfrak{a}})^{-1}\mathcal{O}^\vee && \text{by Corollary 3.1.17} \\
&= \overline{\mathfrak{c}}\mathfrak{a}^\vee && \text{by Corollary 3.1.17} \\
&= \lambda\beta\mathfrak{c}^{-1}\mathfrak{a} && \text{as } \mathfrak{c}\overline{\mathfrak{c}} = \lambda\mathcal{O} \text{ and } \beta\mathfrak{a} = \mathfrak{a}^\vee,
\end{aligned}$$

hence it is principal. So $\mathrm{SCl}(\mathcal{O})$ acts on $S_{\mathcal{O}}$. We now show that this action is faithful. Let $[(\mathfrak{c},\lambda)] \in \mathrm{SCl}(\mathcal{O})$ such that for all $[(\mathfrak{a},\beta)] \in S_{\mathcal{O}}$, we have that

$$[(\mathfrak{a},\beta)] = [(\mathfrak{c}^{-1}\mathfrak{a}, \lambda\beta)].$$

That is, for all $[(\mathfrak{a},\beta)] \in S_{\mathcal{O}}$ there exists an isomorphism

$$(\mathfrak{a},\beta) \longrightarrow (\mathfrak{c}^{-1}\mathfrak{a}, \lambda\beta)$$

in $\mathbf{PId}_{\pi,K_0}$. Recall from Definition 1.3.9 that an isomorphism in $\mathbf{PId}_{\pi,K_0}$ is a 1-isogeny. Hence, for $[(\mathfrak{a},\beta)] \in S_{\mathcal{O}}$, we have that $[(\mathfrak{a},\beta)] = [(\mathfrak{c}^{-1}\mathfrak{a}, \lambda\beta)]$ if and only if there exists $\alpha \in K$ such that

$$\alpha\mathfrak{a} = \mathfrak{c}^{-1}\mathfrak{a} \tag{3.18}$$

and

$$\alpha\lambda\beta\overline{\alpha} = \beta. \tag{3.19}$$

We have (3.19) if and only if $\lambda = (\alpha\overline{\alpha})^{-1}$, and as $\mathfrak{c}$ and $\mathfrak{a}$ are invertible $\mathcal{O}$-ideals, we have (3.18) if and only if $\mathfrak{c} = \alpha^{-1}\mathcal{O}$. In particular,

$$[(\mathfrak{c},\lambda)] = [(\alpha^{-1}\mathcal{O}, (\alpha\overline{\alpha})^{-1})] = [(\mathcal{O},1)].$$

Hence the action is faithful, so it remains to show that it is transitive. That is, it remains to show that if $(\mathfrak{a},\beta)$ and $(\mathfrak{a}',\beta') \in S_{\mathcal{O}}$, then

$$[(\mathfrak{a}(\mathfrak{a}')^{-1}, \beta^{-1}\beta')] \in \mathrm{SCl}(\mathcal{O}). \tag{3.20}$$

First, note that as β and β' are polarisations, for every $\phi \in \Phi_{\pi,j}$, we have that

$$\phi(\beta)/i,\ \phi(\beta')/i \in \mathbb{R}_{<0}.$$

(Recall the definition of $\Phi_{\pi,j}$ from Definition 1.3.5). In particular, for every $\phi \in \Phi_{\pi,j}$, we have that

$$\phi(\beta'\beta^{-1}) = \phi(\beta')\phi(\beta)^{-1} \in \mathbb{R}_{>0},$$

and hence $\beta'\beta^{-1}$ is totally positive. Finally, we have that

$$\begin{aligned}
&\mathfrak{a}(\mathfrak{a}')^{-1}\overline{\mathfrak{a}(\mathfrak{a}')^{-1}} \\
&\quad= \overline{\mathfrak{a}}\mathfrak{a}(\mathcal{O}:\mathfrak{a}')(\overline{\mathfrak{a}'})^{-1} && \text{as } \mathfrak{a}' = (\mathcal{O}:\mathfrak{a}') \\
&\quad= \overline{\mathfrak{a}}\beta^{-1}\mathfrak{a}^{\vee}\beta'(\mathcal{O}:(\mathfrak{a}')^{\vee})(\overline{\mathfrak{a}'})^{-1} && \text{as } \beta\mathfrak{a} = \mathfrak{a}^{\vee} \text{ and } \beta'\mathfrak{a}' = (\mathfrak{a}')^{\vee} \\
&\quad= \beta^{-1}\beta'\overline{\mathfrak{a}}(\overline{\mathfrak{a}})^{-1}\mathcal{O}^{\vee}(\mathcal{O}:\mathcal{O}^{\vee}(\overline{\mathfrak{a}'})^{-1})(\overline{\mathfrak{a}'})^{-1} && \text{by Corollary 3.1.17}
\end{aligned}$$

Now by Corollary 3.1.17, we have that $\beta\mathfrak{a}\overline{\mathfrak{a}} = \mathcal{O}^{\vee}$, and by Proposition 3.1.15, we have that $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal, which implies that $\mathcal{O}^{\vee}$ is an invertible $\mathcal{O}$-ideal, and hence

$$\mathcal{O}^{\vee}(\mathcal{O}:\mathcal{O}^{\vee}(\overline{\mathfrak{a}'})^{-1}) = \mathcal{O}^{\vee}\mathcal{O}(\mathcal{O}^{\vee}(\overline{\mathfrak{a}'})^{-1})^{-1} = \overline{\mathfrak{a}'},$$

giving

$$\mathfrak{a}(\mathfrak{a}')^{-1}\overline{\mathfrak{a}(\mathfrak{a}')^{-1}} = \beta^{-1}\beta'\overline{\mathfrak{a}}(\overline{\mathfrak{a}})^{-1}\overline{\mathfrak{a}'}(\overline{\mathfrak{a}'})^{-1} = \beta^{-1}\beta'\mathcal{O},$$

hence Equation (3.20) holds and the action is transitive. □

3.1.4 Counting horizontal μ-isogenies

Proposition 3.1.19. Suppose that $\mathcal{O}$ is an order in K that is stable under complex conjugation and that satisfies $\mathcal{O}_{K_0}[\pi, \bar{\pi}] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$. Suppose that there exists $(\mathrm{A}, \xi) \in \mathbf{POrd}_{\pi,K_0}$ with $\mathrm{End}(\mathfrak{a}) = \mathcal{O}$. If $\mathfrak{f}_{\mathcal{O}}$ and $\mu\mathcal{O}_K$ are relatively prime, then up to isomorphism, there are exactly m horizontal μ-isogenies from (A, ξ), where

$$m = \begin{cases} 0 & \mu \text{ is inert in } K \\ 1 & \mu \text{ is ramified in } K, \\ 2 & \mu \text{ splits in } K. \end{cases}$$

If $\mathfrak{f}_{\mathcal{O}} = \mu^i \mathfrak{f}_C$ and $i \geq 1$, then there are no horizontal μ-isogenies from (A, ξ). Furthermore, if there exists a horizontal μ-isogeny f from (A, ξ), then there exists $[(\mathfrak{m}, \mu)] \in \mathrm{SCl}(\mathcal{O})$ such that f is isomorphic to a μ-isogeny of the form

$$(\mathrm{A}, \xi) \longrightarrow (\mathfrak{m}, \mu) \cdot (\mathrm{A}, \xi),$$

where the action of $\mathrm{SCl}(\mathcal{O})$ on $V(\mathfrak{f}_{\mathcal{O}})$ is the action defined in Proposition 3.1.18.

We first give a characterisation of μ-isogenous objects in $\mathbf{PId}_{\pi,K_0}$ that have the same endomorphism ring.

Lemma 3.1.20. Suppose that $(\mathfrak{a}, \beta)$ and $(\mathfrak{a}', \beta') \in \mathbf{PId}_{\pi,K_0}$ and that $\mathrm{End}(\mathfrak{a}) = \mathrm{End}(\mathfrak{a}') = \mathcal{O}$. If $\alpha \in (\mathfrak{a}' : \mathfrak{a})$ is a μ-isogeny

$$(\mathfrak{a}, \beta) \longrightarrow (\mathfrak{a}', \beta')$$

then

$$\alpha\mathfrak{a}(\mathfrak{a}')^{-1}\overline{\alpha\mathfrak{a}(\mathfrak{a}')^{-1}} = \mu\mathcal{O}.$$

Proof. By Corollary 3.1.17 we know that

$$\beta\mathfrak{a}\overline{\mathfrak{a}} = \beta'\mathfrak{a}'\overline{\mathfrak{a}'} = \mathcal{O}^\vee.$$

Now given $\alpha \in (\mathfrak{a}' : \mathfrak{a})$, by definition it is a μ-isogeny if and only if

$$\mu\beta = \alpha\overline{\alpha}\beta',$$

which implies that

$$\alpha\overline{\alpha}\beta\mathfrak{a}\overline{\mathfrak{a}} = \mu\beta\mathfrak{a}'\overline{\mathfrak{a}'}.$$

Also, by Proposition 3.1.15, we know that $\mathfrak{a}'$ and $\overline{\mathfrak{a}'}$ are invertible as $\mathcal{O}$-ideals, hence

$$\alpha\mathfrak{a}(\mathfrak{a}')^{-1}\overline{\alpha\mathfrak{a}(\mathfrak{a}')^{-1}} = \mu\mathcal{O}.$$

□

Proof of Proposition 3.1.19. Suppose that there exists $(\mathfrak{a}', \beta') \in \mathbf{PId}_{\pi,K_0}$ with $\mathrm{End}(\mathfrak{a}') = \mathcal{O}$ such that that there exists a μ-isogeny $\alpha \in (\mathfrak{a}' : \mathfrak{a})$ mapping

$$(\mathfrak{a}, \beta) \longrightarrow (\mathfrak{a}', \beta').$$

Then by Lemma 3.1.20, we have that

$$\alpha\mathfrak{a}(\mathfrak{a}')^{-1}\overline{\alpha\mathfrak{a}(\mathfrak{a}')^{-1}} = \mu\mathcal{O}. \tag{3.21}$$

In particular, since $\alpha\mathfrak{a} \subset \mathfrak{a}'$, it can be seen that $\alpha\mathfrak{a}(\mathfrak{a}')^{-1}$ is an $\mathcal{O}$-ideal. That is, there is an $\mathcal{O}$-ideal $\mathfrak{m}$ such that $\mu\mathcal{O} = \mathfrak{m}\overline{\mathfrak{m}}$. In particular, both $\mathfrak{m}$ and $\overline{\mathfrak{m}}$ are invertible, and hence coprime to the conductor. Hence if $\mathfrak{f}_{\mathcal{O}} \subseteq \mu\mathfrak{f}_C$ then there are no horizontal μ-isogenies from $(\mathfrak{a}, \beta)$.

Suppose now that $\mathfrak{f}_{\mathcal{O}} = \mathfrak{f}_C$. Then $\mu\mathcal{O}$ is relatively prime to $\mathfrak{f}_{\mathcal{O}}$, and hence decomposes uniquely into prime ideals. As μ is a prime element of $\mathcal{O}_{K_0}$, the ideal $\mu\mathcal{O}$ is either inert, ramified, or split. If $\mu\mathcal{O}$ is inert, then there exists no $\mathcal{O}$-ideal $\mathfrak{m}$ such that $\mu\mathcal{O} = \mathfrak{m}\overline{\mathfrak{m}}$, so as before, there no horizontal μ-isogenies from $(\mathfrak{a}, \beta)$ in this case.

It remains to consider the case in which $\mu\mathcal{O}$ is split or ramified, so suppose that $\mu\mathcal{O}$ decomposes as $\mu\mathcal{O} = \mathfrak{m}\overline{\mathfrak{m}}$. Then $\mu \in (\mathfrak{m}\mathfrak{a} : \mathfrak{a})$ defines a μ-isogeny

$$(\mathfrak{a}, \beta) \longrightarrow (\mathfrak{m}\mathfrak{a}, \mu^{-1}\beta),$$

and $\mu \in (\overline{\mathfrak{m}}\mathfrak{a} : \mathfrak{a})$ defines a μ-isogeny

$$(\mathfrak{a}, \beta) \longrightarrow (\overline{\mathfrak{m}}\mathfrak{a}, \mu^{-1}\beta).$$

We claim that up to isomorphism these are the only horizontal μ-isogenies from $(\mathfrak{a}, \beta)$. To see this, suppose that there is some $(\mathfrak{a}', \beta') \in \mathbf{PId}_{\pi,K_0}$ with $\mathrm{End}(\mathfrak{a}') = \mathcal{O}$ for which some $\alpha \in (\mathfrak{a}' : \mathfrak{a})$ defines a μ-isogeny

$$(\mathfrak{a}, \beta) \longrightarrow (\mathfrak{a}', \beta').$$

Then $\beta' = (\alpha\overline{\alpha})^{-1}\mu\beta$, and by Lemma 3.1.20, we have that

$$\alpha\mathfrak{a}(\mathfrak{a}')^{-1}\overline{\alpha\mathfrak{a}(\mathfrak{a}')^{-1}} = \mu\mathcal{O},$$

so by unique factorisation, we have that

$$\alpha\mathfrak{a}(\mathfrak{a}')^{-1} = \mathfrak{m} \quad \text{or} \quad \alpha\mathfrak{a}(\mathfrak{a}')^{-1} = \overline{\mathfrak{m}},$$

that is,

$$\mathfrak{a}' = \mu^{-1}\alpha\overline{\mathfrak{m}}\mathfrak{a} \quad \text{or} \quad \mathfrak{a}' = \mu^{-1}\alpha\mathfrak{m}\mathfrak{a}.$$

It is then easy to see that if $\mathfrak{a}' = \mu^{-1}\alpha\overline{\mathfrak{m}}\mathfrak{a}$ then $\mu^{-1}\alpha \in (\mathfrak{a}' : \overline{\mathfrak{m}}\mathfrak{a})$ defines a 1-isogeny (i.e. isomorphism)

$$(\overline{\mathfrak{m}}\mathfrak{a}, \mu^{-1}\beta) \longrightarrow (\alpha\mu^{-1}\overline{\mathfrak{m}}\mathfrak{a}, (\alpha\overline{\alpha})^{-1}\mu\beta),$$

in which case the μ-isogeny defined by $\mu \in (\mathfrak{m}\mathfrak{a} : \mathfrak{a})$ and the μ-isogeny defined by $\alpha \in (\mathfrak{a}' : \mathfrak{a})$ make the diagram

$$\begin{array}{ccc} (\mathfrak{a}, \beta) & \xrightarrow{\mu} & (\mathfrak{m}\mathfrak{a}, \mu^{-1}\beta) \\ \Big\downarrow{\scriptstyle 1} & & \Big\downarrow{\scriptstyle \mu^{-1}\alpha} \\ (\mathfrak{a}, \beta) & \xrightarrow{\alpha} & (\mathfrak{a}', \beta') \end{array}$$

commute and hence are isomorphic by definition. Similarly, if $\mathfrak{a}' = \mu^{-1}\alpha\mathfrak{m}\mathfrak{a}$ then $\mu \in (\overline{\mathfrak{m}}\mathfrak{a} : \mathfrak{a})$ and $\alpha \in (\mathfrak{a}' : \mathfrak{a})$ are isomorphic as μ-isogenies. □

3.1.5 A construction of ascending μ-isogenies

Proposition 3.1.21. From every vertex such that the conductor of its endomorphism ring is not coprime to μ, there exists an ascending μ-isogeny.

Proof. Suppose that $(\mathfrak{a}, \beta) \in \mathbf{PId}_{\pi,K_0}$ and that $\mathrm{End}(\mathfrak{a}) = \mathcal{O}$. Write $\mathfrak{f}_{\mathcal{O}}$ for the conductor of $\mathcal{O}$, and suppose that $\mathfrak{f}_{\mathcal{O}} \subseteq \mu\mathcal{O}_K$. Then write $\mathcal{O}'$ for the order in $\mathcal{O}_K$ of conductor $\mu^{-1}\mathfrak{f}_{\mathcal{O}}$. In particular, we have that

$$(\mathcal{O} : \mathcal{O}') = \mu\mathcal{O}' \tag{3.22}$$

We claim that

$$\mathrm{End}(\mathfrak{a}\mathcal{O}') = \mathcal{O}', \tag{3.23}$$

and that

$$(\mathfrak{a}\mathcal{O}', \mu\beta) \in \mathbf{PId}_{\pi,K_0}. \tag{3.24}$$

Note that (3.24) implies that $1 \in (\mathfrak{a}\mathcal{O}', \mathfrak{a})$ defines a μ-isogeny

$$(\mathfrak{a}, \beta) \longrightarrow (\mathfrak{a}\mathcal{O}', \mu\beta),$$

and (3.23) implies that it is ascending. For (3.23), observe that $\mathfrak{a}\mathcal{O}'$ is an invertible $\mathcal{O}'$-ideal with inverse $\mathfrak{a}^{-1}\mathcal{O}'$, and hence $\mathrm{End}(\mathfrak{a}\mathcal{O}') = \mathcal{O}'$. For (3.24), if we can can show that $(\mathfrak{a}\mathcal{O}')^\vee = \mu\beta\mathfrak{a}\mathcal{O}'$ then by Remark 1.3.8 we have that $\mu\beta$ is a principal polarisation of $\mathfrak{a}'\mathcal{O}'$ as μ is totally positive. By Corollary 3.1.17, it is sufficient to show that

$$\mu\beta\mathfrak{a}\overline{\mathfrak{a}}\mathcal{O}' = (\mathcal{O}')^\vee.$$

Then as β is a principal polarisation of $\mathfrak{a}$, by Corollary 3.1.17 we have already that $\beta\mathfrak{a}\overline{\mathfrak{a}} = \mathcal{O}^\vee$. Hence it suffices to show that

$$\mu\mathcal{O}'\mathcal{O}^\vee = (\mathcal{O}')^\vee.$$

We first prove that

$$\mu\mathcal{O}'\mathcal{O}^\vee \subseteq (\mathcal{O}')^\vee. \tag{3.25}$$

This holds if and only if $\mathcal{O}'\mathcal{O}^\vee \subseteq (\mu\mathcal{O}')^\vee$. But

$$\mathcal{O}' \subseteq (\mathcal{O}')^\vee \subseteq (\mu\mathcal{O}')^\vee$$

and

$$\mathcal{O}^\vee \subseteq ((\mathcal{O} : \mathcal{O}')\mathcal{O}')^\vee = (\mu\mathcal{O}')^\vee,$$

hence (3.25) holds. We now prove that

$$(\mathcal{O}')^\vee \subseteq \mu\mathcal{O}'\mathcal{O}^\vee. \tag{3.26}$$

As $\mathcal{O} \subseteq \mathcal{O}'$, we have immediately that $(\mathcal{O}')^\vee \subseteq \mathcal{O}^\vee$. In particular, we get that

$$(\mathcal{O}^\vee)^{-1}(\mathcal{O}')^\vee \subseteq \mathcal{O}.$$

Now locally away μ, the orders $\mathcal{O}$ and $\mathcal{O}'$ are the same, so (3.26) is trivial, and localising $\mathcal{O}$ at μ, we get a local ring with maximal ideal $\mu\mathcal{O}'$. Furthermore, we have that $(\mathcal{O}^\vee)^{-1}(\mathcal{O}')^\vee$ is an $\mathcal{O}'$-ideal contained in $\mathcal{O}$, and $\mathcal{O}$ is not an $\mathcal{O}'$-ideal, hence

$$(\mathcal{O}^\vee)^{-1}(\mathcal{O}')^\vee \subseteq \mu\mathcal{O}'.$$

Also, we have from Corollary 3.1.17 that $\beta\mathfrak{a}\overline{\mathfrak{a}} = \mathcal{O}^\vee$ and from Proposition 3.1.15 that $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal, and hence $\mathcal{O}^\vee$ is an invertible $\mathcal{O}$-ideal. Therefore

$$(\mathcal{O}')^\vee = \mathcal{O}(\mathcal{O}')^\vee \subseteq \mu\mathcal{O}'\mathcal{O}^\vee.$$

We have now proved (3.24). □

3.1.6 The size of the Shimura class group

Proposition 3.1.22. Suppose that the only roots of unity in $\mathcal{O}_K$ are ± 1, and that $\mathcal{O}' \subset \mathcal{O}$ are orders in $\mathcal{O}_K$ containing $\mathcal{O}_{K_0}[\pi, \overline{\pi}]$ that are stable under complex conjugation. Suppose further that $\mathfrak{f}_{\mathcal{O}'} = \mu\mathfrak{f}_{\mathcal{O}}$. Now define the map

$$\begin{array}{rccc} \rho: & \mathrm{SCl}(\mathcal{O}') & \longrightarrow & \mathrm{SCl}(\mathcal{O}) \\ & [(\mathfrak{a}', \lambda')] & \mapsto & [(\mathfrak{a}'\mathcal{O}, \lambda')]. \end{array}$$

Then ρ is a surjective homomorphism. Furthermore, if $\mu\mathcal{O}_K$ and $\mathfrak{f}_{\mathcal{O}}$ are coprime, then

$$\#\ker(\rho) = \begin{cases} \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) + 1 & \text{if } \mu \text{ is inert in } K \\ \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) & \text{if } \mu \text{ is ramified in } K \\ \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu) - 1 & \text{if } \mu \text{ is split in } K, \end{cases}$$

and otherwise

$$\#\ker(\rho) = \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu).$$

Proof. Note that if $\mathfrak{a}'$ is an invertible $\mathcal{O}'$-ideal then $\mathfrak{a}'\mathcal{O}$ is an invertible $\mathcal{O}$-ideal, and if $\mathfrak{a}'\overline{\mathfrak{a}'} = \lambda'\mathcal{O}'$ then

$$\mathfrak{a}'\mathcal{O}\overline{\mathfrak{a}'\mathcal{O}} = \mathfrak{a}'\overline{\mathfrak{a}'}\mathcal{O} = \lambda'\mathcal{O}'\mathcal{O} = \lambda'\mathcal{O},$$

so ρ is well-defined. Write $f = [\mathcal{O}_K : \mathcal{O}']$. By [BS15, Lemma 7] we have that ρ is surjective and that

$$\ker(\rho) = \frac{(\mathcal{O}/f\mathcal{O}_K)^\times}{(\mathcal{O}'/f\mathcal{O}_K)^\times}. \tag{3.27}$$

We have that

$$\mu\mathcal{O} = (\mathcal{O}' : \mathcal{O}) \supseteq (\mathcal{O}' : \mathcal{O}_K) = \mathfrak{f}_{\mathcal{O}'} \supseteq f\mathcal{O}_K,$$

so that in particular there is a natural map

$$\mathcal{O}/f\mathcal{O}_K \longrightarrow \mathcal{O}/\mu\mathcal{O}$$

and an induced morphism of unit groups

$$(\mathcal{O}/f\mathcal{O}_K)^\times \longrightarrow (\mathcal{O}/\mu\mathcal{O})^\times.$$

Define

$$\varphi : (\mathcal{O}/f\mathcal{O}_K)^\times \longrightarrow \frac{(\mathcal{O}/\mu\mathcal{O})^\times}{(\mathcal{O}'/\mu\mathcal{O})^\times}$$

to be the composition of this with the natural quotient morphism. As

$$\ker(\varphi) = \{x + f\mathcal{O}_K \in (\mathcal{O}/f\mathcal{O}_K)^\times : x + \mu\mathcal{O} \in (\mathcal{O}'/\mu\mathcal{O})^\times\},$$

clearly

$$(\mathcal{O}'/f\mathcal{O}_K)^\times \subseteq \ker(\varphi),$$

and if $(\mathcal{O}'/f\mathcal{O}_K)^\times \neq \ker(\varphi)$ then there must exist

$$y + f\mathcal{O}_K \in (\mathcal{O}/f\mathcal{O}_K)^\times - (\mathcal{O}'/f\mathcal{O}_K)^\times$$

such that $y + \mu\mathcal{O} \in (\mathcal{O}'/\mu\mathcal{O})^\times$. But $(\mathcal{O}'/\mu\mathcal{O})^\times \subseteq (\mathcal{O}'/f\mathcal{O}_K)^\times$, so this is not possible. Hence the following sequence is exact:

$$1 \to (\mathcal{O}'/f\mathcal{O}_K)^\times \to (\mathcal{O}/f\mathcal{O}_K)^\times \to \frac{(\mathcal{O}/\mu\mathcal{O})^\times}{(\mathcal{O}'/\mu\mathcal{O})^\times} \to 1.$$

In particular, this gives us a group isomorphism

$$\frac{(\mathcal{O}/f\mathcal{O}_K)^\times}{(\mathcal{O}'/f\mathcal{O}_K)^\times} \cong \frac{(\mathcal{O}/\mu\mathcal{O})^\times}{(\mathcal{O}'/\mu\mathcal{O})^\times}, \tag{3.28}$$

so that by (3.27),

$$\#\ker(\rho) = \frac{\#(\mathcal{O}/\mu\mathcal{O})^\times}{\#(\mathcal{O}'/\mu\mathcal{O})^\times}. \tag{3.29}$$

Write

$$\ell = \mathrm{Norm}_{K_0/\mathbb{Q}}(\mu).$$

We have that

$$\mathcal{O}'/\mu\mathcal{O} = (\mathcal{O}_{K_0} + \mu\mathcal{O})/\mu\mathcal{O} \cong \mathcal{O}_{K_0}/(\mu\mathcal{O} \cap \mathcal{O}_{K_0}) = \mathcal{O}_{K_0}/\mu\mathcal{O}_{K_0},$$

and $\mu\mathcal{O}_{K_0}$ was assumed to be prime, so that $\mathcal{O}'/\mu\mathcal{O}$ is an integral domain with ℓ elements. Hence

$$\#(\mathcal{O}'/\mu\mathcal{O})^\times = \ell - 1.$$

Similarly, if $\mathfrak{f}_\mathcal{O}$ and $\mu\mathcal{O}_K$ are coprime and μ is inert in K, then $\mu\mathcal{O}$ is prime in $\mathcal{O}$ and hence $\mathcal{O}/\mu\mathcal{O}$ is an integral domain with $\mathrm{Norm}_{K/\mathbb{Q}}(\mu) = \ell^2$ elements, giving

$$\#(\mathcal{O}/\mu\mathcal{O})^\times = \ell^2 - 1.$$

If either $\mathfrak{f}_\mathcal{O}$ and $\mu\mathcal{O}_K$ are coprime and μ is ramified in K or $\mathfrak{f}_\mathcal{O}$ and $\mu\mathcal{O}_K$ are not coprime, then there exists a unique prime ideal $\mathfrak{m}$ of $\mathcal{O}$ lying above $\mu\mathcal{O}$. In this case $\mathfrak{m}/\mu\mathcal{O}$ is the unique maximal ideal in $\mathcal{O}/\mu\mathcal{O}$, hence is the set of zero divisors. Therefore

$$\#(\mathcal{O}/\mu\mathcal{O})^\times = \#(\mathcal{O}/\mu\mathcal{O}) - \#(\mathfrak{m}/\mu\mathcal{O}) = \ell^2 - \ell = \ell(\ell - 1).$$

Finally, if $\mathfrak{f}_\mathcal{O}$ and $\mu\mathcal{O}_K$ are coprime and μ splits in K, then there are 2 distinct prime ideals $\mathfrak{m}$ and $\overline{\mathfrak{m}}$ of $\mathcal{O}$ lying above $\mu\mathcal{O}$. This gives

$$\#(\mathcal{O}/\mu\mathcal{O})^\times = \#(\mathcal{O}/\mathfrak{m}\mathcal{O})^\times \#(\mathcal{O}/\overline{\mathfrak{m}}\mathcal{O})^\times = (\ell - 1)^2.$$

The result now follows from (3.29). □

3.2 Example computation of a μ-isogeny graph

Let us consider the curve

$$\begin{aligned}\mathcal{C} : y^2 = &902701461021360x^6 + 938022069033830x^5 + 2496384827106779x^4 \\ &+ 560788189813847x^3 + 2116308108498283x^2 \\ &+ 1865564692722366x + 2658210628678317\end{aligned}$$

defined over $\mathbb{F}_p$, with $p = 2681144777671301$, which is a prime. This curve has endomorphism ring isomorphic to the maximal order of the quartic CM-field

$$K := \mathbb{Q}[x]/(x^4 + 37x^2 + 281),$$

in which p splits completely and $p = \pi\overline{\pi}$, where $K = \mathbb{Q}(\pi)$, and π is the Frobenius morphism on the Jacobian of $\mathcal{C}$. The maximal totally real subfield of K is $K_0 = \mathbb{Q}(\sqrt{5})$, and we will now fix

$$\mu = (5 + \sqrt{5})/2.$$

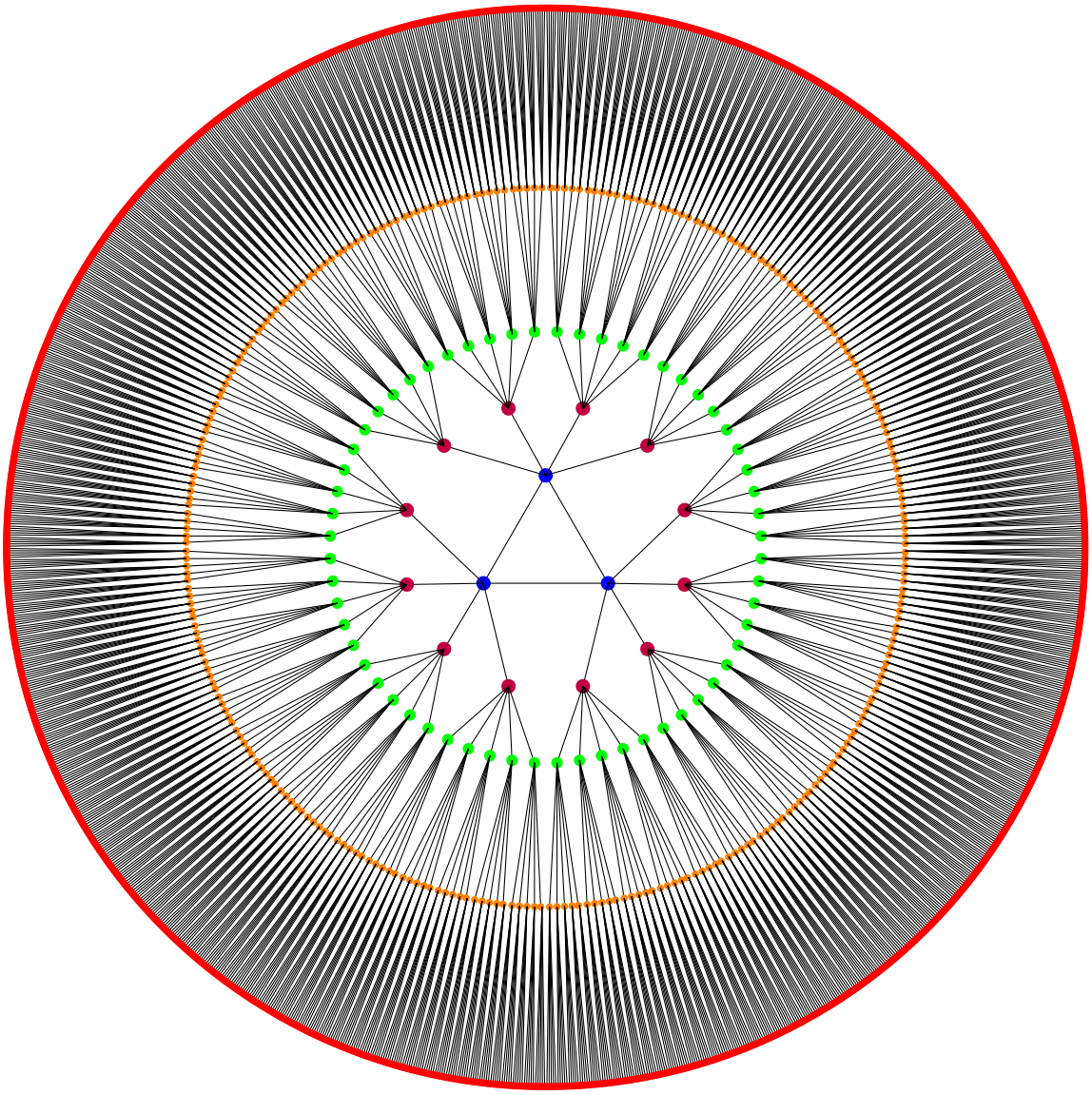
Then μ is a totally positive algebraic integer in K_0 with norm 5. Now using Sage we compute that the order of $\mu\mathcal{O}_K$ in $\mathrm{SCl}(\mathcal{O}_K)$ is 3, and that

$$\max\{n \in \mathbb{Z} : \mu^n\mathcal{O}_K \subseteq (\mathcal{O}_{K_0}[\pi, \overline{\pi}] : \mathcal{O}_K)\} = 4,$$

so that by Theorem 3.1.9, the connected component of the μ-isogeny graph in which $\mathcal{C}$ lies is a $(C_3, 6, 4)$-volcano, pictured below.

Colour	Blue	Purple	Green	Orange	Red
Endomorphism ring	$\mathcal{O}_K$	$\mathcal{O}_{K_0} + \mu\mathcal{O}_K$	$\mathcal{O}_{K_0} + \mu^2\mathcal{O}_K$	$\mathcal{O}_{K_0} + \mu^3\mathcal{O}_K$	$\mathcal{O}_{K_0} + \mu^4\mathcal{O}_K$

Table 3.1: Colour coding



A $(C_3, 6, 4)$-volcano.

Chapter 4

A new algorithm for computing Igusa class polynomials

In many applications, we want to construct a curve over a finite field with a prescribed number of points. For an elliptic curve $E/\mathbb{F}_q$, the number of $\mathbb{F}_q$-points on E is given by

$$\chi_\pi(1) = 1 + q - t,$$

where $\chi_\pi(X)$ is the minimal polynomial of the q-power Frobenius π of E. Given a prime power q and $t \in \mathbb{Z}$, the theory of class polynomials gives us a method to construct elliptic curves $E/\mathbb{F}_q$ with $1 + q - t$ points:

Let $D < -4$ be the discriminant of an imaginary quadratic number field K such that there exists some $x \in \mathbb{Z}$ for which

$$x^2 D = t^2 - 4q. \tag{4.1}$$

Then $\mathbb{C}/\mathcal{O}_K$ is an elliptic curve, and its j-invariant is an algebraic integer, the minimal polynomial of which we define to be $H_{\mathcal{O}_K}(X) \in \mathbb{Z}[X]$, the *Hilbert class polynomial for discriminant* D. The reduction of this polynomial modulo q splits completely in $\mathbb{F}_q$ as

$$H_{\mathcal{O}_K}(X) \bmod q = \prod_{\{j=j(E):\, \mathrm{End}(E)=\mathcal{O}_K\}} (X - j) \in \mathbb{F}_q[X]. \tag{4.2}$$

Now suppose that $E/\mathbb{F}_q$ is an elliptic curve whose j-invariant is a root of $H_{\mathcal{O}_K}(X)$ modulo q. Then the q-power Frobenius of E is either π or $\overline{\pi}$, where $\pi = (t - x\sqrt{D})/2$ (so that by (4.1) we have that $q = \pi\overline{\pi}$), and hence $\#E(\mathbb{F}_q) = 1 + q + t$ or $1 + q - t$. If $\#E(\mathbb{F}_q) = 1 + q + t$, then we take its quadratic twist instead.

This method is called the *CM method*, for which efficient computation of

the Hilbert class polynomial is required. One method of computation, first given by Agashe, Lauter, and Venkatesan in [ALV01], is to compute $H_{\mathcal{O}_K}(X)$ mod q for many small q via Equation (4.2) and to compute bounds on the coefficients of $H_{\mathcal{O}_K}(X)$, and then use the Chinese Remainder Theorem to determine $H_{\mathcal{O}_K}(X) \in \mathbb{Z}[X]$. This method, the *CRT method* has the advantage of optimising both running time and space, with the current state-of-the-art being Sutherlands CRT-style algorithm [Sut11] to compute $H_{\mathcal{O}_K}(X)$ mod q (for any positive integer q), which has expected running time $O(|D|^{1+\epsilon})$ and uses $O(|D|^{1/2+\epsilon}\log q)$ space. In this chapter, we will generalise the algorithm given by Sutherland in [Sut11] to genus 2 curves.

For a genus 2 curve $C/\mathbb{F}_q$ with Jacobian $\mathcal{J}(C)$, there exist integers s and t such that the characteristic polynomial of the Frobenius π is given by

$$\chi_\pi(X) = X^4 - tX^3 + (2q + s)X^2 - tqX + q^2.$$

The number of $\mathbb{F}_q$-points on $\mathcal{J}(C)$ is then

$$\#\mathcal{J}(C) = \chi_\pi(1) = 1 - t + 2q + s - tq + q^2$$

and the number of $\mathbb{F}_q$-points on C is $\#C(\mathbb{F}_q) = 1 + q - t$. Let K be a quartic CM-field for which there exists a Weil q-number π such that $K = \mathbb{Q}(\pi)$. We define the *Igusa class polynomials for* $\mathcal{O}_K$ to be

$$H_{\mathcal{O}_K,n}(X) = \prod_{\{C/\mathbb{C}:\mathrm{End}(\mathcal{J}(C))\cong=\mathcal{O}_K\}_\cong} (X - i_n(C)) \in \mathbb{Q}[X]$$

for $n = 1, 2, 3$, where $(i_1, i_2, i_3)(C)$ are the Igusa invariants of C. Exactly as in the genus 1 case, these polynomials split completely modulo q, and the roots of $H_{\mathcal{O}_K,n}(X)$ mod q are exactly the n^{th} Igusa invariants $i_n(C)$ of the genus 2 curve defined over $\mathbb{F}_q$ for which $\mathcal{J}(C)$ has Endomorphism ring $\mathcal{O}_K$. So, if up to isomorphism there are d curves C for which $\mathrm{End}(\mathcal{J}(C)) = \mathcal{O}_K$ with Igusa invariants $(i_1, i_2, i_3)_1, \ldots, (i_1, i_2, i_3)_d$, then the Igusa class polynomials give us a set of d^3 triples of Igusa invariants containing $(i_1, i_2, i_3)_1, \ldots, (i_1, i_2, i_3)_d$. For each of these d curves, the q-power Frobenius of $\mathcal{J}(C)$ is either π or $\overline{\pi}$, and hence $\#C(\mathbb{F}_q)$ is either $1+q+t$ or $1+q-t$, as before. Einsenträger and Lauter gave the first CRT-style algorithm to compute the Igusa class polynomials in their paper [EL09]. All of the known algorithms to compute $H_{\mathcal{O}_K}(X)$ mod q have the same underlying steps:

1. Choose a sufficiently large set of primes S such that for each $p \in S$ there exists a Weil p-number π in K for which $p = \pi\overline{\pi}$ and $K = \mathbb{Q}(\pi)$.

2. For each $p \in S$, search over triples in $\mathbb{F}_p$ for a triple $(i_1, i_2, i_3) \in \mathbb{F}_p^{\times 3}$ corresponding to the Igusa invariants of a genus 2 curve over $\mathbb{F}_p$ with p-power Frobenius π.

3. Starting from (i_1, i_2, i_3), enumerate all the genus 2 curves with endomorphism ring $\mathcal{O}_K$.

In the algorithms currently in use, Step 2 is the major bottleneck. A naïve algorithm for Step 2 as stated as above will take time $O(p^3/N)$ for each $p \in S$, where N is the number of abelian surfaces over $\mathbb{F}_q$ with maximal complex multiplication. Our new algorithm will use RM isomorphism invariants in place of Igusa invariants. The major difference with the algorithms in use and our new algorithm is in step 3, the enumeration of $\mathrm{Inv}_{\mathbb{F}_p}(\mathcal{O}_K)$, which is significantly sped up by methods involving both modular polynomials and isogeny graphs (detailed for elliptic curves in [Sut11]) which were not previously possible in genus 2. Recall from Corollary 2.6.7 that we only need the first two RM isomorphism invariants to determine all three Igusa invariants. So a naïve algorithm for Step 2 will run in time $O(p^2/N')$ for each p, where N' is the number of abelian surfaces over $\mathbb{F}_q$ with maximal *real* multiplication, since the starting point for Step 3 only has to be some point in the isogeny graph rather then something with maximal endomorphism ring (at least if the narrow class number of the maximal totally real subfield of K is 1). Furthermore, until now, all the known class polynomial algorithms were for computing $H_{\mathcal{O}_K,n}$, but with our knowledge of the structure of isogeny graphs, it is now easy to compute $H_{\mathcal{O},n}$ for any order in $\mathcal{O}_K$ (not just the maximal order), as long as $\mathcal{O}$ contains $\mathcal{O}_{K_0}$. However, in practise we are still very limited to our choices for K and hence the primes $p \in S$ by the fact that we only have very small modular polynomials available (see Table 2.1).

4.1 The algorithm

Recall that we defined $\mathbf{POrd}_{\mathbb{C},K_0}$ to be the category of principally polarised complex abelian varieties with real multiplication by $\mathcal{O}_{K_0}$ in Definition 1.5.2. For any $(\mathrm{A},\xi,\iota) \in \mathbf{POrd}_{\mathbb{C},K_0}$, we have that $\mathrm{End}(\mathrm{A})$ is an order in K, some totally imaginary quadratic extension of K_0, and that $\mathcal{O}_{K_0} \subseteq \mathrm{End}(\mathrm{A})$.

By Lemma 1.5.5, objects in $\mathbf{POrd}_{\mathbb{C},K_0}$ correspond to points on the Hilbert modular variety $\overline{V}$ for $\mathrm{SL}(\mathcal{O}_{K_0} \oplus \mathcal{O}_{K_0}^\vee)$. Recall that in Definition 2.1.1 we defined a RM isomorphism invariant for K_0 to be a choice of $d \leq g+1$ Hilbert modular functions $J_1, \ldots, J_d \in \mathbb{Q}(\mathcal{M}_{K_0}(\mathbb{Z})$ such that

$$\mathbb{C}(\overline{V}) = \mathbb{C}(J_1, \ldots, J_d).$$

In particular, in Section 2.2, we showed that there exists a Zariski-open subset U of $\overline{V}$ such that for every $(\mathrm{A},\xi,\iota) \in \mathbf{POrd}_{\mathbb{C},K_0}$ corresponding to a point in U, the d-tuple $(J_1, \ldots, J_d)(\mathrm{A},\xi,\iota)$ determines (A,ξ,ι) up to isomorphism. For any field k, define

$$\mathrm{Inv}_{\mathcal{O}}(k) = \{(J_1,J_2,J_3)(\mathrm{A},\xi,\iota) : (\mathrm{A},\xi,\iota) \in \mathbf{POrd}_{k,K_0}, \mathrm{End}(\mathrm{A}) = \mathcal{O}\}.$$

We will give an algorithm to compute Igusa-Hilbert class polynomials

$$H_{\mathcal{O},n}(X) = \prod_{(a_1,a_2,a_3) \in \mathrm{Inv}_{\mathcal{O}}(\mathbb{C})} (X - a_n) \in \mathbb{Q}[X],$$

for $n = 1, 2, 3$. Recall that in Section 2.5 we detailed how to obtain the Igusa invariants, and hence the curve from the RM isomorphism invariants. Spallek showed in [Spa94, Satz 5.8]that the coefficients of the Igusa class polynomials are in $\mathbb{Q}$, and we have from Lemma 1.5.15 that $\mathbb{Q}(J_1, J_2, J_3) \otimes \mathbb{C} = \mathbb{C}(\overline{V})$, hence the coefficients of the Igusa-Hilbert class polynomials are also in $\mathbb{Q}$. Therefore for sufficiently large primes p, we can reduce $H_{\mathcal{O},n}(X)$ mod p. Also, by Section 2.6, we know that for sufficiently large p, at least two of the RM isomorphism invariants for a genus 2 curve $C/\mathbb{F}_p$ are the reduction mod p of the RM isomorphism invariants of the naïve lift to $\mathbb{Z}$ of C, so that for $n = 1, 2$, we have that

$$H_{\mathcal{O},n}(X) \bmod p = \prod_{(a_1,a_2,a_3)\in \mathrm{Inv}_{\mathcal{O}}(\mathbb{F}_p)} (X - a_n).$$

Recall that the third RM isomorphism invariant J_3 can be expressed as a polynomial in terms of J_1 and J_2. Therefore, our main task is to give an algorithm to compute

$$\prod_{(a_1,a_2,a_3)\in \mathrm{Inv}_{\mathcal{O}}(\mathbb{F}_p)} (X - a_n).$$

Definition 4.1.1. For a prime power q and a Weil q-number π, define the set

$$\mathrm{Inv}_{\pi}(\mathbb{F}_q) = \{(J_1, J_2, J_3)(\mathrm{A}, \xi) : (\mathrm{A}, \xi) \in \mathbf{POrd}_{\pi,K_0}\}.$$

Then, as isogenous abelian varieties have the same endomorphism algebra, we have

$$\mathrm{Inv}_{\mathcal{O}}(\mathbb{F}_q) \subseteq \mathrm{Inv}_{\pi}(\mathbb{F}_q).$$

Definition 4.1.2. For a totally imaginary quadratic extension K of K_0 and an order $\mathcal{O}$ in K stable under complex conjugation such that $\mathcal{O}_{K_0} \subset \mathcal{O} \subseteq \mathcal{O}_K$, define the set $\mathcal{P}_{\mathcal{O}}$ to be

$$\mathcal{P}_{\mathcal{O}} = \left\{ \begin{array}{ll} (q, \pi) \in \mathbb{Z} \times \mathcal{O} : & q \text{ a power of a prime } p \not| [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]] \\ & \text{and } \pi \text{ a Weil } q\text{-number such that } K = \mathbb{Q}(\pi) \end{array} \right\}.$$

This yields Algorithm 4.1.3, in analogy with Sutherlands algorithm [Sut11, Algorithm 1] for computing Hilbert class polynomials.

Algorithm 4.1.3.
INPUT: A totally imaginary quadratic extension K of K_0, an order $\mathcal{O}$ in K stable under complex conjugation such that $\mathcal{O}_{K_0} \subset \mathcal{O} \subseteq \mathcal{O}_K$, and a pair $(q, \pi) \in \mathcal{P}_{\mathcal{O}}$.
OUTPUT: $H_{\mathcal{O},n}(X)$ mod q, for $n = 1, 2, 3$.

1. Search for a genus 2 curve $C/\mathbb{F}_q$ with Jacobian $\mathcal{J}(C) = (\mathrm{A}, \xi, \iota)$ such that $(J_1, J_2, J_3)(\mathrm{A}, \xi, \iota) \in \mathrm{Inv}_{\pi}(\mathbb{F}_q)$. (Algorithm 4.1.4).

2. Find an isogenous triple $(\mathrm{A}', \xi', \iota')$ with $(J_1, J_2, J_3)(\mathrm{A}', \xi', \iota') \in \mathrm{Inv}_{\mathcal{O}_K}(\mathbb{F}_q)$. (Algorithm 4.1.12).

3. Compute the elements of $\mathrm{Inv}_{\mathcal{O}_K}(\mathbb{F}_q)$ by letting the Shimura class group $\mathrm{SCl}(\mathcal{O}_K)$ act on $(J_1, J_2, J_3)(\mathrm{A}', \xi', \iota')$. (Algorithm 4.1.14).

4. List of the elements of $\mathrm{Inv}_{\mathcal{O}}(\mathbb{F}_q)$ by descending in the isogeny graph from $\mathrm{Inv}_{\mathcal{O}_K}(\mathbb{F}_q)$. (Algorithm 4.1.15).

5. For $n = 1, 2, 3$, compute $\prod_{(a_1,a_2,a_3)\in \mathrm{Inv}_{\mathcal{O}}(\mathbb{F}_q)}(X - a_n)$.

4.1.1 Finding a starting curve

Fix a choice (J_1, J_2, J_3) of RM isomorphism invariants. We write $m(X) \in \mathbb{Q}(J_1, J_2)(X)$ for the minimal polynomial of J_3.

Algorithm 4.1.4.
INPUT: A totally imaginary quadratic extension K of K_0, an order $\mathcal{O}$ in K stable under complex conjugation such that $\mathcal{O}_{K_0} \subset \mathcal{O} \subseteq \mathcal{O}_K$, and a pair $(q, \pi) \in \mathcal{P}_{\mathcal{O}}$.
OUTPUT: An element $(J_1, J_2, J_3)(\mathrm{A}, \xi, \iota)$ of $\mathrm{Inv}_\pi(\mathbb{F}_q)$.

Let

$$\chi_\pi(x) = x^4 - tx^3 + sx^2 - qtx + q^2$$

be the characteristic polynomial of π. Recall that by [HEHCC, Theorem 14.17], a genus 2 curve $C/\mathbb{F}_q$ is in the isogeny class corresponding to π if and only if

$$\#C(\mathbb{F}_q) = q + 1 - t (=: M)$$

and

$$\#\mathcal{J}(C)(\mathbb{F}_q) = 1 - t + s - qt + q^2 (=: N).$$

1. Set $(j_1, j_2) = (0, 0) \in \mathbb{F}_q^{\times 2}$.

2. If $j_2 \neq q-1$, set $(j_1, j_2) = (j_1, j_2+1)$. Otherwise, set $(j_1, j_2) = (j_1+1, 0)$.

3. Compute the Igusa Invariants (i_1, i_2, i_3) corresponding to j_1 and j_2 (for example using Example 2.5.4).

4. Use Mestre's algorithm to construct a curve C with Igusa invariants (i_1, i_2, i_3), and compute the Jacobian $\mathcal{J}(C)$ of C.

5. For a random point $P \in \mathcal{J}(C)(\mathbb{F}_q)$, compute NP.

6. If NP is not the identity, then go to Step 2. Otherwise compute $\#\mathcal{J}(C)(\mathbb{F}_q)$.

7. If $\#\mathcal{J}(C)(\mathbb{F}_q) \neq N$, then go to Step 2. Otherwise compute $\#C(\mathbb{F}_q)$.

8. If $\#C(\mathbb{F}_p) \neq M$, then go to Step 2. Otherwise, choose $j_3 \in \mathbb{F}_q$ such that $m(j_3)|_{(J_1,J_2)=(j_1,j_2)} = 0$, and return (j_1, j_2, j_3).

4.1.2 Finding an isogenous curve

For Step 2 of Algorithm 4.1.3, we use the theory of μ-isogeny graphs that we developed in Chapter 3. Our algorithm is a direct generalisation of the genus 1 algorithm given in [Sut11, Algorithm 1.2]. By Theorem 3.1.9, μ-isogeny graphs have exactly the same structure as ℓ-isogeny graphs for elliptic curves. In particular, where the algorithms for genus 1 used modular polynomials to navigate the isogeny graph, we can use the same algorithm but with Hilbert modular polynomials, for example in the following algorithm to compute a path of a maximum given length in the isogeny graph.

Definition 4.1.5. Let V be a vertex in a (Γ, d, v)-volcano, as defined in Definition 3.1.6. We define the *level* of V to be its shortest distance from Γ.

Algorithm 4.1.6.
INPUT: A μ-isogeny graph G for Weil q-number π given by a (Γ, d, v)-volcano containing a vertex V, an integer n, Hilbert modular polynomials $G_\mu(X_1, X_2, X_3, Y)$ and $H_{2,\mu}(X_1, X_2, X_3 Y, Z) \in \mathbb{F}_q[X_1, X_2, X_3, Y, Z]$, and the minimal polynomial $m(X) \in \mathbb{F}_q(J_1, J_2)$ of J_3.
OUTPUT: A path in G starting at V of length at most n and at least $d - L$, where L is the level of V in G.

1. Set $(j_1, j_2, j_3) = V$ and evaluate $G_\mu(j_1, j_2, j_3, Y)$. If $G_\mu(j_1, j_2, j_3, Y)$ is irreducible then return V. Otherwise choose j_1' such that $G_\mu(j_1, j_2, j_3, j_1') = 0$.

2. Set j_2' to be the unique root of $H_{\mu,2}(j_1, j_2, j_3, j_1', Z) = 0$, and define
$$S = \{j \in \mathbb{F}_q : m(X)_{(J_1,J_2)}(j_1', j_2')(j) = 0\}.$$

3. Set j_3 to be the unique $j \in S$ such that $G_\mu(j_1', j_2', j, j_1) = 0$, set $P = [V, (j_1', j_2', j_3')]$, and set $i = 1$.

4. Write (j_1, j_2, j_3) for the $(i-1)^{\text{th}}$ entry of P and (j_1', j_2', j_3') for the i^{th} entry of P. Compute $G_\mu(j_1', j_2', j_3', Y)/(Y - j_1)$, and if it is irreducible return P. Otherwise choose a root j_1''.

5. Set j_2'' to be the unique root of $H_{\mu,2}(j_1', j_2', j_3', j_1'', Z) = 0$, and define
$$S = \{j \in \mathbb{F}_q : m(X)_{(J_1,J_2)}(j_1'', j_2'')(j) = 0\}.$$

6. Set j_3'' to be the unique $j \in S$ such that $G_\mu(j_1'', j_2'', j, j_1') = 0$, append (j_1'', j_2'', j_3'') to P as the $(i+1)^{\text{th}}$ entry, and set $i = i + 1$.

7. If $i = n$, then return P. Otherwise, go to Step 4.

We can also use the purely graph-theoretical algorithms that are already in use for the elliptic curves case. We first recall these algorithms for the sake of completeness.

Algorithm 4.1.7. ([Koh96, p. 46], [Sut11, Algorithm FINDLEVEL]).
INPUT: A (Γ, d, v)-volcano containing a vertex V.
OUTPUT: The level of V.

1. If $\deg(V) \neq v$ then return d, otherwise fix neighbours $V_1 \neq V_1'$ of V.
2. Compute a path $(V, V_1, \ldots, V_{k_1+1})$ of length $k_1 \leq d$. (See Algorithm 4.1.6).
3. Compute a path $(V, V_1', \ldots, V_{k_2+1}')$ of length $k_2 \leq k_1$. (See Algorithm 4.1.6).
4. Return $d - k_2$.

Algorithm 4.1.8. ([Sut11, Algorithm DESCEND]).
INPUT: A (Γ, d, v)-volcano, and a vertex V on the volcano of level $L < d$.
OUTPUT: A vertex V' on the volcano of level $L + 1$.

1. If $L = 0$, compute a path $(V, V_1, \ldots, V_n)$ using Algorithm 4.1.6 and return $V' = V_{n-d+1}$.
2. If $L > 0$, fix neighbours $V_1 \neq V_1'$ of V.
3. Compute a path $(V, V_1, \ldots, V_{d-L})$ using Algorithm 4.1.6.
4. If $\deg(V_{d-L}) = 1$ then return $V' = V_1$, else return $V' = V_1'$.

Algorithm 4.1.9. ([Sut11, Algorithm ASCEND]).
INPUT: A (Γ, d, v)-volcano, and a vertex V on the volcano of level $L > 0$.
OUTPUT: A vertex V' on the volcano of level $L - 1$.

1. If $\deg(V) = 1$ then let V' be the neighbour of V and return V', else label the neighbours of V as $(V^{(1)})_1, \ldots, (V^{(v)})_1$.
2. For $i = 1, \ldots, v - 1$,
   (a) compute a path $(V, (V^{(i)})_1, \ldots, (V^{(i)})_{d-L})$ using Algorithm 4.1.6
   (b) if $\deg((V^{(i)})_{d-L}) > 1$, then return $V' = (V^{(i)})_{d-L}$.
3. Return $V' = (V^{(v)})_1$.

Definition 4.1.10. Given $(q, \pi) \in \mathcal{P}_{\mathcal{O}_K}$, let $n = [\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]]$ and define the set $S_{K,\pi}$ by

$$S_{K,\pi} = \left\{\mu \in \mathcal{O}_{K_0}^+ : n\mathcal{O}_{K_0} \subseteq \mu\mathcal{O}_{K_0} \text{ and } \mu\mathcal{O}_{K_0} \text{ prime}\right\} / \sim,$$

where $\mathcal{O}_{K_0}^+$ denotes the totally positive elements in $\mathcal{O}_{K_0}$, and $\mu \sim \mu'$ if and only if there is a totally positive unit $u \in \mathcal{O}_{K_0}$ such that $\mu = u\mu'$.

Definition 4.1.11. For a totally imaginary quadratic extension K of K_0 and an order $\mathcal{O}$ in K such that $\mathcal{O}_{K_0} \subset \mathcal{O} \subseteq \mathcal{O}_K$, given $(\mathrm{A}, \xi) \in \mathbf{POrd}_{\pi,K_0}$ with $\mathrm{End}(\mathrm{A}) = \mathcal{O}$, let $\mathfrak{f}_{\mathcal{O}} = (\mathcal{O} : \mathcal{O}_K)$ be the conductor of $\mathcal{O}$, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the prime ideals of $\mathcal{O}_K$ dividing $\mathfrak{f}_{\mathcal{O}}$. We define

$$S_{\mathcal{O}} = \{\mu \in \mathcal{O}_{K_0}^+ : \text{ for some } i \in [1, k],\ \mu\mathcal{O}_{K_0} = \mathfrak{p}_i\}/\sim.$$

Now for every $\mu \in S_{\mathcal{O}}$, we have by Theorem 3.1.9 that (A, ξ, ι) is a vertex in a μ-isogeny volcano of depth

$$\max\{n \in \mathbb{Z} : \mathfrak{f}_{\mathbb{Z}[\pi,\bar{\pi}]} \subseteq \mu^n \mathcal{O}_K\}.$$

Algorithm 4.1.12.
INPUT: A real quadratic number field K_0 of narrow class number 1, a totally imaginary quadratic extension K of K_0, an order $\mathcal{O}$ in K stable under complex conjugation such that $\mathcal{O}_{K_0}[\pi, \overline{\pi}] \subset \mathcal{O} \subseteq \mathcal{O}_K$, a pair $(q, \pi) \in \mathcal{P}_{\mathcal{O}}$, and $v_0 \in \mathrm{Inv}_{\pi}(\mathbb{F}_q)$.
OUTPUT: $V \in \mathrm{Inv}_{\mathcal{O}_K}(\mathbb{F}_q)$.

1. Write $S_{K,\pi} = \{\mu_1, \ldots, \mu_k\}$.
2. For $i = 1, \ldots, k$, factor the modular polynomial $G_{\mu_i}(v_{i-1}, Y)$ mod q, and if $G_{\mu_i}(v_{i-1}, Y)$ has at least one linear factor mod q, then
   (a) first use Algorithm 4.1.7 to determine the level of v_{i-1} in its μ_i-isogeny volcano, and then
   (b) use Algorithm 4.1.9 to obtain v_i of depth 0 in the μ_i-volcano
3. Return v_k.

4.1.3 Enumerating curves with the same endomorphism ring

For a totally imaginary quadratic extension K of K_0, an order $\mathcal{O}$ in K stable complex conjugation such that $\mathcal{O}_{K_0} \subset \mathcal{O}$, and an element $(q, \pi) \in \mathcal{P}_{\mathcal{O}}$, suppose that we have an element $(j_1, j_2, j_3) \in \mathrm{Inv}_{\mathcal{O}}(\mathbb{F}_q)$. We want to use this element to determine $\mathrm{Inv}_{\mathcal{O}}(\mathbb{F}_q)$ completely. To do this, we can again make use of the volcano structure of μ-isogeny graphs, imitating the algorithm for genus 1 in [Sut11, Algorithm 1.3]. In Algorithm 4.1.13 below we give a simple path-walking algorithm along a cycle, when the cycle is the connected component of μ-isogeny graph.

Algorithm 4.1.13.
INPUT: A totally imaginary quadratic extension K of K_0, an element $(q, \pi) \in \mathcal{P}_{\mathcal{O}_K}$, a totally positive prime element $\mu \in K_0$ such that $\mu\mathcal{O}_K$ and $\mathfrak{f}_{\mathbb{Z}[\pi,\overline{\pi}]}$ are coprime, and an element $v_0 \in \mathrm{Inv}_{\mathcal{O}_K}(\mathbb{F}_q)$. Also modular polynomials $G_{\mu}(X_1, X_2, X_3, Y)$ and $H_{\mu,2}(X_1, X_2, X_3, Y, Z_2) \in \mathbb{F}_q[X_1, X_2, X_3, Y, Z_2]$ and the minimal polynomial $m(X) \in \mathbb{F}_q(J_1, J_2)[X]$ of J_3.
OUTPUT: The μ-isogeny graph for Weil q-number π containing v_0.

1. Let j be the first coordinate of v_0, and factor $G_{\mu}(v_0, Y)/(Y - j)$ mod q. If it
   (a) is irreducible, return v_0.

(b) has exactly one $\mathbb{F}_q$-rational root, let this root be j_1 and let j_2 be the unique root of $H_{\mu,2}(v_0, j_1, Z_2)$. Write $v_0 = (j_1', j_2', j_3')$ and let j_3 be the unique root of $m(X)$ evaluated at $(J_1, J_2) = (j_1, j_2)$ for which $G_\mu(j_1, j_2, j_3, j_1') = 0$. Return the 2-cycle $(v_0, (j_1, j_2, j_3))$

(c) has two $\mathbb{F}_q$-rational roots, choose one and call it j_1.

2. Let j_2 be the unique root of $H_{\mu,2}(v_0, j_2, Z_2)$. Write $v_0 = (j_1', j_2', j_3')$ and let j_3 be the unique root of $m(X)$ evaluated at $(J_1, J_2) = (j_1, j_2)$ for which $G_\mu(j_1, j_2, j_3, j_1') = 0$. Set $v_1 = (j_1, j_2, j_3)$ and $N = 1$.

3. Let $j_1^{(N-1)}$ be the first coordinate of v_{N-1}, and factor $G_\mu(v_N, Y)/(Y - j^{(N-1)})$. Let $j_1^{(N+1)}$ be the unique $\mathbb{F}_q$-rational root.

4. Let $j_2^{(N+1)}$ be the unique root of $H_{\mu,2}(v_N, j_1^{(N+1)}, Z_2)$. Let $j_3^{(N+1)}$ be the unique root of $m(X)$ evaluated at $(J_1, J_2) = (j_1^{(N+1)}, j_2^{(N+1)})$ for which $G_\mu(j_1^{(N+1)}, j_2^{(N+1)}, j_3^{(N+1)}, j_1^{(N)}) = 0$. Set $v_{N+1} = (j_1^{(N+1)}, j_2^{(N+1)}, j_3^{(N+1)})$.

5. If $v_{N+1} = v_0$, then return the the $(N+1)$-cycle $(v_0, \ldots, v_{N+1})$. Otherwise, set $N = N + 1$ and go to Step 3.

Recall that by Proposition 3.1.18, we have that

$$\#\mathrm{SCl}(\mathcal{O}) = \#\mathrm{Inv}_{\mathcal{O}}(\mathbb{F}_q),$$

and by Theorem 3.1.9, for any totally positive prime μ in $\mathcal{O}_{K_0}$ such that $\mu\mathcal{O}_K$ is split, if $\mathfrak{f}_{\mathcal{O}}$ and $\mu\mathcal{O}_K$ are coprime, then the μ-isogeny graph containing $V \in \mathrm{Inv}_{\mathcal{O}}(\mathbb{F}_q)$ is a cycle of length n, where n is the order of $[(\mathfrak{m}, \mu)]$ in $\mathrm{SCl}(\mathcal{O})$. This yields Algorithm 4.1.14.

Algorithm 4.1.14.
INPUT: A totally imaginary quadratic extension K of K_0, an element $(q, \pi) \in \mathcal{P}_{\mathcal{O}_K}$, and an element $v_0 \in \mathrm{Inv}_{\mathcal{O}_K}(\mathbb{F}_q)$.
OUTPUT: The set $\mathrm{Inv}_{\mathcal{O}_K}(\mathbb{F}_q)$.

1. If $\#\mathrm{SCl}(\mathcal{O}_K) = 1$, then return $\{v_0\}$.

2. Otherwise, choose totally positive prime elements $\mu_1, \ldots, \mu_n \in \mathcal{O}_{K_0} - S_{\mathcal{O}}$ such μ_i splits in K and, if h_i is the size of the μ_i-isogeny graph containing v_0, then $h_1, \ldots, h_n$ are coprime and $\#\mathrm{SCl}(\mathcal{O}_K) = \prod_{i=1}^n h_i$.

3. Compute the μ_1-isogeny graph G_1 containing v_0 using Algorithm 4.1.13 and let V_1 be the set of vertices of G_1. Set $i = 1$. If $n = 1$ then return V_1.

4. For every element $v \in V_i$, compute the μ_{i+1}-isogeny graph $G_{i+1,v}$ containing v using Algorithm 4.1.13.

5. For every $v \in V_i$, let $V_{i+1,v}$ be the set of vertices of $G_{i+1,v}$, and set $V_{i+1} = \bigcup_{v \in V_i} V_{i+1,v}$.

6. If $n = i + 1$, then return V_{i+1}. Otherwise, set $i = i + 1$ and go to Step 4.

Algorithm 4.1.15.
INPUT: An order $\mathcal{O} \subset \mathcal{O}_K$ stable under complex conjugation and containing $\mathcal{O}_{K_0}$, an element $(q, \pi) \in \mathcal{P}_{\mathcal{O}_K}$, and the set $\mathrm{Inv}_{\mathcal{O}_K}(\mathbb{F}_q)$. Also Hilbert modular polynomials $G_\mu(X_1, X_2, X_3, Y)$ and $H_{\mu,2}(X_1, X_2, X_3, Y, Z_2) \in \mathbb{F}_q[X_1, X_2, X_3, Y, Z_2]$, and the minimal polynomial $m(X) \in \mathbb{F}_q(J_1, J_2)[X]$ of J_3.
OUTPUT: The set $\mathrm{Inv}_{\mathcal{O}}(\mathbb{F}_q)$.

1. Compute $\mathfrak{f}_{\mathcal{O}} = (\mathcal{O} : \mathcal{O}_K)$ and $f = [\mathcal{O}_K : \mathcal{O}]$. Define

   $$\{\mu_1, \ldots, \mu_k\} = \{\mu \in \mathcal{O}_{K_0} : f\mathcal{O}_{K_0} \subseteq \mu\mathcal{O}_{K_0},\ \mu \text{ totally positive, prime }\}/\sim .$$

   Then for $i = 1, \ldots, k$, define

   $$d_i = \max\{d \in \mathbb{Z} : \mathfrak{f}_{\mathcal{O}} \subseteq \mu_i^d \mathcal{O}_K\}.$$

   If $\prod_{i=1}^k \mu_i^{d_i}\mathcal{O}_K \neq \mathfrak{f}_{\mathcal{O}}$, then abort. Otherwise, set $i = 1$ and $V_{1,0} = \mathrm{Inv}_{\mathcal{O}_K}(\mathbb{F}_q)$.

2. If $d_i = 0$, then go to Step 6. Otherwise, for every $v \in V_{i,0}$, write $(j_1, j_2, j_3) = v$. Factor $G_{\mu_i}(j_1, j_2, j_3, X)$, and write R for the set of roots. For every $j_1' \in R$, define j_2' to be the unique element of $\mathbb{F}_q$ satisfying $H_{\mu_i,2}(j_1, j_2, j_3, j_1', j_2') = 0$, and define j_3' to be the unique root of $m(X)_{(J_1,J_2)=(j_1,j_2)}$ that satisfies $G_\mu(j_1', j_2', j_3', j_1)$. Define

   $$V_{i,1,v} = \{(j_1', j_2', j_3') : j_1' \in R,\ (j_1', j_2', j_3') \notin V_{i,0}\}.$$

   Then define

   $$V_{i,1} = \bigcup_{v \in V_{i,0}} V_{i,1,v}.$$

3. If $d_i = 1$, go to Step 6. Otherwise, set $d = 1$.

4. For every $v \in V_{i,d}$, write $(j_1, j_2, j_3) = v$. Factor $G_{\mu_i}(j_1, j_2, j_3, X)$, and write R for the set of roots. For every $j_1' \in R$, define j_2' to be the unique element of $\mathbb{F}_q$ satisfying $H_{\mu_i,2}(j_1, j_2, j_3, j_1', j_2') = 0$, and define j_3' to be the unique root of $m(X)_{(J_1,J_2)=(j_1,j_2)}$ that satisfies $G_\mu(j_1', j_2', j_3', j_1)$. Define

   $$V_{i,d+1,v} = \{(j_1', j_2', j_3') : j_1' \in R,\ (j_1', j_2', j_3') \notin V_{i,d-1}\}.$$

   Then define

   $$V_{i,d+1} = \bigcup_{v \in V_{i,d}} V_{i,d+1,v}.$$

5. If $d + 1 = d_i$, go to Step 6, otherwise set $d = d + 1$ and go to Step 4.

6. If $i = k$, return V_{i,d_i}. Otherwise, set $V_{i+1,0} = V_{i,d_i}$ and $i = i + 1$, and go to Step 2.

4.1.4 Computing the Igusa-Hilbert class polynomials

With Algorithm 4.1.3 we can now compute the Igusa-Hilbert class polynomials modulo infinitely many primes. We can compute bounds on the coefficients for example by approximating the complex coefficients via interval arithmetic and using the denominator bounds of Goren-Lauter in [GL07], so that we can completely determine the coefficients of the Igusa-Hilbert polynomials using the Chinese Remainder Theorem. We use methods of [Sut11, Section 6] to apply the Chinese Remainder Theorem in the most efficient way. To choose the primes p (or prime powers q) for which we compute the Igusa-Hilbert class polynomials mod q we use the following algorithm:

Algorithm 4.1.16.
INPUT: A totally imaginary quadratic extension K of K_0, an order $\mathcal{O}$ in K stable under complex conjugation such that $\mathcal{O}_{K_0} \subset \mathcal{O}$, an integer n, and an upper bound B on the coefficients of the Igusa-Class polynomials.
OUTPUT: A subset of $\mathcal{P}_{\mathcal{O}}$ for which the running time of Algorithm 4.1.4 is optimised with respect to this choice, and which is enough to completely determine the Igusa-Hilbert class polynomials via the Chinese Remainder Theorem if the bound B is correct.

1. Write $\mathcal{P}_{\mathcal{O}} = \{(q_0, \pi_0), (q_1, \pi_1), \ldots\}$, where $q_i \leq q_{i+1}$, set $i = 0$, and let S be the empty set.

2. If $[\mathcal{O}_K : \mathbb{Z}[\pi_i, \bar{\pi}_i]]$ has at least n prime divisors:

   (a) add (q_i, π_i) to S,

   (b) then if $\prod_{(q,\pi)\in S} q > 4B$, return S, otherwise set $i = \min\{j \in \mathbb{Z}_{>i} : q_j \neq q_i\}$ and go to the beginning of Step 2.

   Otherwise, set $i = i + 1$ and repeat.

We ask for at least 'n' divisors so that the class of isogenous curves is large, increasing the likelihood of finding a curve with the correct Frobenius in Algorithm 4.1.4.

Bibliography

[ALV01] A. Agashe, K. Lauter, R. Venkatesan *Constructing elliptic curves with a given number of points over a finite field*, Fields Insitute Comm. Series, Vol. 42 (2001)

[Bass63] H. Bass *On the ubiquity of Gorenstein rings*, Mathematische Zeitschrift, 82:8-28 (1963)

[BB64] W.L. Baily and A. Borel, *On the compactification of arithmetically defined quotients of bounded symmetric domains*, Bull. Amer. Math. Soc. 70 No. 4, 588593 (1964)

[BJW16] E.H. Brooks, D. Jetchev, and B. Wesolawski, *Isogeny graphs of ordinary abelian varieties*, `https://arxiv.org/abs/1609.09793` (2016)

[BLR90] S. Bosch, W. Lütkebonmert, M. Raynaud *Néron Models*, Springer-Verlag (1990)

[BS15] G. Bisson and M. Streng, *On polarised class groups of orders in quartic CM-fields*, `http://arxiv.org/pdf/1302.3756v5.pdf` (2015)

[Del69] P. Deligne, *Variétés abéliennes sur un corps fini*, Invent. Math. 8 (1969), 238-243

[Dol14] I.V. Dolgachev, *Abelian Scheme* Enc. of Math. `http://www.encyclopediaofmath.org/index.php?title=Abelian_scheme&oldid=31904` (2014)

[Dup06] R. Dupont *Moyenne Arithmético-géométrique, Suites de Borchant et Applications* `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/these_soutenance.pdf`, PhD thesis (2006)

[EL09] K. Eisenträger and K. Lauter *A CRT algorithm for constructing genus 2 curves over finite fields*, Séminaires et Congrès Vol. 21, p. 161-176 (2009)

[ET14] A. Enge and E. Thomé *Computing class polynomials for abelian surfaces* `https://eprint.iacr.org/2013/299.pdf` Exp. Math. Vol. 23, p. 129-145 (2014)

[FC90] G. Faltings and C.-L. Chai, *Degeneration of Abelian Varieties*, Springer-Verlag, Vol. 22 (1990)

[FGIKNV05] B.Fantechi, L. Göttsche, L. Illusie, S.L. Kleiman, N. Nitsure, A. Vistoli, *Fundamental Algebraic Geometry: Grothendieck's FGA Explained*, AMS Math. Surveys and Monographs Vol.123 (2005)

[vdG88] G. van der Geer, *Hilbert modular surfaces*, Springer-Verlag, Vol.16 (1988)

[GKS11] P. Gaudry, D. Kohel, and B, Smith *Counting Points on Genus 2 Curves with Real Multiplication*, Lee D.H., Wang X. (eds) Advances in Cryptology - ASIACRYPT 2011. Lecture Notes in Computer Science, vol 7073. Springer, Berlin, Heidelberg (2011)

[Gor02] Eyal Z. Goren, *Lectures on Hilbert Modular Varieties and Modular Forms*, CRM Monograph Series (2002) Volume 14.

[GL07] E. Goren and K. Lauter *Class Invariants for quartic CM fields*, Ann. de l'Institut Fourier, Tome 57, no. 2, p.457-480 (2007)

[Gun63] K.-B. Gundlach, *Die Bestimmung der Funktionen zur Hilbertschen Modulgruppe des Zahlkrpers* $\mathbb{Q}(\sqrt{5})$, Math. Ann. 152 p. 226-256 (1963) (German)

[Har77] R. Hartshorne, *Algebraic Geometry*, Springer Vol. 52 (1977)

[HEHCC] R.M. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Math. and its Applications, Vol. 34 (2005)

[Hon68] T. Honda *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan 20, no. 1-2, 83–95. (1968)

[How95] E. Howe, *Principally Polarized Ordinary Abelian Varieties over Finite Fields*, Trans. of the AMS, Vol. 347, No. 7 (1995)

[HS00] M. Hindry and J.H. Silverman *Diophantine Geometry: An Introduction*, Springer, Vol. 201 (2000)

[Igu62] J. Igusa. *On Siegel modular forms of genus two*, Amer. J. Math. 84 (1962), 175200. MR0141643 (25:5040)

[Igu60] J. Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. vol. 72 (1960) 612-649.

[IT14] S. Ionica and E. Thomé *Isogeny graphs of genus 2 curves with Maximal Real Multiplication* `https://eprint.iacr.org/2014/230.pdf` (2014)

[Kat] *Serre-Tate local moduli* `https://web.math.princeton.edu/~nmk/old/serretatelocmod.pdf`

[Knu91] M.-A. Knus, *Quadratic and Hermitian Forms over Rings*, Springer, Vol. 294 (1991)

[Koh96] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis (1996)

[BGLMMST17] S. Ballentine, A. Guillevic, E. Lorenzo-Garcia, M. Maisserer, C. Martindale, B. Smith, and J. Top, *Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication*, Springer (2017)

[Liu02] Q. Liu *Algebraic geometry and arithmetic curves*, Oxf. Uni. Press, Vol. 6 (2002)

[LMFDB] J. Cremona et. al., *L-Functions and Modular Forms Database*, `www.lmfdb.org`

[LNY15] K. Lauter, M. Naehrig, and T. Yang *Hilbert theta series and invariants of genus 2 curves*, J. of Number Theory (2015)

[LR12] K. Lauter and D. Robert *Improved CRT Algorithm for Class Polynomials in Genus 2*, ANTS X - Algorithmic Number Theory 2012, Math. Sci. Pub., Vol 1., p. 437-467 (2013)

[LST64] J. Lubin, J.P. Serre, and J. Tate *Elliptic Curves and Formal Groups* `http://www.ma.utexas.edu/users/voloch/lst.html` (1964)

[LY11] Kristin Lauter, Tonghai Yang, *Computing genus 2 curves from invariants on the Hilbert moduli space*, Journal of Number Theory 131 (2011) 936-958.

[Mar15] C. Martindale, *The theory of canonical lifts*, `https://pub.math.leidenuniv.nl/~martindalecr` (2015)

[May07] S. Mayar, *Hilbert Modular Forms for the Fields* $\mathbb{Q}(\sqrt{5})$*,* $\mathbb{Q}(\sqrt{13})$ *and* $\mathbb{Q}(\sqrt{17})$ PhD thesis (2007)

[Mes90] J.-F. Mestre, *Construction de courbes de genre 2 a partir de leurs modules*, Effective methods in algebraic geometry, Castiglioncello, (1990), 313-334

[MFK94] D. Mumford, J. Fogarty, and F. Kirwan *Geometric Invariant Theory*, Springer (1994)

[Mul83] R. Müller, *Hilbertsche Modulformen und Modulfunktionen zu* $\mathbb{Q}(\sqrt{8})$, Math. Ann. 266 (1983), no. 1, 83103 (German).

[Mul85] R. Müller, *Hilbertsche Modulformen und Modulfunktionen zu* $\mathbb{Q}(\sqrt{5})$, Arch. der Math. 45 (1985), Issue 3, 239-251 (German).

[Nag83] S. Nagaoka, *On the ring of Hilbert modular forms over* $\mathbb{Z}$, J. Math. Soc. Japan 35 (1983) 589-608.

[Nag58] M. Nagata, *Remarks on a paper of Zariski on the purity of branch-loci*, Proc. Natl. Acad. Sci. U.S.A. 44 no. 8 (1958). 796-9.

[Nak61] Y. Nakai *On the theory of differentials in commutative rings*, J. Math. Soc. Japan, Vol. 13, No. 1 (1961)

[Nak63] Y. Nakai *Notes on Invariant Differentials on Abelian Varieties* J. Sci. Hiroshima Univ. Ser. A-I Math. 27 (1963), no. 1, 7–34. `https://projecteuclid.org/download/pdf_1/euclid.hmj/1206139663`

[Orr15] M. Orr, *On compatibility between isogenies and polarisations of Abelian varities*, arXiv:1506.04011v1 (2015)

[Ray70] M. Raynaud *Faisceaux amples sur les schmas en groupes et les espaces homognes*, Springer, Vol. 119 (1970)

[Rap78] M. Rapoport, *Compactifications de lespace de modules de Hilbert-Blumenthal*, Comp. Math., tome 36, no. 3 (1978), p. 255-335.

[Res74] H.L. Resnikoff, *On the Graded Ring of Hilbert modular forms associated with* $\mathbb{Q}(\sqrt{5})$, Math. Ann. 208 (1974) 161-170.

[Sij09] J. Sijsling, *What is... a Polarization?*, http://pub.math.leidenuniv.nl/ strengtc/cm/polariz.pdf (2009)

[Sil94] J. Silverman *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, Vol. 151 (1994)

[Spa94] A-M. Spallek *Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen* (1994).

[ST61] G. Shimura and Y. Taniyama *Complex Multiplication*, Math. Soc. of Japan (1961)

[Str10] M. Streng, *Complex Multiplication of Abelian Surfaces* PhD thesis, Universiteit Leiden (2010).

[Sut13] A. Sutherland *Isogeny Volcanoes* `http://arxiv.org/pdf/1208.5370.pdf` (2013)

[Sut11] A. Sutherland *Computing Hilbert Class Polynomials with the Chinese Remainder Theorem*, Math. Comp. Vol 80, p. 501-538 (2011)

[Tat67] *Proceedings of a Conference on Local Fields* pp 158-183 (1967)

[Wem99] P. van Wemelen, *Examples of Genus Two CM Curves Defined over the Rationals*, Math. Comp. 68(225), (1999), 307-320.

[Zar58] O. Zariski, *On the purity of the branch locus of algebraic functions*, Proc. Natl. Acad. Sci. U.S.A. 44 no. 8 (1958). 791-6.