Moduli of CM False Elliptic Curves

Author: Andrew Phillips

Boston College Electronic Thesis or Dissertation, 2015

Boston College

The Graduate School of Arts and Sciences

Department of Mathematics

MODULI OF CM FALSE ELLIPTIC CURVES

a dissertation

by

ANDREW PHILLIPS

submitted in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

May 2015

MODULI OF CM FALSE ELLIPTIC CURVES

Andrew Phillips

Advisor: Benjamin Howard

Abstract

We study two moduli problems involving false elliptic curves with complex multiplication (CM), generalizing theorems about the arithmetic degree of certain moduli spaces of CM elliptic curves. The first moduli problem generalizes a space considered by Howard and Yang, and the formula for its arithmetic degree can be seen as a calculation of the intersection multiplicity of two CM divisors on a Shimura curve. This formula is an extension of the Gross-Zagier theorem on singular moduli to certain Shimura curves. The second moduli problem we consider deals with special endomorphisms of false elliptic curves. The formula for its arithmetic degree generalizes a theorem of Kudla, Rapoport, and Yang.

Contents

Acknowledgments

Above all, I would like to thank my advisor Ben Howard for suggesting the problem considered in this thesis and answering all of my countless questions. I also want to thank Avner Ash and Mark Reeder for being on my thesis committee.

Chapter 1

Introduction

In this thesis we study two moduli problems involving false elliptic curves with complex multiplication (CM), generalizing theorems about the arithmetic degree of certain moduli stacks of CM elliptic curves. The first moduli problem, and the one that occupies most of our effort in generalizing, is the main arithmetic content of [14]. The result of that paper can be seen as a refinement of the well-known formula of Gross and Zagier on singular moduli in [11]. We begin by describing how the Gross-Zagier formula and the result of [14] can be interpreted as statements about intersection theory on a modular curve. Our generalization of [14] has a similar interpretation as a result about intersection theory, but now on a Shimura curve. The other moduli problem we study generalizes a space considered in [16].

1.1 Elliptic curves

Let K_1 and K_2 be non-isomorphic imaginary quadratic fields and set $K = K_1 \otimes_{\mathbb{Q}} K_2$. Let F be the real quadratic subfield of K and let $\mathfrak{D} \subset \mathcal{O}_F$ be the different of F. We assume K_1 and K_2 have relatively prime discriminants d_1 and d_2, so K/F is unramified at all finite places and $\mathcal{O}_{K_1} \otimes_{\mathbb{Z}} \mathcal{O}_{K_2}$ is the maximal order in K.

Let $\mathscr{M}$ be the category fibered in groupoids over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{M}(S)$ the category of elliptic curves over the $\mathcal{O}_K$-scheme S. The category $\mathscr{M}$ is an algebraic stack (in the sense of [27], also known as a Deligne-Mumford stack) which is regular and smooth of relative dimension 1 over $\mathrm{Spec}(\mathcal{O}_K)$ (so it is 2-dimensional). For $j \in \{1, 2\}$ let $\mathscr{C}_j$ be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{C}_j(S)$ the category of elliptic curves over the $\mathcal{O}_K$-scheme S with complex multiplication by $\mathcal{O}_{K_j}$. When we speak of an elliptic curve E over an $\mathcal{O}_K$-scheme S with complex multiplication by $\mathcal{O}_{K_j}$, we are assuming that the action $\mathcal{O}_{K_j} \to \mathrm{End}_{\mathscr{O}_S}(\mathrm{Lie}(E))$ is through the structure map $\mathcal{O}_{K_j} \hookrightarrow \mathcal{O}_K \to \mathscr{O}_S(S)$.

The stack $\mathscr{C}_j$ is finite and étale over $\operatorname{Spec}(\mathcal{O}_K)$, so in particular it is 1-dimensional and regular. There is a finite morphism $\mathscr{C}_j \to \mathscr{M}$ defined by forgetting the complex multiplication structure.

A *divisor* on an algebraic stack $\mathscr{X}$ is an element of the free abelian group $\operatorname{Div}(\mathscr{X})$ generated by the integral closed substacks of codimension 1 (the *prime* divisors). Even though the morphism $f : \mathscr{C}_j \to \mathscr{M}$ is not a closed immersion, we view $\mathscr{C}_j$ as a divisor on $\mathscr{M}$ through the image of f ([27, Definition 1.7]). A natural question to now ask is: what is the intersection multiplicity, defined in the appropriate sense below, of the two divisors $\mathscr{C}_1$ and $\mathscr{C}_2$ on $\mathscr{M}$? More generally, if $T_m : \operatorname{Div}(\mathscr{M}) \to \operatorname{Div}(\mathscr{M})$ is the m-th Hecke correspondence on $\mathscr{M}$, what is the intersection multiplicity of $T_m\mathscr{C}_1$ and $\mathscr{C}_2$?

If $\mathscr{D}_1$ and $\mathscr{D}_2$ are two prime divisors on $\mathscr{M}$ intersecting properly, meaning $\mathscr{D}_1 \cap \mathscr{D}_2 = \mathscr{D}_1 \times_{\mathscr{M}} \mathscr{D}_2$ is an algebraic stack of dimension 0 (see [27, Definition 7.9] for the definition of fiber products), define the *intersection multiplicity* of $\mathscr{D}_1$ and $\mathscr{D}_2$ on $\mathscr{M}$ to be

$$I(\mathscr{D}_1, \mathscr{D}_2) = \sum_{\mathfrak{P} \subset \mathcal{O}_K} \log(|\mathbb{F}_{\mathfrak{P}}|) \sum_{x \in [(\mathscr{D}_1 \cap \mathscr{D}_2)(\overline{\mathbb{F}}_{\mathfrak{P}})]} \frac{\operatorname{length}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_1 \cap \mathscr{D}_2, x})}{|\operatorname{Aut}(x)|}, \tag{1.1.1}$$

where $[(\mathscr{D}_1 \cap \mathscr{D}_2)(S)]$ is the set of isomorphism classes of objects in the category $(\mathscr{D}_1 \cap \mathscr{D}_2)(S)$ and $\mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_1 \cap \mathscr{D}_2, x}$ is the strictly Henselian local ring of $\mathscr{D}_1 \cap \mathscr{D}_2$ at the geometric point x (the local ring for the étale topology). Also, the outer sum is over all prime ideals $\mathfrak{P} \subset \mathcal{O}_K$, $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$, and $\operatorname{Spec}(\overline{\mathbb{F}}_{\mathfrak{P}})$ is an $\mathcal{O}_K$-scheme through the reduction map $\mathcal{O}_K \to \mathbb{F}_{\mathfrak{P}}$. This number is also called the *arithmetic degree* of the 0-dimensional stack $\mathscr{D}_1 \cap \mathscr{D}_2$ and is denoted $\deg(\mathscr{D}_1 \cap \mathscr{D}_2)$. The definition of $I(\mathscr{D}_1, \mathscr{D}_2)$ is extended to all divisors $\mathscr{D}_1$ and $\mathscr{D}_2$ by bilinearity, assuming $\mathscr{D}_1$ and $\mathscr{D}_2$ intersect properly (that is, the supports of $\mathscr{D}_1$ and $\mathscr{D}_2$ intersect properly).

The intersection multiplicity $I(\mathscr{C}_1, \mathscr{C}_2)$ relates to the Gross-Zagier formula on singular moduli as follows. Let $L \supset K$ be a number field and suppose E_1 and E_2 are elliptic curves over $\operatorname{Spec}(\mathcal{O}_L)$. The j-invariant determines an isomorphism of schemes $M_{/\mathcal{O}_L} \cong \operatorname{Spec}(\mathcal{O}_L[x])$, where $M \to \operatorname{Spec}(\mathcal{O}_K)$ is the coarse moduli scheme associated with $\mathscr{M}$, and the elliptic curves E_1 and E_2 determine morphisms $\operatorname{Spec}(\mathcal{O}_L) \rightrightarrows M_{/\mathcal{O}_L}$. These morphisms correspond to ring homomorphisms $\mathcal{O}_L[x] \rightrightarrows \mathcal{O}_L$ defined by $x \mapsto j(E_1)$ and $x \mapsto j(E_2)$. Let D_1 and D_2 be the divisors on $M_{/\mathcal{O}_L}$ defined by the morphisms $\operatorname{Spec}(\mathcal{O}_L) \rightrightarrows M_{/\mathcal{O}_L}$. Then

$$D_1 \cap D_2 = \operatorname{Spec}(\mathcal{O}_L \otimes_{\mathcal{O}_L[x]} \mathcal{O}_L) \cong \operatorname{Spec}(\mathcal{O}_L/(j(E_1) - j(E_2))).$$

For τ an imaginary quadratic integer in the complex upper half plane, let $[\tau]$ be its equivalence class under the action of $\mathrm{SL}_2(\mathbb{Z})$. As in [11] define

$$J(d_1, d_2) = \Bigg(\prod_{\substack{[\tau_1],[\tau_2] \\ \mathrm{disc}(\tau_i)=d_i}} (j(\tau_1) - j(\tau_2)) \Bigg)^{4/(w_1 w_2)},$$

where $w_i = |\mathcal{O}_{K_i}^\times|$. It follows from the above discussion that the main result of [11], which is a formula for the prime factorization of the integer $J(d_1, d_2)^2$, is essentially the same as giving a formula for $\deg(\mathscr{C}_1 \cap \mathscr{C}_2) = I(\mathscr{C}_1, \mathscr{C}_2)$.

For each positive integer m define $\mathscr{T}_m$ to be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{T}_m(S)$ the category of triples (E_1, E_2, f) with E_i an object of $\mathscr{C}_i(S)$ and $f \in \mathrm{Hom}_S(E_1, E_2)$ satisfying $\deg(f) = m$ on every connected component of S. In [14] it is shown that there is a decomposition

$$\mathscr{T}_m = \bigsqcup_{\substack{\alpha \in F^\times \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha)=m}} \mathscr{E}'_\alpha$$

for some 0-dimensional stacks $\mathscr{E}'_\alpha \to \mathrm{Spec}(\mathcal{O}_K)$ and then a formula is given for each term in

$$\deg(\mathscr{T}_m) = \sum_{\substack{\alpha \in \mathfrak{D}^{-1}, \alpha \gg 0 \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha)=m}} \deg(\mathscr{E}'_\alpha),$$

with $\deg(\mathscr{T}_m)$ and $\deg(\mathscr{E}'_\alpha)$ defined just as in (1.1.1). We will prove later (in the appendix) that

$$\deg(\mathscr{T}_m) = I(T_m \mathscr{C}_1, \mathscr{C}_2), \tag{1.1.2}$$

so the main result of [14] really is a refinement of the Gross-Zagier formula. Actually, the stacks considered in [14] are all over $\mathbb{Z}$ and the Lie algebra condition in the definition of $\mathscr{C}_i$ is omitted. We will next review these spaces as defined in [14] and later explain the connection with the spaces $\mathscr{E}'_\alpha$ in the above decomposition.

Let $\mathscr{E}$ be the algebraic stack over $\mathrm{Spec}(\mathbb{Z})$ with fiber $\mathscr{E}(S)$ the category of pairs $(\mathbf{E}_1, \mathbf{E}_2)$ where $\mathbf{E}_i = (E_i, \kappa_i)$ with E_i an elliptic curve over the scheme S and $\kappa_i : \mathcal{O}_{K_i} \to \mathrm{End}_S(E_i)$ a ring homomorphism. Let $(\mathbf{E}_1, \mathbf{E}_2)$ be an object of $\mathscr{E}(S)$. The maximal order $\mathcal{O}_K = \mathcal{O}_{K_1} \otimes_{\mathbb{Z}} \mathcal{O}_{K_2}$ acts on the $\mathbb{Z}$-module $L(\mathbf{E}_1, \mathbf{E}_2) = \mathrm{Hom}_S(E_1, E_2)$ by

$$(t_1 \otimes t_2) \bullet f = \kappa_2(t_2) \circ f \circ \kappa_1(\bar{t}_1),$$

where $x \mapsto \overline{x}$ is the nontrivial element of $\mathrm{Gal}(K/F)$, so $L(\mathbf{E}_1, \mathbf{E}_2)$ is an $\mathcal{O}_K$-module. Writing $[\cdot\,,\cdot]$ for the bilinear form on $L(\mathbf{E}_1, \mathbf{E}_2)$ associated with the quadratic form deg, there is a unique $\mathcal{O}_F$-bilinear form

$$[\cdot\,,\cdot]_{\mathrm{CM}} : L(\mathbf{E}_1, \mathbf{E}_2) \times L(\mathbf{E}_1, \mathbf{E}_2) \to \mathfrak{D}^{-1}$$

satisfying $[f_1, f_2] = \mathrm{Tr}_{F/\mathbb{Q}}[f_1, f_2]_{\mathrm{CM}}$. Let $\deg_{\mathrm{CM}}$ be the totally positive definite F-quadratic form on $L(\mathbf{E}_1, \mathbf{E}_2) \otimes_{\mathbb{Z}} \mathbb{Q}$ corresponding to $[\cdot\,,\cdot]_{\mathrm{CM}}$, so $\deg(f) = \mathrm{Tr}_{F/\mathbb{Q}} \deg_{\mathrm{CM}}(f)$.

For any $\alpha \in F^\times$ let $\mathscr{E}_\alpha$ be the algebraic stack over $\mathrm{Spec}(\mathbb{Z})$ with $\mathscr{E}_\alpha(S)$ the category of triples $(\mathbf{E}_1, \mathbf{E}_2, f)$ where $(\mathbf{E}_1, \mathbf{E}_2)$ is an object of $\mathscr{E}(S)$ and $f \in L(\mathbf{E}_1, \mathbf{E}_2)$ satisfies $\deg_{\mathrm{CM}}(f) = \alpha$ on every connected component of S. The category $\mathscr{E}_\alpha$ is empty unless α is totally positive and lies in $\mathfrak{D}^{-1}$. Define the *arithmetic degree* of $\mathscr{E}_\alpha$ to be

$$\deg(\mathscr{E}_\alpha) = \sum_p \log(p) \sum_{x \in [\mathscr{E}_\alpha(\overline{\mathbb{F}}_p)]} \frac{\mathrm{length}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{E}_\alpha, x})}{|\,\mathrm{Aut}(x)|}.$$

Let χ be the quadratic Hecke character associated with the extension K/F and for $\alpha \in F^\times$ define $\mathrm{Diff}(\alpha)$ to be the set of prime ideals $\mathfrak{p} \subset \mathcal{O}_F$ satisfying $\chi_{\mathfrak{p}}(\alpha\mathfrak{D}) = -1$. The set $\mathrm{Diff}(\alpha)$ is finite and nonempty. For any fractional $\mathcal{O}_F$-ideal $\mathfrak{b}$ let $\rho(\mathfrak{b})$ be the number of ideals $\mathfrak{B} \subset \mathcal{O}_K$ satisfying $\mathrm{N}_{K/F}(\mathfrak{B}) = \mathfrak{b}$, where $\mathrm{N}_{K/F}$ is the ideal norm from K to F. For any prime number ℓ let $\rho_\ell(\mathfrak{b})$ be the number of ideals $\mathfrak{B} \subset \mathcal{O}_{K,\ell} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ satisfying $\mathrm{N}_{K_\ell/F_\ell}(\mathfrak{B}) = \mathfrak{b}\mathcal{O}_{K,\ell}$, so there is a product formula

$$\rho(\mathfrak{b}) = \prod_\ell \rho_\ell(\mathfrak{b}).$$

The following theorem, which is [14, Theorem A], is the main result we will generalize in the first part of this work.

Theorem 1 (Howard-Yang)**.** *Suppose $\alpha \in F^\times$ is totally positive. If $\alpha \in \mathfrak{D}^{-1}$ and* $\mathrm{Diff}(\alpha) = \{\mathfrak{p}\}$ *then $\mathscr{E}_\alpha$ is of dimension zero, is supported in characteristic p (the rational prime below $\mathfrak{p}$), and satisfies*

$$\deg(\mathscr{E}_\alpha) = \frac{1}{2}\log(p) \cdot \mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{p}\mathfrak{D}) \cdot \rho(\alpha\mathfrak{p}^{-1}\mathfrak{D}).$$

If $\alpha \notin \mathfrak{D}^{-1}$ or if $\#\,\mathrm{Diff}(\alpha) > 1$, then $\deg(\mathscr{E}_\alpha) = 0$.

The stack $\mathscr{E}_\alpha$ being of dimension zero means the local rings $\mathscr{O}^{\mathrm{sh}}_{\mathscr{E}_\alpha, x}$ are all of dimension zero, and $\mathscr{E}_\alpha$ being supported in characteristic p means it only has geometric points in characteristic p (if any at all).

1.2 False elliptic curves

Our work in generalizing Theorem 1 goes as follows. Let B be an indefinite quaternion algebra over $\mathbb{Q}$, let $\mathcal{O}_B$ be a maximal order of B, and let d_B be the discriminant of B. A *false elliptic curve* over a scheme S is a pair (A, i) where $A \to S$ is an abelian scheme of relative dimension 2 and $i : \mathcal{O}_B \to \mathrm{End}_S(A)$ is a ring homomorphism. Any false elliptic curve A comes equipped with a principal polarization $\lambda : A \to A^\vee$ uniquely determined by a condition described below. If A_1 and A_2 are false elliptic curves over a connected scheme S with corresponding principal polarizations λ_1 and λ_2, then the map

$$f \mapsto \lambda_1^{-1} \circ f^\vee \circ \lambda_2 \circ f : \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \to \mathrm{End}_{\mathcal{O}_B}(A_1)$$

has image in $\mathbb{Z} \subset \mathrm{End}_{\mathcal{O}_B}(A_1)$ and defines a positive definite quadratic form, called the *false degree* and denoted $\deg^*$.

We retain the same number theoretic setup of K_1, K_2, F, and K as above. We also assume each prime dividing d_B is inert in K_1 and K_2, so in particular, K_1 and K_2 split B. Let S be an $\mathcal{O}_K$-scheme. A *false elliptic curve over S with complex multiplication by $\mathcal{O}_{K_j}$*, for $j \in \{1, 2\}$, is a triple $\mathbf{A} = (A, i, \kappa)$ where (A, i) is a false elliptic curve over S and $\kappa : \mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B}(A)$ is a ring homomorphism such that the induced map $\mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B}(\mathrm{Lie}(A))$ is through the structure map $\mathcal{O}_{K_j} \hookrightarrow \mathcal{O}_K \to \mathscr{O}_S(S)$. Let $\mathfrak{m}_B \subset \mathcal{O}_B$ be the unique lattice (which is also an ideal) satisfying $\mathfrak{m}_B \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathcal{O}_{B,p} = \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for all $p \nmid d_B$ and $\mathfrak{m}_B \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathfrak{n}_p$ for all $p \mid d_B$, where $\mathfrak{n}_p \subset \mathcal{O}_{B,p}$ is the unique maximal ideal. Equivalently, $\mathfrak{m}_B \subset \mathcal{O}_B$ is the unique ideal of index d_B^2. Then $\mathcal{O}_B/\mathfrak{m}_B \cong \prod_{p \mid d_B} \mathbb{F}_{p^2}$.

Let $\mathscr{M}^B$ be the category fibered in groupoids over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{M}^B(S)$ the category whose objects are false elliptic curves (A, i) over the $\mathcal{O}_K$-scheme S satisfying the following condition for any $x \in \mathcal{O}_B$: any point of S has an affine open neighborhood $\mathrm{Spec}(R) \to S$ such that $\mathrm{Lie}(A_{/R})$ is a free R-module of rank 2 and there is an equality of polynomials in $R[T]$

$$\mathrm{char}(i(x), \mathrm{Lie}(A_{/R})) = (T - x)(T - x^\iota), \tag{1.2.1}$$

where $x \mapsto x^\iota$ is the main involution on B. The category $\mathscr{M}^B$ is an algebraic stack which is regular and flat of relative dimension 1 over $\mathrm{Spec}(\mathcal{O}_K)$, smooth over $\mathrm{Spec}(\mathcal{O}_K[d_B^{-1}])$ (if B is a division algebra, $\mathscr{M}^B$ is proper over $\mathrm{Spec}(\mathcal{O}_K)$). This 2-dimensional stack $\mathscr{M}^B$ is usually referred to as (the integral model of) a "Shimura curve". For $j \in \{1, 2\}$ let $\mathscr{Y}_j$ be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{Y}_j(S)$ the category of false elliptic curves over the $\mathcal{O}_K$-scheme S with complex multiplication by $\mathcal{O}_{K_j}$. The stack $\mathscr{Y}_j$ is finite and étale over $\mathrm{Spec}(\mathcal{O}_K)$, so in particular it is 1-dimensional and regular. Any object of $\mathscr{Y}_j(S)$ automatically satisfies condition (1.2.1) (see Corollary 5.2.8 below). Therefore there is a finite morphism $\mathscr{Y}_j \to \mathscr{M}^B$ defined by forgetting the complex multiplication structure.

Our main goal is to calculate the intersection multiplicity of the two divisors $T_m\mathscr{Y}_1$ and $\mathscr{Y}_2$ on $\mathscr{M}^B$, defined just as in (1.1.1), where T_m is the m-th Hecke correspondence on $\mathscr{M}^B$. For each positive integer m define $\mathscr{T}^B_m$ to be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{T}^B_m(S)$ the category of triples $(\mathbf{A}_1, \mathbf{A}_2, f)$ with $\mathbf{A}_j$ an object of $\mathscr{Y}_j(S)$ and $f \in \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2)$ satisfying $\deg^*(f) = m$ on every connected component of S. We will show there is a decomposition

$$\mathscr{T}^B_m = \bigsqcup_{\substack{\alpha\in F^\times \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha)=m}} \bigsqcup_{\theta:\mathcal{O}_K\to\mathcal{O}_B/\mathfrak{m}_B} \mathscr{X}_{\theta,\alpha}$$

for some 0-dimensional stacks $\mathscr{X}_{\theta,\alpha} \to \mathrm{Spec}(\mathcal{O}_K)$, where the inner union is over all ring homomorphisms $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$, so then

$$\deg(\mathscr{T}^B_m) = \sum_{\substack{\alpha\in\mathfrak{D}^{-1},\alpha\gg 0 \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha)=m}} \sum_{\theta:\mathcal{O}_K\to\mathcal{O}_B/\mathfrak{m}_B} \deg(\mathscr{X}_{\theta,\alpha}).$$

Just as in the elliptic curve case we will show

$$\deg(\mathscr{T}^B_m) = I(T_m\mathscr{Y}_1, \mathscr{Y}_2). \tag{1.2.2}$$

Our main result is then a formula for $\deg(\mathscr{X}_{\theta,\alpha})$.

A *CM pair* over an $\mathcal{O}_K$-scheme S is a pair $(\mathbf{A}_1, \mathbf{A}_2)$ where $\mathbf{A}_1$ and $\mathbf{A}_2$ are false elliptic curves over S with complex multiplication by $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$, respectively. For such a pair, set

$$L(\mathbf{A}_1, \mathbf{A}_2) = \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2).$$

As before, there is a unique $\mathcal{O}_F$-quadratic form

$$\deg_{\mathrm{CM}} : L(\mathbf{A}_1, \mathbf{A}_2) \to \mathfrak{D}^{-1}$$

satisfying $\mathrm{Tr}_{F/\mathbb{Q}} \deg_{\mathrm{CM}}(f) = \deg^*(f)$. For any false elliptic curve A let $A[\mathfrak{m}_B]$ be its $\mathfrak{m}_B$-torsion, defined as a group scheme below. For any ring homomorphism $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ define $\mathscr{X}_\theta$ to be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_K)$ where $\mathscr{X}_\theta(S)$ is the category of CM pairs $(\mathbf{A}_1, \mathbf{A}_2)$ over the

$\mathcal{O}_K$-scheme S such that the diagram

$$\begin{tikzcd}
\mathcal{O}_{K_j} \arrow[rr] \arrow[dr, "\theta|_{\mathcal{O}_{K_j}}"'] & & \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(A_j[\mathfrak{m}_B]) \\
& \mathcal{O}_B/\mathfrak{m}_B \arrow[ur] &
\end{tikzcd}$$

commutes for $j = 1, 2$, where

$$\mathcal{O}_B/\mathfrak{m}_B \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(A_j[\mathfrak{m}_B])$$

is the map induced by the action of $\mathcal{O}_B$ on A_j. Note that this map makes sense as $\mathcal{O}_B/\mathfrak{m}_B$ is commutative. If $B = \mathrm{M}_2(\mathbb{Q})$ then $\mathfrak{m}_B = \mathcal{O}_B$, so any such θ is necessarily 0 (here $1 = 0$ in the zero ring $\mathcal{O}_B/\mathfrak{m}_B$), and $\mathscr{X}_\theta$ is the stack of all CM pairs over $\mathcal{O}_K$-schemes.

For any $\alpha \in F^\times$ define $\mathscr{X}_{\theta,\alpha}$ to be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{X}_{\theta,\alpha}(S)$ the category of triples $(\mathbf{A}_1, \mathbf{A}_2, f)$ where $(\mathbf{A}_1, \mathbf{A}_2)$ is an object of $\mathscr{X}_\theta(S)$ and $f \in L(\mathbf{A}_1, \mathbf{A}_2)$ satisfies $\deg_{\mathrm{CM}}(f) = \alpha$ on every connected component of S. Define the *arithmetic degree* of $\mathscr{X}_{\theta,\alpha}$ as in (1.1.1) and define a nonempty finite set of prime ideals

$$\mathrm{Diff}_\theta(\alpha) = \{\mathfrak{p} \subset \mathcal{O}_F : \chi_{\mathfrak{p}}(\alpha \mathfrak{a}_\theta \mathfrak{D}) = -1\},$$

where $\mathfrak{a}_\theta = \ker(\theta) \cap \mathcal{O}_F$. Note that $\mathfrak{a}_\theta = \mathcal{O}_F$ if $B = \mathrm{M}_2(\mathbb{Q})$. Our first main result is the following (Proposition 9.1.2 and Theorems 8.3.1 and 9.1.3 in the text).

Theorem 2. *Let $\alpha \in F^\times$ be totally positive and suppose $\alpha \in \mathfrak{D}^{-1}$. Let $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ be a ring homomorphism with $\mathfrak{a}_\theta = \ker(\theta) \cap \mathcal{O}_F$, suppose $\mathrm{Diff}_\theta(\alpha) = \{\mathfrak{p}\}$, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathcal{O}_F$.*
(a) *The stack $\mathscr{X}_{\theta,\alpha}$ is of dimension zero and is supported in characteristic p.*
(b) *If $p \nmid d_B$ then*

$$\deg(\mathscr{X}_{\theta,\alpha}) = \frac{1}{2}\log(p) \cdot \mathrm{ord}_{\mathfrak{p}}(\alpha \mathfrak{p} \mathfrak{D}) \cdot \rho(\alpha \mathfrak{a}_\theta^{-1} \mathfrak{p}^{-1} \mathfrak{D}).$$

(c) *Suppose $p \mid d_B$ and let $\mathfrak{P} \subset \mathcal{O}_K$ be the unique prime over $\mathfrak{p}$. If $\mathfrak{P}$ divides* $\ker(\theta)$ *then*

$$\deg(\mathscr{X}_{\theta,\alpha}) = \frac{1}{2}\log(p) \cdot \mathrm{ord}_{\mathfrak{p}}(\alpha) \cdot \rho(\alpha \mathfrak{a}_\theta^{-1} \mathfrak{p}^{-1} \mathfrak{D}).$$

If $\mathfrak{P}$ does not divide $\ker(\theta)$ *then*

$$\deg(\mathscr{X}_{\theta,\alpha}) = \frac{1}{2}\log(p) \cdot \mathrm{ord}_{\mathfrak{p}}(\alpha \mathfrak{p}) \cdot \rho(\alpha \mathfrak{a}_\theta^{-1} \mathfrak{p}^{-1} \mathfrak{D}).$$

If $\alpha \notin \mathfrak{D}^{-1}$ or if $\#\,\mathrm{Diff}_\theta(\alpha) > 1$, then $\deg(\mathscr{X}_{\theta,\alpha}) = 0$.

The proof of this theorem consists of two general parts: counting the number of geometric points of the stack $\mathscr{X}_{\theta,\alpha}$ (Proposition 4.1.4 and Theorem 7.3.3) and calculating the length of the local ring $\mathscr{O}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}$ (Theorem 8.3.1). This theorem is a generalization of Theorem 1 in the following sense. Let $\mathfrak{P} \subset \mathcal{O}_K$ be a prime ideal, let $\alpha \in F^\times$ be totally positive, and set $\mathbb{F} = \overline{\mathbb{F}}_{\mathfrak{P}}$ for this discussion. Let p be the rational prime below $\mathfrak{P}$ and assume p is nonsplit in K_1 and K_2. Define $\mathscr{E}'_\alpha$ to be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{E}'_\alpha(S)$ the category of triples $(\mathbf{E}_1, \mathbf{E}_2, f)$ where $\mathbf{E}_j = (E_j, \kappa_j)$ is an elliptic curve over the $\mathcal{O}_K$-scheme S with an action $\kappa_j : \mathcal{O}_{K_j} \to \mathrm{End}_S(E_j)$ such that the induced map $\mathcal{O}_{K_j} \to \mathrm{End}_{\mathscr{O}_S}(\mathrm{Lie}(E_j)) \cong \mathscr{O}_S(S)$ is equal to the structure map, and $f \in L(\mathbf{E}_1, \mathbf{E}_2)$ satisfies $\deg_{\mathrm{CM}}(f) = \alpha$ on every connected component of S. The category $\mathscr{E}'_\alpha$ is the same as the category $\mathscr{E}_\alpha$ except for the condition on the Lie algebra. Now take $B = \mathrm{M}_2(\mathbb{Q})$ and $\mathcal{O}_B = \mathrm{M}_2(\mathbb{Z})$. In this case we claim any false elliptic curve A over $\mathbb{F}$ with CM by $\mathcal{O}_{K_j}$ is superspecial: $A \cong E^2 = E \times E$ for some supersingular elliptic curve E over $\mathbb{F}$ (note that any such A is necessarily supersingular as p is nonsplit in K_j (Lemma 3.2.6)). To see this, let α_p be the usual p-th roots of zero group scheme over $\mathbb{F}$. The $\mathbb{F}$-vector space $\mathrm{Hom}_{\mathbb{F}}(\alpha_p, A)$ is a module over $\mathrm{M}_2(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{F} \cong \mathrm{M}_2(\mathbb{F})$, so its $\mathbb{F}$-dimension $a(A)$ is even. The number $a(A)$ is known to be either 1 or 2, and equal to 2 if and only if A is superspecial ([21, Theorem 2, Remark 3]).

There is an equivalence of categories $\mathscr{E}'_\alpha(\mathbb{F}) \to \mathscr{X}_{\theta,\alpha}(\mathbb{F})$ given by

$$(\mathbf{E}_1, \mathbf{E}_2, f) \mapsto (\mathbf{A}_1, \mathbf{A}_2, f'),$$

where $\mathbf{A}_j = (A_j, i_j, \kappa'_j)$ with $A_j = E_j^2$, $i_j : \mathrm{M}_2(\mathbb{Z}) \to \mathrm{End}(A_j) \cong \mathrm{M}_2(\mathrm{End}(E_j))$ the natural inclusion, and $\kappa'_j = \mathrm{diag}(\kappa_j, \kappa_j)$. Similarly $f' = \mathrm{diag}(f, f)$. We have $\deg_{\mathrm{CM}}(f') = \alpha$ since $\deg^*(f') = \deg(f)$. It follows that if we define $\deg(\mathscr{E}'_\alpha)$ as in (1.1.1), then Theorem 2(b) shows that if $\alpha \in \mathfrak{D}^{-1}$ and $\mathrm{Diff}(\alpha) = \{\mathfrak{p}\}$, then

$$\deg(\mathscr{E}'_\alpha) = \frac{1}{2}\log(p) \cdot \mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{p}\mathfrak{D}) \cdot \rho(\alpha\mathfrak{p}^{-1}\mathfrak{D}).$$

This formula for $\deg(\mathscr{E}'_\alpha)$ agrees with the formula for $\deg(\mathscr{E}_\alpha)$ in Theorem 1 even though there is a slight difference in the definitions of $\mathscr{E}'_\alpha$ and $\mathscr{E}_\alpha$ because of the change in the definition of arithmetic degree between these two spaces (see [14, proof of Theorem 2.27]). In generalizing Theorem 1 we found it more natural to include this Lie algebra condition in the definition of the moduli problem, and it simplified the deformation theory used in calculating the lengths of the local rings of the stack.

1.3 Special endomorphisms

Next we will describe the second moduli problem considered in this thesis. Now let K be an imaginary quadratic field with discriminant d_K, let s be the number of distinct prime factors of d_K, and write $x \mapsto \overline{x}$ for the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$. Let e_p be the ramification index of $K/\mathbb{Q}$ at a prime p. Let $\mathscr{X}$ be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_K)$ with fiber $\mathscr{X}(S)$ the category of pairs (E, κ) where E is an elliptic curve over the $\mathcal{O}_K$-scheme S and $\kappa : \mathcal{O}_K \to \mathrm{End}_S(E)$ is an action such that the induced map $\mathcal{O}_K \to \mathrm{End}_{\mathscr{O}_S}(\mathrm{Lie}(E)) \cong \mathscr{O}_S(S)$ is the structure map. A *special endomorphism* of an object (E, κ) of $\mathscr{X}(S)$ is an endomorphism $f \in \mathrm{End}_S(E)$ satisfying

$$\kappa(x) \circ f = f \circ \kappa(\overline{x})$$

for all $x \in \mathcal{O}_K$. For any positive integer m let $\mathscr{X}^m$ be the algebraic stack over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{X}^m(S)$ the category of triples (E, κ, f) where (E, κ) is an object of $\mathscr{X}(S)$ and $f \in \mathrm{End}_S(E)$ is a special endomorphism satisfying $\deg(f) = m$ on every connected component of S. Define the *arithmetic degree* of $\mathscr{X}^m$ to be

$$\deg(\mathscr{X}^m) = \sum_{\mathfrak{p} \subset \mathcal{O}_K} \log(|\mathbb{F}_\mathfrak{p}|) \sum_{z \in [\mathscr{X}^m(\overline{\mathbb{F}}_\mathfrak{p})]} \mathrm{length}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{X}^m, z}), \tag{1.3.1}$$

where the outer sum is over all prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ and $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$.

For each $m \in \mathbb{Z}^+$ define a nonempty finite set of prime numbers

$$\mathrm{Diff}(m) = \{\ell < \infty : (d_K, -m)_\ell = -1\},$$

where $(\cdot, \cdot)_\ell$ is the usual Hilbert symbol. For any positive integer m let $R(m)$ be the number of ideals in $\mathcal{O}_K$ of norm m. For any prime ℓ let $R_\ell(m)$ be the number of ideals in $\mathcal{O}_{K,\ell} = \mathcal{O}_K \otimes_\mathbb{Z} \mathbb{Z}_\ell$ of norm $m\mathbb{Z}_\ell$, so there is a product formula

$$R(m) = \prod_\ell R_\ell(m).$$

The following is [16, Theorem 5.15] (at least a restatement of it, in the case where $-d_K$ is prime; the version stated here follows from our generalization below).

Theorem 3 (Kudla-Rapoport-Yang). *Let $m \in \mathbb{Z}^+$ and suppose $\mathrm{Diff}(m) = \{p\}$ for some prime p. Then the stack $\mathscr{X}^m$ is of dimension zero, it is supported in characteristic p, and*

$$\deg(\mathscr{X}^m) = 2^s \log(p) \cdot R(mp^{e_p - 2}) \cdot (\mathrm{ord}_p(m) + 1).$$

If $\#\operatorname{Diff}(m) > 1$ *then* $\deg(\mathscr{Z}^m) = 0$.

We continue with K an imaginary quadratic field, B an indefinite quaternion algebra over $\mathbb{Q}$, and $\mathcal{O}_B$ a maximal order of B. We assume each prime dividing d_B is inert in K. Let $\mathscr{Y}$ be the algebraic stack over $\operatorname{Spec}(\mathcal{O}_K)$ with $\mathscr{Y}(S)$ the category of false elliptic curves over the $\mathcal{O}_K$-scheme S with complex multiplication by $\mathcal{O}_K$. A *special endomorphism* of an object (A, κ) of $\mathscr{Y}(S)$ is an endomorphism $f \in \operatorname{End}_{\mathcal{O}_B}(A)$ satisfying

$$\kappa(x) \circ f = f \circ \kappa(\overline{x})$$

for all $x \in \mathcal{O}_K$. For any positive integer m let $\mathscr{Y}^m$ be the algebraic stack over $\operatorname{Spec}(\mathcal{O}_K)$ with $\mathscr{Y}^m(S)$ the category of triples (A, κ, f) where (A, κ) is an object of $\mathscr{Y}(S)$ and $f \in \operatorname{End}_{\mathcal{O}_B}(A)$ is a special endomorphism satisfying $\deg^*(f) = m$ on every connected component of S. Define the *arithmetic degree* of $\mathscr{Y}^m$ just as in (1.3.1). For each $m \in \mathbb{Z}^+$ define a nonempty finite set of prime numbers

$$\operatorname{Diff}_B(m) = \{\ell < \infty : (d_K, -m)_\ell \cdot \operatorname{inv}_\ell(B) = -1\},$$

where $\operatorname{inv}_\ell(B)$ is the local invariant of B at ℓ (it is -1 if B is ramified at ℓ and 1 otherwise). For any prime p set $\varepsilon_p = 1 - \operatorname{ord}_p(d_B)$ and let r be the number of primes dividing d_B. The following (Theorem 10.5.2 in the text) is our generalization of Theorem 3. The proof of this theorem is similar to that of Theorem 2 and is carried out in the final chapter of this thesis.

Theorem 4. *Let* $m \in \mathbb{Z}^+$ *and suppose* $\operatorname{Diff}_B(m) = \{p\}$. *The stack* $\mathscr{Y}^m$ *is of dimension zero, it is supported in characteristic* p, *and*

$$\deg(\mathscr{Y}^m) = 2^{r+s} \log(p) \cdot R(md_B^{-1} p^{(e_p-1)\varepsilon_p - 1}) \cdot (\operatorname{ord}_p(m) + \varepsilon_p).$$

If $\#\operatorname{Diff}_B(m) > 1$ *then* $\deg(\mathscr{Y}^m) = 0$.

1.4 Eisenstein series

Theorem 1 and Theorem 3 are really only half of a larger story, one that gives a better explanation of the definitions of the arithmetic degree of $\mathscr{E}_\alpha$ and $\mathscr{Z}^m$ and provides a surprising connection between arithmetic geometry and analysis. To explain this in the case of the moduli space $\mathscr{E}_\alpha$, let K_1, K_2, K, and F be as in Section 1.1, let $D = \operatorname{disc}(F)$, and let σ_1 and σ_2 be the two real embeddings of F.

For τ_1, τ_2 in the complex upper half plane and $s \in \mathbb{C}$ define an Eisenstein series

$$E^*(\tau_1, \tau_2, s) = D^{(s+1)/2}\left(\pi^{-(s+2)/2}\Gamma\left(\frac{s+2}{2}\right)\right)^2 \sum_{\mathfrak{a}\in \mathrm{Cl}(F)} \chi(\mathfrak{a})\mathrm{N}(\mathfrak{a})^{1+s}$$
$$\times \sum_{(0,0)\neq(m,n)\in\mathfrak{a}\times\mathfrak{a}/\mathcal{O}_F^\times} \frac{(v_1v_2)^{s/2}}{[m,n](\tau_1,\tau_2)|[m,n](\tau_1,\tau_2)|^s},$$

where $\mathrm{Cl}(F)$ is the ideal class group of F, $v_i = \mathrm{Im}(\tau_i)$, and

$$[m,n](\tau_1,\tau_2) = (\sigma_1(m)\tau_1 + \sigma_1(n))(\sigma_2(m)\tau_2 + \sigma_2(n)).$$

This series, which is convergent for $\mathrm{Re}(s) \gg 0$, has meromorphic continuation to all $s \in \mathbb{C}$ and defines a non-holomorphic Hilbert modular form of weight 1 for $\mathrm{SL}_2(\mathcal{O}_F)$ which is holomorphic in s in a neighborhood of $s = 0$. The derivative of $E^*(\tau_1, \tau_2, s)$ at $s = 0$ has a Fourier expansion

$$(E^*)'(\tau_1,\tau_2,0) = \sum_{\alpha\in\mathfrak{D}^{-1}} a_\alpha(v_1,v_2)\cdot q^\alpha,$$

where $e(x) = e^{2\pi i x}$ and $q^\alpha = e(\sigma_1(\alpha)\tau_1 + \sigma_2(\alpha)\tau_2)$. The connection between this analytic theory and the moduli space $\mathscr{E}_\alpha$ lies in the next theorem ([14, Theorem B, Theorem C]).

Theorem (Howard-Yang). *Suppose $\alpha \in F^\times$ is totally positive. If $\alpha \in \mathfrak{D}^{-1}$ then $a_\alpha = a_\alpha(v_1, v_2)$ is independent of v_1, v_2 and $a_\alpha = 4\cdot\deg(\mathscr{E}_\alpha)$.*

There is a similar theorem about $\mathscr{Z}^m$ which goes as follows. Let K be an imaginary quadratic field with discriminant d_K and assume $q = -d_K$ is prime. For each place $\ell \leqslant \infty$ of $\mathbb{Q}$ define a character $\psi_\ell : \mathbb{Q}_\ell^\times \to \{\pm1\}$ by $\psi_\ell(x) = (x, d_K)_\ell$ and for any

$$\gamma = \begin{bmatrix} a & b \\ c & d\end{bmatrix} \in \Gamma = \mathrm{SL}_2(\mathbb{Z})$$

define

$$\Phi^-(\gamma) = \begin{cases} \psi_q(a) & \text{if } q \mid c \\ -iq^{-1/2}\psi_q(c) & \text{if } q \nmid c.\end{cases}$$

For $\tau = u + iv$ in the complex upper half plane and $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ define

$$E^*(\tau, s) = v^{s/2}q^{(s+1)/2}\pi^{-(s+2)/2}\Gamma\left(\frac{s+2}{2}\right)L(s,\psi_q)\sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\frac{\Phi^-(\gamma)}{(c\tau+d)|c\tau+d|^s},$$

where $\Gamma_\infty = \{\gamma \in \Gamma : c = 0\}$. This series has meromorphic continuation to all $s \in \mathbb{C}$ and defines a non-holomorphic modular form of weight 1. It has a Fourier expansion

$$E^*(\tau, s) = \sum_{m \in \mathbb{Z}} a_m(v, s) \cdot e^{2\pi i m \tau}$$

for some functions $a_m(v, s)$ holomorphic in a neighborhood of $s = 0$. The following is [16, Theorem 3].

Theorem (Kudla-Rapoport-Yang)**.** *Let $m \in \mathbb{Z}^+$ and assume $-d_K$ is prime. The derivative $a'_m = a'_m(v, 0)$ is independent of v and* $\deg(\mathscr{Z}^m) = -a'_m$.

It seems likely that there are theorems in the spirit of the above two for the moduli spaces $\mathscr{X}_{\theta,\alpha}$ and $\mathscr{Y}^m$, but we do not pursue that direction here.

1.5 Notation and conventions

If X is an abelian variety or a p-divisible group over a field k, we write $\mathrm{End}(X)$ for $\mathrm{End}_k(X)$. If X is a scheme or a p-divisible group over $\mathrm{Spec}(R)$ for some ring R and $R \to R'$ is a ring homomorphism, we write $X \otimes_R R'$ for the fiber product $X \times_{\mathrm{Spec}(R)} \mathrm{Spec}(R')$. When we say "stack" we mean algebraic stack in the sense of [27], also called a Deligne-Mumford stack. We do not use stacks in a serious way in this work; they are merely a convenient language to use to make precise certain notions involving moduli spaces. If E is an elliptic curve over an algebraically closed field k, we write E^2 for the product $E \times E$, which, in the language of schemes, is really the fiber product $E \times_{\mathrm{Spec}(k)} E$. We write $\overline{\mathbb{F}}_p$ for an algebraic closure of the field of p elements. For any scheme S we write $\mathbf{Sch}/S$ for the category of S-schemes and we write **Sets** for the category of sets. By "scheme" we always mean locally Noetherian scheme. If $\mathscr{X}$ is a category, we write $X \in \mathscr{X}$ to mean X is an object of $\mathscr{X}$.

Chapter 2

False elliptic curves

In this chapter we review the basic theory of false elliptic curves. Although this material is "well-known", some of the proofs we provide do not seem to explicitly appear in the literature. For the remainder of this thesis fix an indefinite quaternion algebra B over $\mathbb{Q}$ and a maximal order $\mathcal{O}_B$ of B. We do not exclude the case where B is split, that is, where $B = \mathrm{M}_2(\mathbb{Q})$. As B is split at the infinite place ∞ of $\mathbb{Q}$, all maximal orders of B are conjugate by elements of $B^\times$. Let d_B be the discriminant of B.

2.1 Basic theory

Definition 2.1.1. Let S be a scheme. A *false elliptic curve* over S is a pair (A, i) where $A \to S$ is an abelian scheme of relative dimension 2 and $i : \mathcal{O}_B \hookrightarrow \mathrm{End}_S(A)$ is an injective ring homomorphism.

Definition 2.1.2. Let (A_1, i_1) and (A_2, i_2) be two false elliptic curves over a scheme S. A *homomorphism* $f : A_1 \to A_2$ of false elliptic curves is a homomorphism of abelian schemes over S satisfying $i_2(x) \circ f = f \circ i_1(x)$ for all $x \in \mathcal{O}_B$. If in addition f is an isogeny of abelian schemes, then f is called an *isogeny* of false elliptic curves.

We will see below that any nonzero homomorphism of false elliptic curves $A_1 \to A_2$ is necessarily an isogeny (which is false for a general homomorphism of abelian schemes $A_1 \to A_2$). We write $\mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2)$ for the $\mathbb{Z}$-module of homomorphisms of false elliptic curves $A_1 \to A_2$. For each place v of $\mathbb{Q}$ let $\mathrm{inv}_v : \mathrm{Br}_2(\mathbb{Q}_v) \to \{\pm 1\}$ be the unique isomorphism. If D is a quaternion algebra over $\mathbb{Q}$, we write $\mathrm{inv}_v(D)$ for $\mathrm{inv}_v(D \otimes_{\mathbb{Q}} \mathbb{Q}_v)$.

Definition 2.1.3. For each prime number p, define $B^{(p)}$ to be the quaternion algebra over $\mathbb{Q}$

determined by

$$\mathrm{inv}_v(B^{(p)}) = \begin{cases} \mathrm{inv}_v(B) & \text{if } v \notin \{p, \infty\} \\ -\mathrm{inv}_v(B) & \text{if } v \in \{p, \infty\}. \end{cases}$$

Note that $B^{(p)}$ is always a division algebra because it is ramified at ∞. In particular, if $B = \mathrm{M}_2(\mathbb{Q})$ then $B^{(p)}$ is the quaternion division algebra ramified at p and ∞.

Proposition 2.1.4. *Suppose (A, i) is a false elliptic curve over $\overline{\mathbb{F}}_p$. Then $\mathrm{End}^0_{\mathcal{O}_B}(A) = \mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is either*

(1) *an imaginary quadratic field L which admits an embedding $L \hookrightarrow B$, or*

(2) *the definite quaternion algebra $B^{(p)}$.*

Furthermore, A is isogenous to E^2 for some elliptic curve E over $\overline{\mathbb{F}}_p$, with E ordinary in case (1) *and supersingular in case* (2).

Our proof follows [18, Proposition 5.2].

Proof. Let $D = \mathrm{End}^0(A)$. Note that

$$\mathrm{End}^0_{\mathcal{O}_B}(A) = C_D(B) = \{d \in D : db = bd \text{ for all } b \in B\}$$

is the centralizer of B in D, via the embedding $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Q} = B \hookrightarrow D$. First suppose A is isogenous to $E_1 \times E_2$ for some elliptic curves E_1 and E_2 over $\overline{\mathbb{F}}_p$, with E_1 supersingular. Then $E_1 \sim E_2$ because otherwise there is a ring homomorphism

$$B \to \mathrm{End}^0(A) \cong \mathrm{End}^0(E_1) \times \mathrm{End}^0(E_2) \to \mathrm{End}^0(E_1),$$

which is injective since B is a simple $\mathbb{Q}$-algebra and thus the kernel, which is a two sided ideal of B, is zero (it is not the zero homomorphism as $1 \mapsto 1$). Then $\mathrm{End}^0(E_1) \cong B$ by counting $\mathbb{Q}$-dimensions, but $\mathrm{End}^0(E_1)$ is ramified at ∞ and B is not. Hence $A \sim E^2$ with E a supersingular elliptic curve, so $D_{p,\infty} = \mathrm{End}^0(E)$ is the quaternion division algebra over $\mathbb{Q}$ ramified at p and ∞, and $D = \mathrm{End}^0(A) \cong \mathrm{M}_2(D_{p,\infty})$. The center of D is $\mathbb{Q}$, so D is a central simple algebra over $\mathbb{Q}$. Let C be the centralizer of B in D. Since $B \subset D$ is a simple subalgebra, $\dim_{\mathbb{Q}} D = (\dim_{\mathbb{Q}} B)(\dim_{\mathbb{Q}} C)$ by the double centralizer theorem. It follows that the natural map $B \otimes_{\mathbb{Q}} C \to D$ defined by $b \otimes c \mapsto bc$ is an isomorphism of $\mathbb{Q}$-algebras, which means $[B][C] = [D] = [D_{p,\infty}]$ in $\mathrm{Br}(\mathbb{Q})$. Then $\mathrm{inv}_v(B)\,\mathrm{inv}_v(C) = \mathrm{inv}_v(D_{p,\infty})$ for all v, so from

$$\mathrm{inv}_v(D_{p,\infty}) = \begin{cases} 1 & \text{if } v \notin \{p, \infty\} \\ -1 & \text{if } v \in \{p, \infty\}, \end{cases}$$

we have $\mathrm{inv}_v(C) = \mathrm{inv}_v(B)$ for all $v \notin \{p, \infty\}$ and $\mathrm{inv}_v(C) = -\mathrm{inv}_v(B)$ for $v \in \{p, \infty\}$.

Now suppose A is simple or isogenous to a square of an ordinary elliptic curve (A cannot be isogenous to a product of two non-isogenous ordinary elliptic curves for a reason similar to that above). Let $\mathbb{F}_q \subset \overline{\mathbb{F}}_p$ be a subfield such that A and all of its endomorphisms are defined over $\mathbb{F}_q$, and let π be the Frobenius endomorphism of $A/\mathbb{F}_q$. Let L be the center of the simple $\mathbb{Q}$-algebra $D = \mathrm{End}^0_{\mathbb{F}_q}(A)$, so L is a field. More specifically, $L = \mathbb{Q}[\pi]$ in either case and in addition $L = \mathrm{End}^0(E)$ when $A \sim E^2$ for some ordinary elliptic curve E. If L has a real embedding (necessarily when A is simple) then by the Honda-Tate theorem A is isogenous over a quadratic extension of $\mathbb{F}_q$ to E^2 where E is a supersingular elliptic curve, a contradiction. If A is simple then again the Honda-Tate theorem implies that $4 = 2\dim(A) = (\dim_L D)^{1/2}[L : \mathbb{Q}]$, so $[L : \mathbb{Q}] \leqslant 2$ because otherwise $D = L$ is commutative, contradicting $D \supset B$. Hence L is an imaginary quadratic field in either case.

Let C be the centralizer of B in D, so $C \supset L$. Also, let L' be the center of C, so $L' \supset L$. We claim that $C = L'$. Suppose $C \supsetneq L'$ and let $c \in C \smallsetminus L'$. Also, since B is not commutative, there is a $b \in B \smallsetminus C$. Then b and c commute, so the subalgebra $R \subset D$ generated by L', b, and c is commutative, and $\dim_{L'} R \geqslant 4$. Hence D contains a commutative $\mathbb{Q}$-subalgebra of dimension strictly larger than $4 = 2\dim(A)$, a contradiction since the maximal commutative $\mathbb{Q}$-subalgebra has dimension $2\dim(A)$. Thus $C = L'$. Now, if $c \in L' = Z(C)$ then c commutes with all elements of C, so $c \in C_D(C)$, the centralizer of C in D. However, $C_D(C) = B$ by the double centralizer theorem (D is a central simple algebra over L and $B \subset D$ is a simple subalgebra). It follows that $L \subset L' \subset B$. But B is a central simple algebra of dimension 4 over $\mathbb{Q}$, so the maximal subfield of B has degree 2 over $\mathbb{Q}$, which means $L' = L$. Therefore $C = L$ is an imaginary quadratic field and $L \hookrightarrow B$.

Finally, since $\dim_L D = (\dim_L B)(\dim_L C) = 2$ by the double centralizer theorem, A is not simple because otherwise the Honda-Tate theorem implies $\dim_L D = 4$. Therefore $A \sim E^2$ for some ordinary elliptic curve. □

Proposition 2.1.5. *If A is a false elliptic curve over $\mathbb{C}$ then either A is simple, in which case $\mathrm{End}^0(A) \cong B$, or $A \sim E^2$ for some elliptic curve E over $\mathbb{C}$, with, in the case of B a division algebra, complex multiplication by an imaginary quadratic field which splits B.*

The proof is taken from [6, Proposition 52]

Proof. Suppose A is simple, so $D = \mathrm{End}^0(A)$ is a division algebra. Write $A(\mathbb{C}) = \mathbb{C}^2/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}^2$. Then there is a ring homomorphism $D \to \mathrm{End}_{\mathbb{Q}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{Q})$ (the rational representation), so $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ is a free D-module, since D is a division algebra. Hence $4 = \dim_{\mathbb{Q}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}) = \mathrm{rank}_D(\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}) \dim_{\mathbb{Q}}(D)$, so $\dim_{\mathbb{Q}} D \leqslant 4$. However, $B \hookrightarrow D$, which means $D \cong B$ by counting $\mathbb{Q}$-dimensions.

Now suppose $A \sim E_1 \times E_2$ for some elliptic curves E_1 and E_2 over $\mathbb{C}$. If E_1 is not isogenous to

E_2 then there is an injective ring homomorphism

$$B \to \mathrm{End}^0(A) \cong \mathrm{End}^0(E_1) \times \mathrm{End}^0(E_2) \to \mathrm{End}^0(E_1),$$

a contradiction because E_1 is an elliptic curve over $\mathbb{C}$. Hence $A \sim E^2$ for some elliptic curve E, so $D = \mathrm{End}^0(A) \cong \mathrm{M}_2(\mathrm{End}^0(E))$. If B is a division algebra and $\mathrm{End}^0(E) = \mathbb{Q}$, then $B \hookrightarrow \mathrm{M}_2(\mathbb{Q})$, a contradiction. Therefore E is an elliptic curve over $\mathbb{C}$ with complex multiplication by some imaginary quadratic field L, and thus $D \cong \mathrm{M}_2(L)$.

Finally, to show L splits B, note that since $B \hookrightarrow \mathrm{M}_2(L)$, B acts on an L-vector space V of dimension 2. Then V is a free B-module of rank 1, so $V \cong B$ as B-modules, which means B is an L-vector space of dimension 2. Hence L is the maximal subfield of B containing $\mathbb{Q}$ and therefore $L \otimes_{\mathbb{Q}} B \cong \mathrm{M}_2(L)$. □

Proposition 2.1.6. *If A is a false elliptic curve over $\mathbb{C}$ then $\mathrm{End}^0_{\mathcal{O}_B}(A)$ is either $\mathbb{Q}$ or an imaginary quadratic field which splits B.*

Proof. As above, $\mathrm{End}^0_{\mathcal{O}_B}(A) = C_D(B)$, the centralizer of B in $D = \mathrm{End}^0(A)$, via the embedding $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Q} = B \hookrightarrow D$. If A is simple then $D \cong B$, so $\mathrm{End}^0_{\mathcal{O}_B}(A) = C_B(B) = Z(B) = \mathbb{Q}$. Now suppose $A \sim E^2$ for some elliptic curve E. If E does not have complex multiplication then necessarily $B = D = \mathrm{M}_2(\mathbb{Q})$ and thus $\mathrm{End}^0_{\mathcal{O}_B}(A) = C_D(B) = Z(B) = \mathbb{Q}$. If E has complex multiplication then $D \cong \mathrm{M}_2(L)$ for some imaginary quadratic field L satisfying $L \otimes_{\mathbb{Q}} B \cong \mathrm{M}_2(L)$ (clearly this is still true when $B = \mathrm{M}_2(\mathbb{Q})$). Hence

$$\mathrm{End}^0_{\mathcal{O}_B}(A) = C_D(B) \cong C_{L\otimes_{\mathbb{Q}}B}(\mathbb{Q} \otimes_{\mathbb{Q}} B) \cong C_L(\mathbb{Q}) \otimes_{\mathbb{Q}} C_B(B) = L \otimes_{\mathbb{Q}} \mathbb{Q} = L. \qquad \square$$

Often we can reduce the proof of a statement about false elliptic curves over an arbitrary base scheme to the case of false elliptic curves defined over an algebraically closed field by using the following general result.

Lemma 2.1.7. *Let $\mathscr{A} \to S$ be an abelian scheme and $\overline{s} : \mathrm{Spec}(k) \to S$ a geometric point of S. The natural map $\mathrm{End}_S(\mathscr{A}) \to \mathrm{End}_k(\mathscr{A}_{\overline{s}})$, where $\mathscr{A}_{\overline{s}} = \mathscr{A} \times_S \mathrm{Spec}(k)$ is the geometric fiber, is injective.*

Proof. See [20, Corollary 6.2]. □

Proposition 2.1.8. *Suppose A is a false elliptic curve over a field extension L of $\overline{\mathbb{F}}_p$. Then $\mathrm{End}(A)$ embeds into $\mathrm{End}(A')$ for some false elliptic curve A' defined over a finite extension of $\mathbb{F}_p$. In particular, $\mathrm{End}^0_{\mathcal{O}_B}(A)$ embeds into an imaginary quadratic field or the definite quaternion algebra $B^{(p)}$.*

Proof. First note that we may descend to the case of A defined over a field L having finite transcendence degree over $\overline{\mathbb{F}}_p$. Now we will use induction on the transcendence degree of L over $\overline{\mathbb{F}}_p$. The result is trivial if L has transcendence degree 0 over $\overline{\mathbb{F}}_p$, so assume the result holds for any false elliptic curve defined over any field L' with a fixed transcendence degree over $\overline{\mathbb{F}}_p$, and suppose A is a false elliptic curve defined over a field L with transcendence degree 1 over L'. Then L is an algebraic extension of $L'(x)$ for some $x \in L$ transcendental over L'. As before we may descend to the case of L finite over $L'(x)$. Let $\mathcal{O}_L$ be the integral closure of $L'[x]$ in L, and fix a prime $\mathfrak{p} \subset \mathcal{O}_L$ of good reduction for A. This means that there is an abelian scheme $\mathscr{A}$ over $\operatorname{Spec}(\mathcal{O}_{L,\mathfrak{p}})$ whose generic fiber is A, that is,

$$\mathscr{A} \otimes_{\mathcal{O}_{L,\mathfrak{p}}} \operatorname{Frac}(\mathcal{O}_{L,\mathfrak{p}}) \cong A.$$

Since $\mathscr{A}$ is an abelian scheme, it is the Néron model of its generic fiber A ([1, Corollary 1.4]), so $\operatorname{End}(A) \cong \operatorname{End}_{\mathcal{O}_{L,\mathfrak{p}}}(\mathscr{A})$ by the universal property of the Néron model. Now let

$$\widetilde{A} = \mathscr{A} \otimes_{\mathcal{O}_{L,\mathfrak{p}}} \widetilde{L}$$

be the reduction of $\mathscr{A}$ modulo $\mathfrak{p}$, where $\widetilde{L} = \mathcal{O}_L/\mathfrak{p}$. By [7, Theorem 2.1(2)] the natural map $\operatorname{End}_{\mathcal{O}_{L,\mathfrak{p}}}(\mathscr{A}) \to \operatorname{End}(\widetilde{A})$ is injective. Since $\widetilde{L}$ is a finite extension of L', we have an inclusion $\operatorname{End}(A) \hookrightarrow \operatorname{End}(\widetilde{A})$ with $\widetilde{A}$ a false elliptic curve defined over a field with transcendence degree one less than L, the field A is defined over, so we are done by induction. □

Lemma 2.1.9. *Let (A_1, i_1) and (A_2, i_2) be false elliptic curves over an algebraically closed field k and suppose A_1 and A_2 are isogenous as abelian varieties. Then A_1 and A_2 are isogenous as false elliptic curves.*

This argument is taken from [18, p. 179].

Proof. By Propositions 2.1.4, 2.1.5, and 2.1.8, the ring $\operatorname{End}^0(A_2)$ is a central simple algebra over either $\mathbb{Q}$ or an imaginary quadratic field L which embeds into B, with one possible exception: the field k has positive transcendence degree over $\overline{\mathbb{F}}_p$ for some prime p, A_2 is simple, and $D = \operatorname{End}^0(A_2) \hookrightarrow \mathrm{M}_2(D_{p,\infty})$ is a quaternion division algebra over a quadratic extension L of $\mathbb{Q}$ (not necessarily imaginary; by counting dimensions this forces $D \cong B \otimes_{\mathbb{Q}} L$ and thus L does not embed in B). Let $f : A_1 \to A_2$ be an isogeny of abelian varieties and let $f_* : \operatorname{End}^0(A_1) \to \operatorname{End}^0(A_2)$ be the corresponding homomorphism of $\mathbb{Q}$-algebras defined by $f_*(\varphi) = f \circ \varphi \circ f^{-1}$, where $f^{-1} : A_2 \to A_1$ is the inverse of f in $\operatorname{Hom}^0(A_2, A_1)$. Then we have the ring homomorphisms $i_2 : B \to \operatorname{End}^0(A_2)$ and $f_* \circ i_1 : B \to \operatorname{End}^0(A_2)$, so by the Noether-Skolem theorem there is a $u \in \operatorname{End}^0(A_2)^\times$ such that

$$i_2(x) = u \circ (f_*(i_1(x))) \circ u^{-1} = u \circ f \circ i_1(x) \circ f^{-1} \circ u^{-1}$$

for all $x \in B$. Hence $i_2(x) \circ u \circ f = u \circ f \circ i_1(x)$, so the map $mu \circ f : A_1 \to A_2$ is an isogeny of false elliptic curves, where m is an integer such that $mu \in \mathrm{End}(A_2)$. □

Lemma 2.1.10. *Let (A, i) be a false elliptic curve over a scheme S and assume B is a division algebra. If $x \in \mathcal{O}_B$ is nonzero then $i(x) \in \mathrm{End}_S(A)$ is an isogeny of degree $\mathrm{Nrd}(x)^2$, where $\mathrm{Nrd} : B^\times \to \mathbb{Q}^\times$ is the reduced norm.*

Proof. As x is nonzero there is a $y \in B^\times$ such that $xy = yx = 1$ and thus $i(x) \circ i(y) = i(y) \circ i(x) = \mathrm{id}$ in $\mathrm{End}^0_S(A)$. This shows $i(x)$ is an isogeny. To compute its degree we may assume $S = \mathrm{Spec}(k)$ for k an algebraically closed field. Applying the Noether-Skolem theorem as in Lemma 2.1.9 to the two maps $B \to \mathrm{End}^0(A)$ given by $b \mapsto i(b)$ and $b \mapsto i(b^\iota)$, where $b \mapsto b^\iota$ is the main involution on B, we find that there is an $u \in \mathrm{End}^0(A)^\times$ such that $i(b) = u \circ i(b^\iota) \circ u^{-1}$ for all $b \in B$. Hence $\deg(i(x)) = \deg(i(x^\iota))$ and

$$\deg(i(x))^2 = \deg(i(x)) \deg(i(x^\iota)) = \deg(i(xx^\iota)) = \deg([\mathrm{Nrd}(x)]) = \mathrm{Nrd}(x)^4.$$

Since $\deg(i(x))$ is a positive integer, $\deg(i(x)) = \mathrm{Nrd}(x)^2$. □

The following result is needed below in defining the false degree.

Lemma 2.1.11. *Positive involutions on rational division algebras are classified as follows.*
(a) *Suppose D is a quaternion division algebra over $\mathbb{Q}$ and $x \mapsto x'$ is a positive involution on D trivial on $Z(D) = \mathbb{Q}$. If D is indefinite then $x \mapsto x'$ is given by $x' = a^{-1}x^\iota a$ for some $a \in D$ with $a^2 \in \mathbb{Q}$ negative, where $x \mapsto x^\iota$ is the main involution. If D is definite then $x \mapsto x'$ is the main involution.*
(b) *Suppose D is a division algebra over $\mathbb{Q}$ of finite dimension with a positive involution not trivial on $Z(D)$. Then $L = Z(D)$ is totally complex and the restriction of the involution to L is complex conjugation. In particular, the only nontrivial positive involution on an imaginary quadratic field is complex conjugation.*

Proof. For (a) see [2, Theorem 5.5.3] and for (b) see [2, Lemma 5.5.4]. □

Let $x \mapsto x^\iota$ be the main involution of B and fix $a \in \mathcal{O}_B$ satisfying $a^2 = -d_B$ (such an a exists since $\mathbb{Q}(\sqrt{-d_B})$ splits B). Define another involution on B by $x \mapsto x^* = a^{-1}x^\iota a$. The order $\mathcal{O}_B$ is stable under $x \mapsto x^*$.

If (A, i) is a false elliptic curve over S, then so is the dual abelian scheme $A^\vee$, with corresponding homomorphism $i^\vee : \mathcal{O}_B \hookrightarrow \mathrm{End}_S(A^\vee)$ defined by $i^\vee(x) = i(x)^\vee$ for all $x \in \mathcal{O}_B$. If $f : (A_1, i_1) \to (A_2, i_2)$ is a homomorphism of false elliptic curves, then $f^\vee : A_2^\vee \to A_1^\vee$ is also a homomorphism of false elliptic curves since

$$i_1^\vee(x) \circ f^\vee = i_1(x)^\vee \circ f^\vee = (f \circ i_1(x))^\vee = (i_2(x) \circ f)^\vee = f^\vee \circ i_2(x)^\vee = f^\vee \circ i_2^\vee(x)$$

for all $x \in \mathcal{O}_B$.

Proposition 2.1.12. *Let A be a false elliptic curve over a scheme S. There is a unique principal polarization $\lambda : A \to A^\vee$ such that if $\overline{s}$ is a geometric point of S, then the corresponding Rosati involution $\varphi \mapsto \varphi^\dagger = \lambda_{\overline{s}}^{-1} \circ \varphi^\vee \circ \lambda_{\overline{s}}$ on $\mathrm{End}^0(A_{\overline{s}})$ induces the involution $x \mapsto x^*$ on $\mathcal{O}_B \subset \mathrm{End}(A_{\overline{s}})$.*

Proof. See [4, p. 3] and [3, Proposition III.3.3]. □

The last condition in the proposition means that if $i : \mathcal{O}_B \to \mathrm{End}(A)$ is the $\mathcal{O}_B$-action, then $\lambda_{\overline{s}}^{-1} \circ i(x)^\vee \circ \lambda_{\overline{s}} = i(x^*)$ for all $x \in \mathcal{O}_B$.

Let (A_1, i_1) and (A_2, i_2) be false elliptic curves over S with corresponding principal polarizations $\lambda_1 : A_1 \to A_1^\vee$ and $\lambda_2 : A_2 \to A_2^\vee$. Suppose $f : A_1 \to A_2$ is an isogeny of false elliptic curves. Then f induces an isogeny $f^\vee : A_2^\vee \to A_1^\vee$ of false elliptic curves. Using the principal polarizations λ_1 and λ_2, we obtain a map $f^t : A_2 \to A_1$ defined as the composition

$$f^t = \lambda_1^{-1} \circ f^\vee \circ \lambda_2 : A_2 \to A_1.$$

This is an isogeny of abelian schemes and is $\mathcal{O}_B$-linear since $i_j(x) = \lambda_j^{-1} \circ i_j(x^*)^\vee \circ \lambda_j$ implies

$$\begin{aligned} f^t \circ i_2(x) &= \lambda_1^{-1} \circ f^\vee \circ \lambda_2 \circ \lambda_2^{-1} \circ i_2(x^*)^\vee \circ \lambda_2 \\ &= \lambda_1^{-1} \circ (i_2(x^*) \circ f)^\vee \circ \lambda_2 \\ &= \lambda_1^{-1} \circ (f \circ i_1(x^*))^\vee \circ \lambda_2 \\ &= \lambda_1^{-1} \circ i_1(x^*)^\vee \circ \lambda_1 \circ \lambda_1^{-1} \circ f^\vee \circ \lambda_2 \\ &= i_1(x) \circ f^t \end{aligned}$$

for all $x \in \mathcal{O}_B$ (it sufficed to check this on geometric fibers). The isogeny $f^t : A_2 \to A_1$ is called the *dual isogeny* to f.

Lemma 2.1.13. *The map $f \mapsto f^t$ satisfies the following properties.*
(a) *Suppose A_1 and A_2 are false elliptic curves and $f, g : A_1 \to A_2$ are isogenies. Then $(f^t)^t = f$ and $(f + g)^t = f^t + g^t$.*
(b) *Suppose A_1, A_2, and A_3 are false elliptic curves and $f : A_1 \to A_2$ and $g : A_2 \to A_3$ are isogenies. Then $(g \circ f)^t = f^t \circ g^t$.*

Proof. The first claim in (a) follows from $(f^\vee)^\vee = f$, once we make the identifications $(A_1^\vee)^\vee \cong A_1$ and $(A_2^\vee)^\vee \cong A_2$. The other claims follow immediately from $(f+g)^\vee = f^\vee + g^\vee$ and $(g \circ f)^\vee = f^\vee \circ g^\vee$. □

Proposition 2.1.14. *Let $f : A_1 \to A_2$ be an isogeny of false elliptic curves over a scheme S. The isogeny $f^t \circ f : A_1 \to A_1$ is locally on S multiplication by an integer.*

What this means is that any point of S has an affine open neighborhood U such that the map $f^t \circ f : A_1 \times_S U \to A_1 \times_S U$ is multiplication by an integer.

Proof. This can be checked on geometric fibers, so we may assume A_1 is a false elliptic curve over an algebraically closed field k. Viewing $f^t \circ f \in \mathrm{End}^0_{\mathcal{O}_B}(A_1)$, we will show $f^t \circ f$ is fixed by the Rosati involution and then show that the set of fixed points of the Rosati involution is $\mathbb{Q}$. First, to show $f^t \circ f \in \mathrm{End}^0_{\mathcal{O}_B}(A_1)$ is fixed by the Rosati involution corresponding to λ_1, compute

$$\begin{aligned}
(f^t \circ f)^\dagger &= \lambda_1^{-1} \circ (f^t \circ f)^\vee \circ \lambda_1 \\
&= \lambda_1^{-1} \circ (\lambda_1^{-1} \circ f^\vee \circ \lambda_2 \circ f)^\vee \circ \lambda_1 \\
&= \lambda_1^{-1} \circ f^\vee \circ \lambda_2^\vee \circ f \circ (\lambda_1^{-1})^\vee \circ \lambda_1 \\
&= \lambda_1^{-1} \circ f^\vee \circ \lambda_2 \circ f \\
&= f^t \circ f.
\end{aligned}$$

If k has positive transcendence degree over $\overline{\mathbb{F}}_p$ then $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$ embeds into an imaginary quadratic field or a definite quaternion algebra, so we are reduced to considering the following. Since k is algebraically closed, $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$ is one of (i) the quaternion algebra $B^{(p)}$ (when $k = \overline{\mathbb{F}}_p$), (ii) an imaginary quadratic field L (when k is $\overline{\mathbb{F}}_p$ or $\mathbb{C}$), or (iii) the field $\mathbb{Q}$ (when $k = \mathbb{C}$). The Rosati involution $\varphi \mapsto \varphi^\dagger$ is a positive involution on $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$. In case (i), we have $\mathrm{End}^0_{\mathcal{O}_B}(A_1) = B^{(p)}$ and the Rosati involution is trivial on $Z(B^{(p)}) = \mathbb{Q}$, so $x^\dagger = x^\iota$ is the main involution because $B^{(p)}$ is definite. The set of fixed points of the main involution is $\mathbb{Q}$. In case (ii), $\mathrm{End}^0_{\mathcal{O}_B}(A_1) = L$ and $x^\dagger = \overline{x}$ is complex conjugation, so the set of fixed points is $\mathbb{R} \cap L = \mathbb{Q}$. Therefore in each case $f^t \circ f \in \mathbb{Q}$, so $f^t \circ f : A_1 \to A_1$ is multiplication by an integer. □

Definition 2.1.15. If the integer in the previous proposition is constant on S, then it is called the *false degree* of f, and is denoted $\deg^*(f)$.

For any $f \in \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2)$ and $n \in \mathbb{Z}$, we have

$$\deg^*(nf) = \deg^*([n]_{A_2}) \deg^*(f) = n^2 \deg^*(f).$$

Using this we can extend the definition of $\deg^*$ to $\mathrm{Hom}^0_{\mathcal{O}_B}(A_1, A_2)$ by setting

$$\deg^*(g) = n^{-2}\deg^*(ng),$$

where n is any integer such that $ng \in \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2)$.

Corollary 2.1.16. *Let (A_1, i_1) and (A_2, i_2) be two false elliptic curves over a scheme S and suppose $f : A_1 \to A_2$ is an isogeny of false degree n. Then the map*

$$\Phi : \mathrm{End}^0_{\mathcal{O}_B}(A_1) \to \mathrm{End}^0_{\mathcal{O}_B}(A_2)$$

defined by $\Phi(\varphi) = n^{-1} f \circ \varphi \circ f^t$ is an isomorphism of $\mathbb{Q}$-algebras.

Here we are implicitly using that if f is an isogeny then $\deg^*(f) \neq 0$. We prove that below in Proposition 2.1.19.

Proof. First note that since $f^t \circ f = [n] : A_1 \to A_1$, we also have $f \circ f^t = [n] : A_2 \to A_2$. Indeed,

$$f^t \circ (f \circ f^t) = (f^t \circ f) \circ f^t = [n]_{A_1} \circ f^t = f^t \circ [n]_{A_2},$$

so $(f \circ f^t) - [n]_{A_2}$ maps A_2 to the finite group scheme $\ker(f^t)$ and thus $(f \circ f^t) - [n]_{A_2} = 0$. Now the corollary follows from observing that the map

$$\Psi : \mathrm{End}^0_{\mathcal{O}_B}(A_2) \to \mathrm{End}^0_{\mathcal{O}_B}(A_1)$$

defined by $\Psi(\psi) = n^{-1} f^t \circ \psi \circ f$ is the inverse of Φ. □

For any isogeny $f : A_1 \to A_2$ let $f^{-1} = f^t \otimes \deg^*(f)^{-1} \in \mathrm{Hom}^0_{\mathcal{O}_B}(A_2, A_1)$, so $f^{-1} \circ f = [1]_{A_1}$ in $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$ and $f \circ f^{-1} = [1]_{A_2}$ in $\mathrm{End}^0_{\mathcal{O}_B}(A_2)$.

Corollary 2.1.17. *Let A_1 and A_2 be false elliptic curves over a connected scheme S and suppose $f \in \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2)$ is an isogeny. Then $\deg^*(f^t) = \deg^*(f)$ and $\deg(f) = \deg^*(f)^2$.*

Proof. This can be checked on geometric fibers, so we may assume $S = \mathrm{Spec}(k)$ for k an algebraically closed field. Let $d = \deg^*(f)$. The first claim follows from $(f^t)^t = f$ and $f \circ f^t = [d]_{A_2}$. For the second claim, since $f^t \circ f = [d]_{A_1}$, we have

$$\deg(f^t)\deg(f) = d^4.$$

However, $\deg(f^t) = \deg(f^\vee) = \deg(f)$, so $\deg(f) = d^2$. □

Lemma 2.1.18. *Let A_1 and A_2 be false elliptic curves over a scheme S. Any nonzero element of $\mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2)$ is an isogeny.*

Proof. Assume $f \in \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2)$ is nonzero. To show f is an isogeny it suffices to check that the map on fibers f_s is an isogeny for all $s \in S$ ([5, 1.4.2.3]), and this further reduces to checking $f_{\overline{s}}$ is an isogeny for all geometric points $\overline{s}$ of S ([9, Remark 12.16]), so we may assume $S = \mathrm{Spec}(k)$ for k an algebraically closed field. By Propositions 2.1.4 and 2.1.5 we see that since $\mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \neq 0$, there is an isogeny of abelian varieties $A_1 \to A_2$ and thus an isogeny of false elliptic curves $A_1 \to A_2$ by Lemma 2.1.9. It follows that

$$\mathrm{Hom}^0_{\mathcal{O}_B}(A_1, A_2) \cong \mathrm{Hom}^0_{\mathcal{O}_B}(A_2, A_1)$$

has the structure of a division algebra and therefore each nonzero element is an isogeny. □

Proposition 2.1.19. *Let A_1 and A_2 be false elliptic curves over a connected scheme S. The map $\deg^* : \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \to \mathbb{Z}$ is a positive definite quadratic form.*

Proof. For $f, g \in \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2)$ let

$$[f, g] = \deg^*(f + g) - \deg^*(f) - \deg^*(g).$$

Using the injective ring homomorphism $[\,\cdot\,] : \mathbb{Z} \to \mathrm{End}_{\mathcal{O}_B}(A_1)$, we have

$$\begin{aligned}[][f, g]] &= [\deg^*(f + g)] - [\deg^*(f)] - [\deg^*(g)] \\ &= (f + g)^t \circ (f + g) - f^t \circ f - g^t \circ g \\ &= f^t \circ g + g^t \circ f.\end{aligned}$$

Since this expression is additive in f and g, and $[\,\cdot\,]$ is injective, $[\cdot, \cdot]$ is bilinear. Finally, $\deg^*(-f) = \deg^*(f)$, so $\deg^*$ is a quadratic form.

If $f = 0$ then clearly $\deg^*(f) = 0$, so suppose $f : A_1 \to A_2$ is an isogeny. To show $\deg^*(f) > 0$, it suffices to check this on geometric fibers, so we may assume A_1 and A_2 are false elliptic curves over an algebraically closed field k. Define an isogeny of abelian varieties

$$\Phi : A_1 \times A_2 \to A_1 \times A_2$$

by $\Phi(x, y) = (f^t(y), f(x))$ (on points in k-schemes). Using the isomorphism $(A_1 \times A_2)^\vee \cong A_1^\vee \times A_2^\vee$, consider the isogeny $\Phi^\vee : A_1^\vee \times A_2^\vee \to A_1^\vee \times A_2^\vee$. In general, if $\varphi : X \to Y$ is any homomorphism of abelian varieties, and $\mathscr{P}_X$ and $\mathscr{P}_Y$ are the Poincaré sheaves on $X \times X^\vee$ and $Y \times Y^\vee$, respectively, then $\varphi^\vee : Y^\vee \to X^\vee$ is the unique homomorphism such that

$$(\mathrm{id}_X \times \varphi^\vee)^* \mathscr{P}_X \cong (\varphi \times \mathrm{id}_{Y^\vee})^* \mathscr{P}_Y$$

as sheaves on $X \times Y^\vee$. Also, if

$$p : X \times Y \times X^\vee \times Y^\vee \to X \times X^\vee, \quad q : X \times Y \times X^\vee \times Y^\vee \to Y \times Y^\vee$$

are the projections, then $\mathscr{P}_{X\times Y} \cong p^*\mathscr{P}_X \otimes q^*\mathscr{P}_Y$. Using these two facts it is straightforward to check that $\Phi^\vee$ is given on points by $\Phi^\vee(u,v) = (f^\vee(v), (f^t)^\vee(u))$.

If $\lambda_j : A_j \to A_j^\vee$, $j = 1, 2$, are the usual principal polarizations, then we get a principal polarization

$$\lambda = \lambda_1 \times \lambda_2 : A_1^\vee \times A_2^\vee \to A_1^\vee \times A_2^\vee.$$

The corresponding Rosati involution on $\mathrm{End}^0(A_1 \times A_2)$ has the following effect on Φ:

$$\begin{aligned}
\Phi^\dagger(x,y) &= (\lambda^{-1} \circ \Phi^\vee \circ \lambda)(x,y) \\
&= (\lambda^{-1} \circ \Phi^\vee)(\lambda_1(x), \lambda_2(y)) \\
&= \lambda^{-1}\big(f^\vee(\lambda_2(y)), (f^t)^\vee(\lambda_1(x))\big) \\
&= \big((\lambda_1^{-1} \circ f^\vee \circ \lambda_2)(y), (\lambda_2^{-1} \circ (f^t)^\vee \circ \lambda_1)(x)\big) \\
&= (f^t(y), (f^t)^t(x)) \\
&= \Phi(x,y).
\end{aligned}$$

Hence $\Phi^\dagger = \Phi$, so

$$(\Phi \circ \Phi^\dagger)(x,y) = \Phi(f^t(y), f(x)) = ((f^t \circ f)(x), (f \circ f^t)(y)) = \deg^*(f) \cdot (x,y),$$

which shows $\Phi \circ \Phi^\dagger = [\deg^*(f)]$. Since the Rosati involution is positive and $\Phi \circ \Phi^\dagger \in \mathbb{Q}$, we have $\mathrm{Trd}(\Phi \circ \Phi^\dagger) = d \cdot \deg^*(f) > 0$, where Trd is the reduced trace on $\mathrm{End}^0(A_1 \times A_2)$ and $d = (\dim_L \mathrm{End}^0(A_1 \times A_2))^{1/2} > 0$ (L is the center of $\mathrm{End}^0(A_1 \times A_2)$). Therefore $\deg^*(f) > 0$. □

2.2 Quaternion algebras

We conclude this chapter with a brief discussion of quaternion algebras over local fields. Let L be a nonarchimedean local field of characteristic 0. Up to isomorphism there is a unique quaternion division algebra D over L. Any quadratic extension of L can be embedded into D and D contains a unique maximal order $\mathcal{O}_D$, with all orders of D contained in $\mathcal{O}_D$. The maximal order $\mathcal{O}_D$ is the set of all elements of D integral over the ring of integers of L. We will encounter these objects in two settings. First, if p is a prime dividing d_B and $L = \mathbb{Q}_p$, then $B_p = B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is the unique (up to isomorphism) quaternion division algebra over $\mathbb{Q}_p$, and $\mathcal{O}_{B,p} = \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is its unique maximal order.

The other setting is the following. Fix a prime number p. Let $\mathfrak{g}$ be the unique (up to isomorphism) connected p-divisible group of height 2 and dimension 1 over $\overline{\mathbb{F}}_p$, so $\mathfrak{g} \cong E[p^\infty]$ for any supersingular elliptic curve E over $\overline{\mathbb{F}}_p$. Set $\Delta = \mathrm{End}(\mathfrak{g})$. Then Δ is the maximal order in the quaternion division algebra $\Delta_{\mathbb{Q}} = \Delta \otimes_{\mathbb{Q}} \mathbb{Q}_p$ over $\mathbb{Q}_p$. Let $\mathbb{Q}_{p^2}$ be the unique unramified quadratic extension of $\mathbb{Q}_p$ and let $\mathbb{Z}_{p^2} \subset \mathbb{Q}_{p^2}$ be its ring of integers. An explicit description of Δ is given by

$$\Delta \cong \left\{ \begin{bmatrix} a & pb \\ \overline{b} & \overline{a} \end{bmatrix} : a, b \in \mathbb{Z}_{p^2} \right\},$$

where $x \mapsto \overline{x}$ is the nontrivial element of $\mathrm{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$. Now consider the reduced norm $\mathrm{Nrd} : \Delta_{\mathbb{Q}} \to \mathbb{Q}_p$, which, using the above description of Δ, corresponds to the determinant map. One can check that $x \in \Delta_{\mathbb{Q}}^\times$ is in $\Delta^\times$ if and only if $\mathrm{Nrd}(x) \in \mathbb{Z}_p^\times$. Define a function $v_\Delta : \Delta \to \mathbb{Z}$ by $v_\Delta(x) = \mathrm{ord}_p(\mathrm{Nrd}(x))$ (note that since $x \in \Delta$, it is integral over $\mathbb{Z}_p$, so $\mathrm{Nrd}(x) \in \mathbb{Z}_p$). Then v_Δ is a valuation on Δ and there is an element $\Pi \in \Delta$, called a *uniformizer*, with $v_\Delta(\Pi) = 1$; namely, we may take

$$\Pi = \begin{bmatrix} 0 & p \\ 1 & 0 \end{bmatrix}.$$

This makes Δ into a "noncommutative discrete valuation ring", where Δ has a unique maximal ideal $\mathfrak{m}_\Delta = \{x \in \Delta : v_\Delta(x) > 0\}$, $\Delta^\times = \{x \in \Delta : v_\Delta(x) = 0\}$, and $\Delta/\mathfrak{m}_\Delta \cong \mathbb{F}_{p^2}$. As a $\mathbb{Z}_{p^2}$-module, we have a decomposition $\Delta = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}\Pi$, and as a ring $\Delta = \mathbb{Z}_{p^2}[\Pi]$, with multiplication determined by $\Pi^2 = p$ and $\Pi x = \overline{x}\Pi$ for all $x \in \mathbb{Z}_{p^2}$.

Chapter 3

CM pairs

3.1 CM false elliptic curves

We recall the number theoretic setup in the introduction. Let K_1 and K_2 be non-isomorphic imaginary quadratic fields with discriminants d_1 and d_2, and set $K = K_1 \otimes_{\mathbb{Q}} K_2$. Let $F = \mathbb{Q}(\sqrt{d_1 d_2})$ be the real quadratic subfield of K, and let $\mathfrak{D}$ be the different of $F/\mathbb{Q}$. Let $x \mapsto \overline{x}$ denote complex conjugation on K, in other words, the nontrivial element of $\mathrm{Gal}(K/F)$. Assume $(d_1, d_2) = 1$ so K/F is unramified at all finite places, and $\mathcal{O}_{K_1} \otimes_{\mathbb{Z}} \mathcal{O}_{K_2}$ is the maximal order in K. Also, we assume any prime dividing d_B is inert in K_1 and K_2. In particular, each $p \mid d_B$ is nonsplit in K_1 and K_2, which implies K_1 and K_2 embed into B, or equivalently, K_1 and K_2 split B.

If a prime number p is inert in both K_1 and K_2, then p is split in F and each prime of F lying over p is inert in K. If p is ramified in one of K_1 or K_2, then p is ramified in F and the unique prime of F lying over p is inert in K.

Let S be a scheme and (A, i) a false elliptic curve over S. Let $e : S \to A$ be the identity section of A as an abelian scheme. Since $A \to S$ is smooth of relative dimension 2, the sheaf of relative differentials $\Omega_{A/S}$ is a locally free sheaf of rank 2 on A, so $e^*\Omega_{A/S}$ is a locally free sheaf of rank 2 on S. Define the *Lie algebra* $\mathrm{Lie}(A)$ to be the sheaf

$$(e^*\Omega_{A/S})^\vee = \mathscr{H}om_{\mathscr{O}_S}(e^*\Omega_{A/S}, \mathscr{O}_S)$$

on S. This is a locally free $\mathscr{O}_S$-module of rank 2.

For each $x \in \mathcal{O}_B$ there is an S-morphism $i(x) : A \to A$, which induces an $\mathscr{O}_S$-module homomorphism $i(x) : \mathrm{Lie}(A) \to \mathrm{Lie}(A)$, so $\mathrm{Lie}(A)$ is naturally an $\mathcal{O}_B$-module. We write $\mathrm{End}_{\mathcal{O}_B}(\mathrm{Lie}(A))$ for the set of all morphisms of sheaves of $\mathscr{O}_S$-modules $\mathrm{Lie}(A) \to \mathrm{Lie}(A)$ that are also $\mathcal{O}_B$-linear.

Lemma 3.1.1. *If $k = \mathbb{C}$ or $k = \overline{\mathbb{F}}_p$ for $p \nmid d_B$, then* $\mathrm{End}_{\mathcal{O}_B}(\mathrm{Lie}(A)) \cong k$ *for any false elliptic curve A over k.*

Proof. For such a k we have $\mathcal{O}_B \otimes_{\mathbb{Z}} k \cong \mathrm{M}_2(k)$, so $\mathrm{End}_{\mathcal{O}_B}(\mathrm{Lie}(A)) \cong \mathrm{End}_{\mathrm{M}_2(k)}(k^2) \cong k$. □

Definition 3.1.2. Let R be an order in K_1 or K_2 and S an $\mathcal{O}_K$-scheme. A *false elliptic curve over S with complex multiplication by R* is a pair $\mathbf{A} = (A, \kappa)$, where (A, i) is a false elliptic curve over S and $\kappa : R \to \mathrm{End}_{\mathcal{O}_B}(A)$ is a ring homomorphism such that if $\kappa^{\mathrm{Lie}} : R \to \mathrm{End}_{\mathcal{O}_B}(\mathrm{Lie}(A))$ is the induced homomorphism, then the diagram

$$\begin{tikzcd}
R \arrow[rr, "\kappa^{\mathrm{Lie}}"] \arrow[dr] & & \mathrm{End}_{\mathcal{O}_B}(\mathrm{Lie}(A)) \\
& \mathscr{O}_S(S) \arrow[ur] &
\end{tikzcd}$$

commutes, where $R \hookrightarrow \mathcal{O}_K \to \mathscr{O}_S(S)$ is the structure map. We call the commutativity of this diagram the *CM normalization condition.*

Note that since $\kappa : R \to \mathrm{End}_{\mathcal{O}_B}(A)$, we have $i(x) \circ \kappa(y) = \kappa(y) \circ i(x)$ for all $x \in \mathcal{O}_B$ and $y \in R$. Also, any ring homomorphism $R \to \mathrm{End}_{\mathcal{O}_B}(A)$ is automatically injective. To see this, it suffices to show that the composition

$$R \to \mathrm{End}_{\mathcal{O}_B}(A) \to \mathrm{End}_{\mathcal{O}_B}(A_{\overline{s}})$$

is injective where $\overline{s}$ is any geometric point of S, so we may assume $S = \mathrm{Spec}(k)$ for k an algebraically closed field. But then $\mathrm{End}_{\mathcal{O}_B}(A)$ is a torsion free $\mathbb{Z}$-module, so the above map must be injective because otherwise $\mathrm{End}_{\mathcal{O}_B}(A)$ contains a torsion $\mathbb{Z}$-module. In fact, a similar proof shows that any ring homomorphism $\mathcal{O}_B \to \mathrm{End}_S(A)$ is injective, so we did not need to assume this in the definition of a false elliptic curve.

When we speak of a CM false elliptic curve A over $\overline{\mathbb{F}}_{\mathfrak{P}}$ for some prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, where $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$, it is understood that $\mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{P}})$ is an $\mathcal{O}_K$-scheme through the reduction map $\mathcal{O}_K \to \mathbb{F}_{\mathfrak{P}} \hookrightarrow \overline{\mathbb{F}}_{\mathfrak{P}}$. Less precisely, when we speak of a CM false elliptic curve A over $\overline{\mathbb{F}}_p$ for some prime number p, we really mean A is a CM false elliptic curve over $\overline{\mathbb{F}}_{\mathfrak{P}}$ for some prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ lying over p. We will say A is defined over $\overline{\mathbb{F}}_p$ when it is not important to specify the prime ideal $\mathfrak{P}$.

Suppose (A, i) is a false elliptic curve over a field with complex multiplication by an order $R \subset \mathcal{O}_{K_1}$ via the map $\kappa : R \to \mathrm{End}_{\mathcal{O}_B}(A)$. Since K_2 embeds in B by assumption, there is a ring homomorphism $K \to \mathrm{End}^0(A)$ given by

$$x_1 \otimes x_2 \mapsto \kappa(x_1) \circ i(x_2) = i(x_2) \circ \kappa(x_1),$$

where we are extending κ to a map $K_1 = R \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{End}^0_{\mathcal{O}_B}(A)$ and viewing $x_2 \in K_2 \subset B$. This shows A is a CM abelian variety in the traditional sense.

Definition 3.1.3. A *CM pair* over an $\mathcal{O}_K$-scheme S is a pair $(\mathbf{A}_1, \mathbf{A}_2)$ where $\mathbf{A}_1$ and $\mathbf{A}_2$ are false elliptic curves over S with complex multiplication by $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$, respectively. An *isomorphism* between CM pairs $(\mathbf{A}'_1, \mathbf{A}'_2) \to (\mathbf{A}_1, \mathbf{A}_2)$ is a pair (f_1, f_2) where each $f_j : A'_j \to A_j$ is an $\mathcal{O}_{K_j}$-linear isomorphism of false elliptic curves.

Given a CM pair $(\mathbf{A}_1, \mathbf{A}_2)$ over an $\mathcal{O}_K$-scheme S and a morphism of $\mathcal{O}_K$-schemes $T \to S$, there is a CM pair $(\mathbf{A}_1, \mathbf{A}_2)_{/T}$ over T defined as the base change to T.

For every CM pair $(\mathbf{A}_1, \mathbf{A}_2)$ over an $\mathcal{O}_K$-scheme S, set

$$L(\mathbf{A}_1, \mathbf{A}_2) = \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2)$$

and

$$V(\mathbf{A}_1, \mathbf{A}_2) = L(\mathbf{A}_1, \mathbf{A}_2) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

If S is connected we have the quadratic form $\deg^*$ on $L(\mathbf{A}_1, \mathbf{A}_2)$. Let $[f, g] = f^t \circ g + g^t \circ f$ be the associated bilinear form. Then $\mathcal{O}_K = \mathcal{O}_{K_1} \otimes_{\mathbb{Z}} \mathcal{O}_{K_2}$ acts on the $\mathbb{Z}$-module $L(\mathbf{A}_1, \mathbf{A}_2)$ by

$$(x_1 \otimes x_2) \bullet f = \kappa_2(x_2) \circ f \circ \kappa_1(\overline{x}_1). \tag{3.1.1}$$

Note that $(x_1 \otimes x_2) \bullet f \in L(\mathbf{A}_1, \mathbf{A}_2)$ since $\kappa_1(\overline{x}_1), f$, and $\kappa_2(x_2)$ are $\mathcal{O}_B$-linear.

Lemma 3.1.4. *Suppose A is a false elliptic curve with complex multiplication by $\mathcal{O}_{K_j}$ via the homomorphism $\kappa : \mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B}(A)$. If $x \in \mathcal{O}_{K_j}$ is nonzero then $\kappa(x)$ is an isogeny and $\kappa(x)^t = \kappa(\overline{x})$, where $x \mapsto \overline{x}$ is complex conjugation on K_j. In particular, $\deg^*(\kappa(x)) = \mathrm{N}_{K_j/\mathbb{Q}}(x)$ for all $x \in K_j$.*

Proof. The homomorphism $\kappa(x)$ is an isogeny for the same reason that $i(b)$ is an isogeny for any nonzero $b \in \mathcal{O}_B$ (Lemma 2.1.10). For the rest, it suffices to assume A is defined over an algebraically closed field. From the embedding $\kappa : K_j \hookrightarrow \mathrm{End}^0_{\mathcal{O}_B}(A)$ and our classification of such endomorphism algebras over fields, either $\mathrm{End}^0_{\mathcal{O}_B}(A)$ is K_j or a definite quaternion algebra over $\mathbb{Q}$. It follows that there is an embedding $\kappa' : K_j \hookrightarrow \mathrm{End}^0_{\mathcal{O}_B}(A)$ such that the Rosati involution on $\mathrm{End}^0_{\mathcal{O}_B}(A)$ corresponding to the principal polarization $\lambda : A \to A^\vee$ restricts to complex conjugation on $\kappa'(K_j)$. Then using the Noether-Skolem theorem, there is a $u \in \mathrm{End}^0_{\mathcal{O}_B}(A)^\times$ such that $\kappa(x) = u \circ \kappa'(x) \circ u^{-1}$ for all $x \in K_j$, and hence $\deg^*(\kappa(x)) = \deg^*(\kappa'(x))$.

The Rosati involution on $\mathrm{End}^0_{\mathcal{O}_B}(A)$ is given by $\varphi \mapsto \lambda^{-1} \circ \varphi^\vee \circ \lambda = \varphi^t$, so by construction,

$\kappa'(x)^t = \kappa'(\overline{x})$ for any $x \in K_j$. Hence

$$[\deg^*(\kappa'(x))] = \kappa'(x)^t \circ \kappa'(x) = \kappa'(\overline{x}) \circ \kappa'(x) = \kappa'(\overline{x}x) = [\mathrm{N}_{K_j/\mathbb{Q}}(x)],$$

which means $\deg^*(\kappa(x)) = \mathrm{N}_{K_j/\mathbb{Q}}(x)$ for all $x \in K_j$. Then, for any $x \in \mathcal{O}_{K_j}$,

$$\kappa(\overline{x}) \circ \kappa(x) = [\mathrm{N}_{K_j/\mathbb{Q}}(x)] = [\deg^*(\kappa(x))] = \kappa(x)^t \circ \kappa(x)$$

and composing both sides on the right with $\kappa(x)^t$ gives

$$[\deg^*(\kappa(x))] \circ \kappa(\overline{x}) = [\deg^*(\kappa(x))] \circ \kappa(x)^t.$$

Since $\mathrm{End}(A)$ is a torsion-free $\mathbb{Z}$-module it follows that $\kappa(x)^t = \kappa(\overline{x})$. □

Lemma 3.1.5. *If L'/L is a finite separable extension of fields, then for any finite dimensional L'-vector space V, the trace map $\mathrm{Tr}_{L'/L}$ induces an isomorphism $\mathrm{Hom}_{L'}(V, L') \to \mathrm{Hom}_L(V, L)$.*

Proof. If $\varphi \in \mathrm{Hom}_{L'}(V, L')$ is nonzero then it is surjective, so $\mathrm{Tr}_{L'/L} \circ\varphi$ is surjective since $\mathrm{Tr}_{L'/L}$ is (as L'/L is separable). Hence, the L-linear map $\mathrm{Hom}_{L'}(V, L') \to \mathrm{Hom}_L(V, L)$ given by $\varphi \mapsto \mathrm{Tr}_{L'/L} \circ\varphi$ is injective. It is then an isomorphism since each space has L-dimension $\dim_L(V)$. □

Proposition 3.1.6. *Let $(\mathbf{A}_1, \mathbf{A}_2)$ be a CM pair.*
(a) *There is a unique F-bilinear form $[\cdot\,,\cdot]_{\mathrm{CM}}$ on $V(\mathbf{A}_1, \mathbf{A}_2)$ satisfying $[f, g] = \mathrm{Tr}_{F/\mathbb{Q}}[f, g]_{\mathrm{CM}}$. Under this pairing,*

$$[L(\mathbf{A}_1, \mathbf{A}_2), L(\mathbf{A}_1, \mathbf{A}_2)]_{\mathrm{CM}} \subset \mathfrak{D}^{-1}.$$

(b) *The quadratic form $\deg_{\mathrm{CM}}(f) = \frac{1}{2}[f, f]_{\mathrm{CM}}$ is the unique F-quadratic form on $V(\mathbf{A}_1, \mathbf{A}_2)$ satisfying $\deg^*(f) = \mathrm{Tr}_{F/\mathbb{Q}} \deg_{\mathrm{CM}}(f)$.*
(c) *There is a unique K-Hermitian form $\langle\cdot\,,\cdot\rangle_{\mathrm{CM}}$ on $V(\mathbf{A}_1, \mathbf{A}_2)$ which satisfies $[f, g]_{\mathrm{CM}} = \mathrm{Tr}_{K/F}\langle f, g\rangle_{\mathrm{CM}}$.*

Proof. (a) Let $V = V(\mathbf{A}_1, \mathbf{A}_2)$. For any $g \in V$ we have $[\cdot\,, g] \in \mathrm{Hom}_{\mathbb{Q}}(V, \mathbb{Q})$, so by Lemma 3.1.5, $[\cdot\,, g] = \mathrm{Tr}_{F/\mathbb{Q}}(\varphi_g)$ for a unique $\varphi_g \in \mathrm{Hom}_F(V, F)$. Define $[f, g]_{\mathrm{CM}} = \varphi_g(f)$, so $[\cdot\,,\cdot]_{\mathrm{CM}}$ is an F-bilinear form and $[f, g] = \mathrm{Tr}_{F/\mathbb{Q}}[f, g]_{\mathrm{CM}}$.

(b) We have

$$\mathrm{Tr}_{F/\mathbb{Q}} \deg_{\mathrm{CM}}(f) = \mathrm{Tr}_{F/\mathbb{Q}}(\tfrac{1}{2}[f, f]_{\mathrm{CM}}) = \tfrac{1}{2} \mathrm{Tr}_{F/\mathbb{Q}}[f, f]_{\mathrm{CM}} = \tfrac{1}{2}[f, f] = \deg^*(f),$$

and the uniqueness follows from Lemma 3.1.5.

(c) Extending the action (3.1.1) of $\mathcal{O}_K$ on $L(\mathbf{A}_1, \mathbf{A}_2)$, $V = V(\mathbf{A}_1, \mathbf{A}_2)$ is a K-vector space. We claim that $[x \bullet f, g] = [f, \overline{x} \bullet g]$ for all $x \in K$ and $f, g \in V$. For $x = x_1 \otimes x_2 \in K$ compute

$$\begin{aligned}[x \bullet f, g] &= (\kappa_2(x_2) \circ f \circ \kappa_1(\overline{x}_1))^t \circ g + g^t \circ (\kappa_2(x_2) \circ f \circ \kappa_1(\overline{x}_1)) \\ &= \kappa_1(x_1) \circ f^t \circ \kappa_2(\overline{x}_2) \circ g + g^t \circ \kappa_2(x_2) \circ f \circ \kappa_1(\overline{x}_1),\end{aligned}$$

so as elements of $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$,

$$\begin{aligned}[x \bullet f, g] &= \kappa_1(x_1)^{-1} \circ [x \bullet f, g] \circ \kappa_1(x_1) \\ &= f^t \circ \kappa_2(\overline{x}_2) \circ g \circ \kappa_1(x_1) + \kappa_1(x_1)^{-1} \circ g^t \circ \kappa_2(x_2) \circ f \circ [\mathrm{N}_{K_1/\mathbb{Q}}(x_1)].\end{aligned}$$

Hence

$$[f, \overline{x} \bullet g] = f^t \circ \kappa_2(\overline{x}_2) \circ g \circ \kappa_1(x_1) + (\kappa_2(\overline{x}_2) \circ g \circ \kappa_1(x_1))^t \circ f = [x \bullet f, g].$$

For any $g \in V$ we have $[\,\cdot\,, g]_{\mathrm{CM}} \in \mathrm{Hom}_F(V, F)$, so by Lemma 3.1.5 there is a unique $\varphi_g \in \mathrm{Hom}_K(V, K)$ such that $\mathrm{Tr}_{K/F}(\varphi_g) = [\,\cdot\,, g]_{\mathrm{CM}}$. For $f, g \in V$ set $\langle f, g \rangle_{\mathrm{CM}} = \varphi_g(f)$. Then $\langle \cdot, \cdot \rangle_{\mathrm{CM}}$ is K-linear in the first entry and additive in the second, and $\mathrm{Tr}_{K/F}\langle f, g \rangle_{\mathrm{CM}} = [f, g]_{\mathrm{CM}}$. For any $x \in K$ we have

$$\begin{aligned}\mathrm{Tr}_{K/F}\langle f, x \bullet g \rangle_{\mathrm{CM}} &= [f, x \bullet g]_{\mathrm{CM}} = [\overline{x} \bullet f, g]_{\mathrm{CM}} = \mathrm{Tr}_{K/F}\langle \overline{x} \bullet f, g \rangle_{\mathrm{CM}} \\ &= \mathrm{Tr}_{K/F}(\overline{x}\langle f, g \rangle_{\mathrm{CM}}),\end{aligned}$$

so $\langle f, x \bullet g \rangle_{\mathrm{CM}} = \overline{x}\langle f, g \rangle_{\mathrm{CM}}$. The uniqueness again follows from Lemma 3.1.5. □

3.2 Moduli spaces

Definition 3.2.1. For $j \in \{1, 2\}$ define $\mathscr{Y}_j$ to be the category whose objects are triples (A, i, κ), where (A, i) is a false elliptic curve over some $\mathcal{O}_K$-scheme with complex multiplication $\kappa : \mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B}(A)$. A morphism $(A', i', \kappa') \to (A, i, \kappa)$ between two such triples defined over $\mathcal{O}_K$-schemes T and S, respectively, is a morphism of $\mathcal{O}_K$-schemes $T \to S$ together with an $\mathcal{O}_{K_j}$-linear isomorphism $A' \to A \times_S T$ of false elliptic curves.

The category $\mathscr{Y}_j$ is a stack of finite type over $\mathrm{Spec}(\mathcal{O}_K)$. In fact, the structure morphism $\mathscr{Y}_j \to \mathrm{Spec}(\mathcal{O}_K)$ is étale by Corollary 5.1.3 below, proper by a proof identical to that of [13, Proposition 3.3.5], and quasi-finite by Propositions 4.2.1 and 5.1.4 below, so the morphism is finite étale. Let us recall the definition of the fiber $\mathscr{Y}_j(S)$, a general concept for any stack. Let $G : \mathscr{Y}_j \to \mathbf{Sch}/\mathcal{O}_K$ be the functor sending an object of $\mathscr{Y}_j$ over an $\mathcal{O}_K$-scheme S to the $\mathcal{O}_K$-scheme S, and sending an arrow between two objects of $\mathscr{Y}_j$ over $\mathcal{O}_K$-schemes T and S to the morphism $T \to S$ in the definition of an arrow in the category $\mathscr{Y}_j$. Then $\mathscr{Y}_j(S)$ is defined to be the category whose objects are the objects x of $\mathscr{Y}_j$ satisfying $G(x) = S$, and whose arrows are the arrows f of $\mathscr{Y}_j$ satisfying $G(f) = \mathrm{id}_S$. It follows from the definitions that all arrows in $\mathscr{Y}_j(S)$ are isomorphisms. Let $[\mathscr{Y}_j(S)]$ denote the set of isomorphism classes of objects in $\mathscr{Y}_j(S)$.

For each prime p dividing d_B there is a unique maximal ideal $\mathfrak{m}_p \subset \mathcal{O}_B$ of residue characteristic p, and $\mathcal{O}_B/\mathfrak{m}_p$ is a finite field with p^2 elements. Set $\mathfrak{m}_B = \bigcap_{p|d_B} \mathfrak{m}_p$. We have $\mathfrak{m}_B = \prod_{p|d_B} \mathfrak{m}_p$ because for any two primes p and q dividing d_B, $\mathfrak{m}_p\mathfrak{m}_q = \mathfrak{m}_q\mathfrak{m}_p$ since these lattices have equal completions at each prime number. Let x_B be any element of $\mathfrak{m}_B$ whose image generates the principal ideal $\mathfrak{m}_B/d_B\mathcal{O}_B \subset \mathcal{O}_B/d_B\mathcal{O}_B$. Note that

$$\mathcal{O}_B/\mathfrak{m}_B \cong \prod_{p|d_B} \mathbb{F}_{p^2}$$

as rings, so the kernel of any ring homomorphism $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ is of the form $\mathfrak{P}_1 \cdots \mathfrak{P}_r$ for some prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ of $\mathcal{O}_K$ lying over the r primes dividing d_B. Also, giving such a homomorphism θ is equivalent to giving homomorphisms $\theta_j^{\mathfrak{m}_p} : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_p$ for $j = 1, 2$ and each $p \mid d_B$. Let (A, i) be a false elliptic curve over a scheme S. The d_B-torsion $A[d_B]$ is a finite flat commutative S-group scheme with a natural action of $\mathfrak{m}_B/d_B\mathcal{O}_B$. Define the $\mathfrak{m}_B$-torsion of A to be

$$A[\mathfrak{m}_B] = \ker(i(x_B) : A[d_B] \to A[d_B]),$$

which again is a finite flat commutative S-group scheme ($i(x_B) : A \to A$ is an isogeny). This definition does not depend on the choice of x_B. The group scheme $A[\mathfrak{m}_B]$ has a natural action of $\mathcal{O}_B/\mathfrak{m}_B$ given on points by $\overline{x} \cdot a = i(x)(a)$ for $\overline{x} \in \mathcal{O}_B/\mathfrak{m}_B$ and $a \in A[\mathfrak{m}_B](T)$ for any S-scheme T. All the statements of this paragraph are vacuous if B is split.

Definition 3.2.2. Let $j \in \{1, 2\}$ and let $\theta_j : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_B$ be a ring homomorphism. Define $\mathscr{Y}_j^{\theta_j}$ to be the category whose objects are objects (A, i, κ) of $\mathscr{Y}_j$ such that the diagram

$$\begin{tikzcd}
\mathcal{O}_{K_j} \arrow[rr, "\kappa^{\mathfrak{m}_B}"] \arrow[dr, "\theta_j"'] & & \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(A[\mathfrak{m}_B]) \\
& \mathcal{O}_B/\mathfrak{m}_B \arrow[ur] &
\end{tikzcd}$$

commutes, where $\kappa^{\mathfrak{m}_B}$ is the map on $\mathfrak{m}_B$-torsion induced by κ and

$$\mathcal{O}_B/\mathfrak{m}_B \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(A[\mathfrak{m}_B])$$

is the map induced by i. Morphisms are defined in the same way as in the category $\mathscr{Y}_j$.

Note that $\mathscr{Y}_j^{\theta_j} = \mathscr{Y}_j$ if B is split. Recall from the introduction that $\mathscr{C}_j$ is the stack over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{C}_j(S)$ the category of elliptic curves over the $\mathcal{O}_K$-scheme S with CM by $\mathcal{O}_{K_j}$. We will prove below that there is an isomorphism of stacks over $\mathrm{Spec}(\mathcal{O}_K)$

$$\bigsqcup_{\theta_j : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_B} \mathscr{C}_j \to \mathscr{Y}_j \tag{3.2.1}$$

inducing an equivalence of categories $\mathscr{C}_j \to \mathscr{Y}_j^{\theta_j}$ for any θ_j (Theorem 5.2.6). It follows that $\mathscr{Y}_j^{\theta_j}$ has the structure of a stack, finite étale over $\mathrm{Spec}(\mathcal{O}_K)$, and $\mathscr{Y}_j \cong \mathscr{C}_j$ in the case of B split.

Definition 3.2.3. Let $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ be a ring homomorphism. Define $\mathscr{X}_\theta$ to be the category whose objects are CM pairs $(\mathbf{A}_1, \mathbf{A}_2)$ over $\mathcal{O}_K$-schemes such that $\mathbf{A}_j$ is an object of $\mathscr{Y}_j^{\theta_j}$ for $j = 1, 2$, where $\theta_j = \theta|_{\mathcal{O}_{K_j}}$. A morphism $(\mathbf{A}'_1, \mathbf{A}'_2) \to (\mathbf{A}_1, \mathbf{A}_2)$ between two such pairs defined over $\mathcal{O}_K$-schemes T and S, respectively, is a morphism of $\mathcal{O}_K$-schemes $T \to S$ together with an isomorphism (in the above sense) of CM pairs $(\mathbf{A}'_1, \mathbf{A}'_2) \cong (\mathbf{A}_1, \mathbf{A}_2)_{/T}$ over T.

Definition 3.2.4. Let $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ be a ring homomorphism. For any $\alpha \in F^\times$ define $\mathscr{X}_{\theta,\alpha}$ to be the category whose objects are triples $(\mathbf{A}_1, \mathbf{A}_2, f)$ where $(\mathbf{A}_1, \mathbf{A}_2) \in \mathscr{X}_\theta(S)$ for some $\mathcal{O}_K$-scheme S and $f \in L(\mathbf{A}_1, \mathbf{A}_2)$ satisfies $\deg_{\mathrm{CM}}(f) = \alpha$ on every connected component of S. A morphism

$$(\mathbf{A}'_1, \mathbf{A}'_2, f') \to (\mathbf{A}_1, \mathbf{A}_2, f)$$

between two such triples, with $(\mathbf{A}'_1, \mathbf{A}'_2)$ and $(\mathbf{A}_1, \mathbf{A}_2)$ CM pairs over $\mathcal{O}_K$-schemes T and S, respectively, is a morphism of $\mathcal{O}_K$-schemes $T \to S$ together with an isomorphism

$$g : (\mathbf{A}'_1, \mathbf{A}'_2) \to (\mathbf{A}_1, \mathbf{A}_2)_{/T}$$

of CM pairs over T compatible with f and f' in the following sense. Let $g = (g_1, g_2)$ where each $g_j : A'_j \to A_j \times_S T$ is an $\mathcal{O}_{K_j}$-linear isomorphism of false elliptic curves. We require that the diagram

$$\begin{tikzcd}
A'_1 \arrow[r, "g_1"] \arrow[d, "f'"'] & A_1 \times_S T \arrow[d, "f \times \mathrm{id}_T"] \\
A'_2 \arrow[r, "g_2"] & A_2 \times_S T
\end{tikzcd}$$

commute.

As before, the categories $\mathscr{X}_\theta$ and $\mathscr{X}_{\theta,\alpha}$ are stacks of finite type over $\mathrm{Spec}(\mathcal{O}_K)$. Let S be an

$\mathcal{O}_K$-scheme and suppose $(\mathbf{A}_1, \mathbf{A}_2, f)$ is an object of $\mathscr{T}^B_m(S)$, with notation as in the introduction. Set $\alpha = \deg_{\mathrm{CM}}(f)$, so $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = \deg^*(f) = m$ on every connected component of S. By (3.2.1) the pair $(\mathbf{A}_1, \mathbf{A}_2) \in \mathscr{X}_\theta(S)$ for a unique $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$, so $(\mathbf{A}_1, \mathbf{A}_2, f)$ is an object of $\mathscr{X}_{\theta,\alpha}(S)$ and is not an object of $\mathscr{X}_{\eta,\beta}(S)$ for any pair $(\eta, \beta) \neq (\theta, \alpha)$. Therefore there is a decomposition

$$\mathscr{T}^B_m = \bigsqcup_{\substack{\alpha \in F^\times \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = m}} \bigsqcup_{\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B} \mathscr{X}_{\theta,\alpha}.$$

Definition 3.2.5. A false elliptic curve (A, i) over $\overline{\mathbb{F}}_p$ is *supersingular* if the underlying abelian variety A is supersingular: A is isogenous to E^2 for some supersingular elliptic curve E over $\overline{\mathbb{F}}_p$. A CM pair $(\mathbf{A}_1, \mathbf{A}_2)$ over $\overline{\mathbb{F}}_p$ is *supersingular* if the underlying abelian varieties A_1 and A_2 are supersingular.

Lemma 3.2.6. *If p is a prime dividing d_B, or more generally, a prime nonsplit in K_j, then any $A \in \mathscr{Y}_j(\overline{\mathbb{F}}_p)$ is supersingular.*

Proof. By Proposition 2.1.4 there are two possibilities for A up to isogeny. Suppose $A \sim E^2$ for some ordinary elliptic curve E over $\overline{\mathbb{F}}_p$. Then $\mathrm{End}^0(E) \cong L$ for some imaginary quadratic field L and $\mathrm{End}^0_{\mathcal{O}_B}(A) \cong L$. But $K_j \hookrightarrow \mathrm{End}^0_{\mathcal{O}_B}(A)$, so $L \cong K_j$. Tensoring the p-adic representation $\mathrm{End}(E) \to \mathrm{End}_{\mathbb{Z}_p}(T_p(E))$ with $\mathbb{Q}_p$ gives a $\mathbb{Q}_p$-algebra homomorphism

$$K_{j,p} = K_j \otimes_{\mathbb{Q}} \mathbb{Q}_p \to \mathbb{Q}_p.$$

This map cannot be injective by counting dimensions, so $K_{j,p}$ is not a field, which means p is split in K_j. □

Proposition 3.2.7. *Let k be an algebraically closed field of characteristic $p \geqslant 0$ and let $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ be a ring homomorphism. Let $\alpha \in F^\times$ and suppose $(\mathbf{A}_1, \mathbf{A}_2, f) \in \mathscr{X}_{\theta,\alpha}(k)$.*
(a) *We have $p > 0$ and $\mathrm{End}^0_{\mathcal{O}_B}(A_1) \cong \mathrm{End}^0_{\mathcal{O}_B}(A_2) \cong B^{(p)}$. In particular, if $k = \overline{\mathbb{F}}_p$ then $(\mathbf{A}_1, \mathbf{A}_2)$ is a supersingular CM pair.*
(b) *There is an isomorphism of F-quadratic spaces*

$$(V(\mathbf{A}_1, \mathbf{A}_2), \deg_{\mathrm{CM}}) \cong (K, \beta \cdot \mathrm{N}_{K/F})$$

for some $\beta \in F^\times$, with β determined up to multiplication by a norm from $K^\times$. Also, β is totally positive.

(c) *There is an isomorphism of* $\mathbb{Q}$*-quadratic spaces*

$$(V(\mathbf{A}_1, \mathbf{A}_2), \deg^*) \cong (B^{(p)}, \mathrm{Nrd}),$$

where Nrd *is the reduced norm on* $B^{(p)}$*.*

(d) *If* p *does not divide* d_B *then it is nonsplit in* K_1 *and* K_2*.*

Proof. (a) Suppose $p = 0$, so we may assume A_1 and A_2 are false elliptic curves over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$, respectively. Since $\deg^*(f) \neq 0$ by assumption, $f : A_1 \to A_2$ is an isogeny, so it induces an isomorphism $\mathrm{End}^0_{\mathcal{O}_B}(A_1) \cong \mathrm{End}^0_{\mathcal{O}_B}(A_2)$ of $\mathbb{Q}$-algebras. Also by assumption we have embeddings $\kappa_1 : K_1 \hookrightarrow \mathrm{End}^0_{\mathcal{O}_B}(A_1)$ and $\kappa_2 : K_2 \hookrightarrow \mathrm{End}^0_{\mathcal{O}_B}(A_2)$. If A_1, which is isogenous to A_2, is simple then $\mathrm{End}^0_{\mathcal{O}_B}(A_1) \cong \mathrm{End}^0_{\mathcal{O}_B}(A_2) \cong \mathbb{Q}$, which is impossible. The other possibility is $A_1 \sim E^2$ for some elliptic curve E over $\mathbb{C}$, in which case $\mathrm{End}^0_{\mathcal{O}_B}(A_1) \cong \mathrm{End}^0_{\mathcal{O}_B}(A_2) \cong L$ for some imaginary quadratic field L. But then κ_1 and κ_2 induce isomorphisms $K_1 \cong L \cong K_2$, contrary to our assumption about K_1 and K_2. Therefore $p > 0$.

If k has positive transcendence degree over $\overline{\mathbb{F}}_p$, then $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$, which already contains K_1, embeds into an imaginary quadratic field or into $B^{(p)}$. This forces $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$ to be an imaginary quadratic field or $B^{(p)}$ (by counting dimensions over $\mathbb{Q}$). The same statement holds if $k = \overline{\mathbb{F}}_p$. It follows that $\mathrm{End}^0_{\mathcal{O}_B}(A_1) \cong \mathrm{End}^0_{\mathcal{O}_B}(A_2) \cong B^{(p)}$ because otherwise $K_1 \cong K_2$ as above.

(b) Since $f : A_1 \to A_2$ is an isogeny, it induces an isomorphism of $\mathbb{Q}$-vector spaces $V(\mathbf{A}_1, \mathbf{A}_2) \to \mathrm{End}^0_{\mathcal{O}_B}(A_1)$ defined by $\varphi \mapsto f^t \circ \varphi$. As $\mathrm{End}^0_{\mathcal{O}_B}(A_1) \cong B^{(p)}$ has dimension 4 as a $\mathbb{Q}$-vector space, $V(\mathbf{A}_1, \mathbf{A}_2)$ has dimension 1 over K. Therefore $V(\mathbf{A}_1, \mathbf{A}_2)$, together with $\langle \cdot, \cdot \rangle_{\mathrm{CM}}$, is a Hermitian K-module of dimension 1. This means that there is a $\gamma \in K^\times$ such that $\langle v, w \rangle_{\mathrm{CM}} = v\gamma\overline{w}$ for all $v, w \in K$, so

$$\deg_{\mathrm{CM}}(v) = \frac{1}{2}[v, v]_{\mathrm{CM}} = \frac{1}{2}\mathrm{Tr}_{K/F}\langle v, v \rangle_{\mathrm{CM}} = \frac{1}{2}\mathrm{Tr}_{K/F}(v\overline{v}\gamma) = \beta \cdot \mathrm{N}_{K/F}(v),$$

where $\beta = \frac{1}{2}\mathrm{Tr}_{K/F}(\gamma) \in F^\times$. This proves the existence of the isomorphism of F-quadratic spaces.

Now suppose $\gamma' \in K^\times$ is another element satisfying $\langle v, w \rangle_{\mathrm{CM}} = v\gamma'\overline{w}$ for all $v, w \in K$. Then $\gamma = u\gamma'\overline{u} = \gamma' \cdot \mathrm{N}_{K/F}(u)$ for some $u \in K^\times$, so

$$\beta = \frac{1}{2}\mathrm{Tr}_{K/F}(\gamma) = \frac{1}{2}\mathrm{N}_{K/F}(u)\,\mathrm{Tr}_{K/F}(\gamma') = \beta' \cdot \mathrm{N}_{K/F}(u),$$

where β' is the element of $F^\times$ corresponding to γ'. Finally, since $\deg^*$ is positive, $\deg_{\mathrm{CM}}$ is totally positive, so β is totally positive.

(c) Under the isomorphism $V(\mathbf{A}_1, \mathbf{A}_2) \to \mathrm{End}^0_{\mathcal{O}_B}(A_1)$ defined above, the quadratic form $\deg^*$

on $V(\mathbf{A}_1, \mathbf{A}_2)$ corresponds to the quadratic form $b^{-1}\deg^*$ on $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$, where $b = \deg^*(f)$. We claim that under the isomorphism $\mathrm{End}^0_{\mathcal{O}_B}(A_1) \to B^{(p)}$, the quadratic form $\deg^*$ on $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$ corresponds to the quadratic form Nrd on $B^{(p)}$. The Rosati involution $\varphi \mapsto \varphi^\dagger = \varphi^t$ on $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$ corresponds to a positive involution on the definite quaternion algebra $B^{(p)}$, which must be the main involution $x \mapsto x^\iota$ by Lemma 2.1.11(a). Since $\mathrm{Nrd}(x) = xx^\iota$ and $\deg^*(\varphi) = \varphi \circ \varphi^t$, this proves the claim. Therefore there is an isomorphism of $\mathbb{Q}$-quadratic spaces

$$(V(\mathbf{A}_1, \mathbf{A}_2), \deg^*) \cong (B^{(p)}, b^{-1}\,\mathrm{Nrd}).$$

However, since $b > 0$ it is in the image of Nrd, so there is an isomorphism of $\mathbb{Q}$-quadratic spaces

$$(B^{(p)}, b^{-1}\,\mathrm{Nrd}) \cong (B^{(p)}, \mathrm{Nrd}).$$

(d) Suppose $p \nmid d_B$, so p ramifies in $B^{(p)}$. If p splits in K_j then, since K_j embeds in $B^{(p)}$, we have $B^{(p)} \otimes_{\mathbb{Q}} \mathbb{Q}_p \supset K_j \otimes_{\mathbb{Q}} \mathbb{Q}_p \cong \mathbb{Q}_p \times \mathbb{Q}_p$. This is impossible because $B^{(p)} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra. □

Chapter 4

Group actions

In this chapter we describe two group actions on the set $[\mathscr{Y}_j(S)]$, the first of which is used in defining a number called the orbital integral, an important tool used in counting the number of geometric points of $\mathscr{X}_{\theta,\alpha}$. Let $\mathbb{A}_f = \widehat{\mathbb{Q}} = \mathbb{Q} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ denote the ring of finite adeles over $\mathbb{Q}$. More generally, for any number field L, $\widehat{L} = L \otimes_{\mathbb{Q}} \widehat{\mathbb{Q}}$ is the ring of finite adeles over L. For any $\mathbb{Z}$-module M, let $\widehat{M} = M \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ and for any $\mathbb{Q}$-vector space V, let $\widehat{V} = V \otimes_{\mathbb{Q}} \widehat{\mathbb{Q}}$. For any prime number ℓ and any CM pair $(\mathbf{A}_1, \mathbf{A}_2)$, set

$$L_\ell(\mathbf{A}_1, \mathbf{A}_2) = L(\mathbf{A}_1, \mathbf{A}_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell, \quad V_\ell(\mathbf{A}_1, \mathbf{A}_2) = V(\mathbf{A}_1, \mathbf{A}_2) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

For any sets $Y \subset X$ we write $\mathbf{1}_Y : X \to \{0,1\}$ for the characteristic function of Y. For $j \in \{1,2\}$ define an algebraic group T_j over $\mathbb{Q}$ with functor of points given by $T_j(R) = (K_j \otimes_{\mathbb{Q}} R)^\times$ for any $\mathbb{Q}$-algebra R. Note that T_j is the Weil restriction $\mathrm{Res}_{K_j/\mathbb{Q}}(\mathbb{G}_{\mathrm{m}})$. Define a map $\nu_j : T_j \to \mathbb{G}_{\mathrm{m}}$, given on points by $\nu_j(t_j) = t_j\bar{t}_j$, and define an algebraic group T over $\mathbb{Q}$ with functor of points

$$T(R) = \{(t_1, t_2) \in T_1(R) \times T_2(R) : \nu_1(t_1) = \nu_2(t_2)\}.$$

Define another algebraic group T^1 over $\mathbb{Q}$ with

$$T^1(R) = \{z \in (K \otimes_{\mathbb{Q}} R)^\times : \mathrm{N}_{K/F}(z) = 1\}.$$

There is a homomorphism $\nu : T \to \mathbb{G}_{\mathrm{m}}$ given on points by $\nu(t) = \nu_1(t_1) = \nu_2(t_2)$ for $t = (t_1, t_2) \in T(R)$, and there is a homomorphism $\eta : T \to T^1$ defined on points by $\eta(t) = \nu(t)^{-1} \cdot (t_1 \otimes t_2)$.

Let $U \subset T(\mathbb{A}_f)$ be the compact open subgroup

$$U = T(\mathbb{A}_f) \cap (\widehat{\mathcal{O}}_{K_1}^\times \times \widehat{\mathcal{O}}_{K_2}^\times)$$

and let $V = \eta(U) \subset T^1(\mathbb{A}_f)$. There are factorizations $U = \prod_\ell U_\ell$ and $V = \prod_\ell V_\ell$ for some compact open subgroups $U_\ell \subset T(\mathbb{Q}_\ell)$ and $V_\ell \subset T^1(\mathbb{Q}_\ell)$.

Lemma 4.0.8. *If R is a field of characteristic 0, the ring of adeles over $\mathbb{Q}$, or the ring of finite adeles over $\mathbb{Q}$, then the sequence*

$$1 \to R^\times \to T(R) \xrightarrow{\eta} T^1(R) \to 1$$

is exact, where $R^\times \to T(R)$ is the diagonal embedding.

Proof. See [14, Proposition 2.13]. □

Using this one easily shows that $\eta : T \to T^1$ induces an isomorphism of groups

$$T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U \cong T^1(\mathbb{Q})\backslash T^1(\mathbb{A}_f)/V.$$

For $j \in \{1, 2\}$ let $\mathrm{Cl}(\mathcal{O}_{K_j})$ be the ideal class group of K_j and set $\Gamma = \mathrm{Cl}(\mathcal{O}_{K_1}) \times \mathrm{Cl}(\mathcal{O}_{K_2})$. Define a homomorphism

$$I : T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U \to \Gamma$$

by sending $(t_1, t_2) \in T(\mathbb{A}_f)$ to the pair of ideal classes $(\mathfrak{a}_1, \mathfrak{a}_2) \in \Gamma$ with

$$\mathfrak{a}_j = \prod_{\mathfrak{p} \subset \mathcal{O}_{K_j}} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}((t_j)_\mathfrak{p})},$$

where the product is over all prime ideals of $\mathcal{O}_{K_j}$ and $(t_j)_\mathfrak{p}$ is the $\mathfrak{p}$-th component of the idele t_j. Note that if $(t_1, t_2) \in T(\mathbb{A}_f)$ then $t_j \in T_j(\widehat{\mathbb{Q}}) = \widehat{K}_j^\times$ is a finite idele of K_j.

Proposition 4.0.9. *The map I is an isomorphism of groups.*

Proof. See [14, Proposition 2.14]. □

4.1 The Serre tensor construction

For any $\mathcal{O}_K$-scheme S we will describe how the group Γ acts on the set $[\mathscr{X}_\theta(S)]$ using a general construction of Serre which we now recall. We state these results only over a commutative ring, which suffices for our purposes, but they hold more generally over any associative ring, but then care must be taken in distinguishing between left and right modules. For more details see [7, Section 7].

Theorem 4.1.1. *Let R be a commutative ring, M a finitely generated projective R-module (in particular, M is locally free), with dual module $M^\vee = \operatorname{Hom}_R(M, R)$, and $\mathscr{M}$ an R-module scheme over a scheme S (that is, $\mathscr{M}$ is a commutative S-group scheme together with an R-action).*
(a) *The functor $X \mapsto M \otimes_R \mathscr{M}(X) \cong \operatorname{Hom}_R(M^\vee, \mathscr{M}(X))$ on S-schemes is represented by a commutative group scheme over S, denoted $M \otimes_R \mathscr{M}$ or $\operatorname{Hom}_R(M^\vee, \mathscr{M})$.*
(b) *Suppose $\mathscr{M} \to S$ is a locally finite type R-module scheme. If $\mathscr{M}$ is smooth or proper over S, then so is $M \otimes_R \mathscr{M}$. If the S-fibers of $\mathscr{M}$ are connected, then so are the S-fibers of $M \otimes_R \mathscr{M}$. In particular, if $\mathscr{M} \to S$ is an abelian scheme then so is $M \otimes_R \mathscr{M}$. Furthermore, if $\mathscr{M}$ has fibers over S of dimension d and M has constant local rank r over R, then $M \otimes_R \mathscr{M}$ has fibers of dimension dr.*
(c) *Let M and N be finitely generated projective R-modules. For any two R-module schemes $\mathscr{M}$ and $\mathscr{N}$ over a scheme S, view the group $\operatorname{Hom}_S(\mathscr{M}, \mathscr{N})$ as an R-module via the action on $\mathscr{N}$. Then the natural map*

$$\xi_{N,M} : N^\vee \otimes_R \operatorname{Hom}_S(\mathscr{M}, \mathscr{N}) \otimes_R M \to \operatorname{Hom}_S(\operatorname{Hom}_R(M, \mathscr{M}), \operatorname{Hom}_R(N, \mathscr{N})),$$

defined on points in S-schemes by

$$(\xi_{N,M}(\ell \otimes \varphi \otimes m))(f) : n \mapsto \ell(n)\varphi(f(m)),$$

is an isomorphism of R-modules. In other words,

$$\operatorname{Hom}_S(M \otimes_R \mathscr{M}, N \otimes_R \mathscr{N}) \cong N \otimes_R \operatorname{Hom}_S(\mathscr{M}, \mathscr{N}) \otimes_R M^\vee.$$

Now suppose (A, κ) is a false elliptic curve over an $\mathcal{O}_K$-scheme S with complex multiplication by an order R in K_1 or K_2, and let $\mathfrak{a}$ be a fractional ideal of R. Since there is a ring homomorphism $\kappa : R \to \operatorname{End}_S(A)$, we may view A as an R-module scheme over S, so from $\mathfrak{a}$ being a finitely generated projective R-module, there is a commutative S-group scheme $\mathfrak{a} \otimes_R A$ with $(\mathfrak{a} \otimes_R A)(X) = \mathfrak{a} \otimes_R A(X)$ for any S-scheme X. As $A \to S$ is an abelian scheme of relative dimension 2 and $\mathfrak{a}$ is locally free of rank 1, we see that $\mathfrak{a} \otimes_R A \to S$ is an abelian scheme of relative dimension 2. Next, the ring homomorphism $i : \mathcal{O}_B \to \operatorname{End}_S(A)$ induces a ring homomorphism

$$i_{\mathfrak{a}} : \mathcal{O}_B \to \operatorname{End}_S(\mathfrak{a} \otimes_R A)$$

given on points by

$$i_{\mathfrak{a}}(x)(a \otimes \alpha) = a \otimes i(x)(\alpha)$$

for any S-scheme X, $x \in \mathcal{O}_B$, and $\alpha \in A(X)$. In the same way, the ring homomorphism $\kappa : R \to \mathrm{End}_{\mathcal{O}_B}(A)$ induces a ring homomorphism

$$\kappa_{\mathfrak{a}} : R \to \mathrm{End}_S(\mathfrak{a} \otimes_R A)$$

satisfying $\kappa_{\mathfrak{a}}(y) \circ i_{\mathfrak{a}}(x) = i_{\mathfrak{a}}(x) \circ \kappa_{\mathfrak{a}}(y)$ for all $x \in \mathcal{O}_B$ and $y \in R$.

Finally we consider the CM normalization condition. There is a natural isomorphism of $\mathscr{O}_S$-modules $\mathrm{Lie}(\mathfrak{a} \otimes_R A) \cong \mathfrak{a} \otimes_R \mathrm{Lie}(A)$, which can be seen by using the following functorial definition of $\mathrm{Lie}(A)$: for any S-scheme X,

$$\mathrm{Lie}(A)(X) = \ker(A(X[\varepsilon]) \to A(X)),$$

where $X[\varepsilon] = X \otimes_{\mathbb{Z}} \mathbb{Z}[\varepsilon]$ and $\mathbb{Z}[\varepsilon] = \mathbb{Z}[Y]/(Y^2)$. (The connection between the two descriptions of $\mathrm{Lie}(A)$ is as follows. Viewing $\mathrm{Lie}(A)$ as a sheaf of $\mathscr{O}_S$-modules, the functor $X \mapsto \mathrm{Lie}(A)(X)$ on S-schemes is given by

$$X \mapsto (\mathrm{Lie}(A) \otimes_{\mathscr{O}_S} \mathscr{O}_X)(X),$$

the global sections of the $\mathscr{O}_X$-module $\mathrm{Lie}(A) \otimes_{\mathscr{O}_S} \mathscr{O}_X$. Going the other direction, viewing $\mathrm{Lie}(A)$ as a functor on S-schemes as above, it defines an $\mathscr{O}_S$-module by restricting to open immersions $X \to S$.) Using this isomorphism, the induced map

$$\kappa_{\mathfrak{a}}^{\mathrm{Lie}} : R \to \mathrm{End}_{\mathcal{O}_B}(\mathrm{Lie}(\mathfrak{a} \otimes_R A)) \cong \mathrm{End}_{\mathcal{O}_B}(\mathfrak{a} \otimes_R \mathrm{Lie}(A))$$

is given by $\kappa_{\mathfrak{a}}^{\mathrm{Lie}}(y)(a \otimes t) = a \otimes \kappa^{\mathrm{Lie}}(y)(t)$ for any $t \in \mathrm{Lie}(A)(U)$ with $U \subset S$ an open set. Since κ^{Lie} satisfies the CM normalization condition, it follows that $\kappa_{\mathfrak{a}}^{\mathrm{Lie}}$ does as well. This shows $\mathfrak{a} \otimes_R A$ is a false elliptic curve over S with complex multiplication by R.

For any $\mathcal{O}_K$-scheme S and any ring homomorphism $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$, we claim that the group Γ acts on the set $[\mathscr{X}_\theta(S)]$ by

$$(\mathfrak{a}_1, \mathfrak{a}_2) \cdot (\mathbf{A}_1, \mathbf{A}_2) = (\mathfrak{a}_1 \otimes_{\mathcal{O}_{K_1}} A_1, \mathfrak{a}_2 \otimes_{\mathcal{O}_{K_2}} A_2).$$

(This action clearly only depends on $\mathfrak{a}_j$ through its ideal class.) We will write $\mathfrak{a}_j \otimes \mathbf{A}_j$ for the false elliptic curve $\mathfrak{a}_j \otimes_{\mathcal{O}_{K_j}} A_j$ with complex multiplication by $\mathcal{O}_{K_j}$. Let $(\mathbf{A}_1, \mathbf{A}_2) \in \mathscr{X}_\theta(S)$ and

$(\mathfrak{a}_1, \mathfrak{a}_2) \in \Gamma$. Since

$$(i_j)_{\mathfrak{a}_j} : \mathcal{O}_B \to \mathrm{End}_S(\mathfrak{a}_j \otimes A_j)$$

is given on points by $(i_j)_{\mathfrak{a}_j}(x)(a \otimes \alpha) = a \otimes i_j(x)(\alpha)$, there is an isomorphism of $\mathcal{O}_{K_j}$-module schemes over S

$$(\mathfrak{a}_j \otimes A_j)[\mathfrak{m}_B] \cong \mathfrak{a}_j \otimes A_j[\mathfrak{m}_B].$$

The map

$$(\kappa_j^{\mathfrak{m}_B})_{\mathfrak{a}_j} : \mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(\mathfrak{a}_j \otimes A_j[\mathfrak{m}_B])$$

is then given on points by $(\kappa_j^{\mathfrak{m}_B})_{\mathfrak{a}_j}(x)(a \otimes t) = a \otimes \kappa_j^{\mathfrak{m}_B}(x)(t)$. Since $(\mathbf{A}_1, \mathbf{A}_2) \in \mathscr{X}_\theta(S)$, it follows that the diagram

$$\begin{tikzcd}
\mathcal{O}_{K_j} \arrow[rr, "(\kappa_j^{\mathfrak{m}_B})_{\mathfrak{a}_j}"] \arrow[dr, "\theta_j"'] & & \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(\mathfrak{a}_j \otimes A_j[\mathfrak{m}_B]) \\
& \mathcal{O}_B/\mathfrak{m}_B \arrow[ur] &
\end{tikzcd}$$

commutes, which means $(\mathfrak{a}_1 \otimes \mathbf{A}_1, \mathfrak{a}_2 \otimes \mathbf{A}_2) \in \mathscr{X}_\theta(S)$.

Now let $(\mathbf{A}_1, \mathbf{A}_2)$ be a CM pair over an algebraically closed field. Recall that K acts on $V(\mathbf{A}_1, \mathbf{A}_2)$ by

$$(x_1 \otimes x_2) \bullet f = \kappa_2(x_2) \circ f \circ \kappa_1(\overline{x}_1).$$

By restriction we see that $T^1(\mathbb{Q}) \subset K^\times$ acts on $V(\mathbf{A}_1, \mathbf{A}_2)$, and by composing with the homomorphism $\eta : T \to T^1$, $T(\mathbb{Q})$ acts on $V(\mathbf{A}_1, \mathbf{A}_2)$. This action is given by

$$t \bullet f = \kappa_2(t_2) \circ f \circ \kappa_1(t_1)^{-1}$$

for $t = (t_1, t_2) \in T(\mathbb{Q})$ because

$$\kappa_1(t_1)^{-1} = \kappa_1(t_1)^t \otimes \deg^*(\kappa_1(t_1))^{-1} = \kappa_1(\bar{t}_1) \otimes \mathrm{N}_{K_1/\mathbb{Q}}(t_1)^{-1}$$

in $\mathrm{End}^0_{\mathcal{O}_B}(A_1)$, while $\eta(t) = \mathrm{N}_{K_1/\mathbb{Q}}(t_1)^{-1} \cdot (t_1 \otimes t_2)$.

Now fix $t = (t_1, t_2) \in T(\mathbb{A}_f)$ and let $(\mathfrak{a}_1, \mathfrak{a}_2) = I(t) \in \Gamma$, with I the isomorphism in Proposition 4.0.9. For $j \in \{1, 2\}$ there is an $\mathcal{O}_{K_j}$-linear quasi-isogeny

$$f_j \in \mathrm{Hom}_{\mathcal{O}_B}(A_j, \mathfrak{a}_j \otimes A_j) \otimes_{\mathbb{Z}} \mathbb{Q},$$

defined on points by $f_j(x) = 1 \otimes x$. Then the map

$$V(\mathfrak{a}_1 \otimes \mathbf{A}_1, \mathfrak{a}_2 \otimes \mathbf{A}_2) \to V(\mathbf{A}_1, \mathbf{A}_2)$$

given by $\varphi \mapsto f_2^{-1} \circ \varphi \circ f_1$ is an $\mathcal{O}_K$-linear isomorphism of vector spaces. This map identifies $L(\mathfrak{a}_1 \otimes \mathbf{A}_1, \mathfrak{a}_2 \otimes \mathbf{A}_2)$ with the $\mathcal{O}_K$-submodule

$$\kappa_2(\mathfrak{a}_2) \circ L(\mathbf{A}_1, \mathbf{A}_2) \circ \kappa_1(\mathfrak{a}_1^{-1}) \subset V(\mathbf{A}_1, \mathbf{A}_2).$$

We may extend the map $\kappa_j : \mathcal{O}_{K_j} \to \mathrm{End}(A_j)$ to a map $K_{j,\ell} \to \mathrm{End}(A_j) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ or to a map $\widehat{K}_j \to \mathrm{End}(A_j) \otimes_{\mathbb{Z}} \widehat{\mathbb{Q}}$ by tensoring with $\mathbb{Q}_\ell$ or $\widehat{\mathbb{Q}}$. Then we have a $\widehat{K}$-linear isomorphism of $\widehat{F}$-quadratic spaces

$$\widehat{V}(\mathbf{A}_1, \mathbf{A}_2) \cong \widehat{V}(\mathfrak{a}_1 \otimes \mathbf{A}_1, \mathfrak{a}_2 \otimes \mathbf{A}_2)$$

with $\widehat{L}(\mathfrak{a}_1 \otimes \mathbf{A}_1, \mathfrak{a}_2 \otimes \mathbf{A}_2)$ isomorphic to the $\widehat{\mathcal{O}}_K$-submodule

$$t \bullet \widehat{L}(\mathbf{A}_1, \mathbf{A}_2) = \{\kappa_2(t_2) \circ f \circ \kappa_1(t_1)^{-1} : f \in \widehat{L}(\mathbf{A}_1, \mathbf{A}_2)\}$$

of $\widehat{V}(\mathbf{A}_1, \mathbf{A}_2)$.

Definition 4.1.2. Let $(\mathbf{A}_1, \mathbf{A}_2)$ be a supersingular CM pair over an algebraically closed field of positive characteristic. For each prime number ℓ and $\alpha \in F_\ell^\times$ define the *orbital integral* at ℓ by

$$O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2) = \sum_{t \in \mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell} \mathbf{1}_{L_\ell(\mathbf{A}_1, \mathbf{A}_2)}(t^{-1} \bullet f)$$

if there is an $f \in V_\ell(\mathbf{A}_1, \mathbf{A}_2)$ satisfying $\deg_{\mathrm{CM}}(f) = \alpha$. If no such f exists then set $O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2) = 0$.

Since $T(\mathbb{Q}_\ell)$ acts transitively on the set of all $f \in V_\ell(\mathbf{A}_1, \mathbf{A}_2)$ such that $\deg_{\mathrm{CM}}(f) = \alpha$, the orbital integral does not depend on the choice of f in the definition.

Lemma 4.1.3. *Let S be an $\mathcal{O}_K$-scheme and for $j \in \{1, 2\}$ set $w_j = |\mathcal{O}_{K_j}^\times|$. Every $x \in \mathscr{X}_\theta(S)$, viewed as an element of the set $[\mathscr{X}_\theta(S)]$, has trivial stabilizer in Γ and satisfies $|\operatorname{Aut}_{\mathscr{X}_\theta(S)}(x)| = w_1 w_2$.*

Proof. Suppose we have $(\mathfrak{a}_1, \mathfrak{a}_2) \in \Gamma$ and a CM pair $x = (\mathbf{A}_1, \mathbf{A}_2) \in \mathscr{X}_\theta(S)$ satisfying $(\mathbf{A}_1, \mathbf{A}_2) \cong (\mathfrak{a}_1 \otimes \mathbf{A}_1, \mathfrak{a}_2 \otimes \mathbf{A}_2)$. This means that there is an $\mathcal{O}_{K_j}$-linear isomorphism of false elliptic curves $A_j \cong \mathfrak{a}_j \otimes A_j$ for $j = 1, 2$. Set $\mathcal{O}_j = \mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_{K_j}$ and let $\mathrm{Hom}_{\mathcal{O}_j}(A_j, \mathfrak{a}_j \otimes A_j)$ be the $\mathcal{O}_{K_j}$-module of $\mathcal{O}_{K_j}$-linear homomorphisms $A_j \to \mathfrak{a}_j \otimes A_j$ of false elliptic curves. Then there is an isomorphism of $\mathcal{O}_{K_j}$-modules

$$\mathrm{Hom}_{\mathcal{O}_j}(A_j, A_j) \cong \mathrm{Hom}_{\mathcal{O}_j}(A_j, \mathfrak{a}_j \otimes A_j).$$

By Theorem 4.1.1(c) there is an isomorphism of $\mathcal{O}_{K_j}$-modules

$$\mathrm{Hom}_{\mathcal{O}_{K_j}}(A_j, \mathfrak{a}_j \otimes A_j) \cong \mathfrak{a}_j \otimes_{\mathcal{O}_{K_j}} \mathrm{End}_{\mathcal{O}_{K_j}}(A_j),$$

so $\mathrm{End}_{\mathcal{O}_j}(A_j) \cong \mathfrak{a}_j \otimes_{\mathcal{O}_{K_j}} \mathrm{End}_{\mathcal{O}_j}(A_j)$. We claim that $\mathrm{End}_{\mathcal{O}_j}(A_j) \cong \mathcal{O}_{K_j}$ as a ring and as an $\mathcal{O}_{K_j}$-module. By definition, $\mathrm{End}_{\mathcal{O}_j}(A_j)$ is the centralizer of $\mathcal{O}_{K_j}$ in $\mathrm{End}_{\mathcal{O}_B}(A_j)$. Picking any geometric point $\overline{s}$ of S, there are inclusions

$$\mathcal{O}_{K_j} \hookrightarrow \mathrm{End}_{\mathcal{O}_B}(A_j) \hookrightarrow \mathrm{End}_{\mathcal{O}_B}((A_j)_{\overline{s}}),$$

the second coming from Lemma 2.1.7. By our classification of such endomorphism rings, either $\mathrm{End}_{\mathcal{O}_B}((A_j)_{\overline{s}}) \cong \mathcal{O}_{K_j}$ or $\mathrm{End}_{\mathcal{O}_B}((A_j)_{\overline{s}})$ is an order in a quaternion algebra, so the same is true of $\mathrm{End}_{\mathcal{O}_B}(A_j)$. The centralizer of $\mathcal{O}_{K_j}$ in either such ring is $\mathcal{O}_{K_j}$. Hence $\mathfrak{a}_j \cong \mathcal{O}_{K_j}$ as an $\mathcal{O}_{K_j}$-module, which means $\mathfrak{a}_j$ is principal. Finally, by definition, an automorphism of x in $\mathscr{X}_\theta(S)$ is a pair of elements (a_1, a_2) with $a_j \in \mathrm{Aut}_{\mathcal{O}_j}(A_j) \cong \mathcal{O}_{K_j}^\times$, so $|\mathrm{Aut}_{\mathscr{X}_\theta(S)}(x)| = w_1 w_2$. □

Proposition 4.1.4. *Let p be a prime number that is nonsplit in K_1 and K_2 and suppose $(\mathbf{A}_1, \mathbf{A}_2)$ is a CM pair over $\overline{\mathbb{F}}_p$ (necessarily supersingular). For any $\alpha \in F^\times$ totally positive,*

$$\sum_{(\mathfrak{a}_1,\mathfrak{a}_2)\in\Gamma} \#\{f \in L(\mathfrak{a}_1 \otimes \mathbf{A}_1, \mathfrak{a}_2 \otimes \mathbf{A}_2) : \deg_{\mathrm{CM}}(f) = \alpha\} = \frac{w_1 w_2}{2} \prod_\ell O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2).$$

Proof. The proof is formally the same as [14, Proposition 2.18], replacing the definitions there with our analogous definitions. □

This result will form part of our calculation of the number of geometric points of $\mathscr{X}_{\theta,\alpha}$. The other part will be to find an expression for the product of the orbital integrals, which we do below in Theorem 7.3.3.

4.2 The Atkin-Lehner group

The other important group action on $[\mathscr{Y}_j(S)]$ comes from the Atkin-Lehner group W_0 of $\mathcal{O}_B$. By definition, $W_0 = \mathrm{N}_{B^\times}(\mathcal{O}_B)/\mathbb{Q}^\times\mathcal{O}_B^\times = \langle w_p : p \mid d_B \rangle$, where $w_p \in \mathcal{O}_B$ has reduced norm p. As an abstract group, $W_0 \cong \prod_{p|d_B} \mathbb{Z}/2\mathbb{Z}$. The group W_0 acts on the set $[\mathscr{Y}_j(S)]$ for any $\mathcal{O}_K$-scheme S as follows: for $w \in W_0$ and $x = (A, i, \kappa) \in \mathscr{Y}_j(S)$, define $w \cdot x = (A, i_w, \kappa)$, where $i_w : \mathcal{O}_B \to \mathrm{End}_S(A)$

is given by $i_w(a) = i(waw^{-1})$. Note that

$$\begin{aligned}\mathrm{End}_{\mathcal{O}_B}(w \cdot A) &= \{f \in \mathrm{End}(A) : f \circ i_w(a) = i_w(a) \circ f \text{ for all } a \in \mathcal{O}_B\} \\ &= \{f \in \mathrm{End}(A) : f \circ i(a) = i(a) \circ f \text{ for all } a \in \mathcal{O}_B\} \\ &= \mathrm{End}_{\mathcal{O}_B}(A),\end{aligned}$$

and the CM action $\kappa : \mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B}(w \cdot A) = \mathrm{End}_{\mathcal{O}_B}(A)$ is unchanged under the action of w, so (A, i_w, κ) still satisfies the CM normalization condition. As described above, $\mathrm{Cl}(\mathcal{O}_{K_j})$ acts on $[\mathscr{Y}_j(S)]$ through Serre's tensor construction. Clearly the actions of W_0 and $\mathrm{Cl}(\mathcal{O}_{K_j})$ commute, so there is an induced action of $W_0 \times \mathrm{Cl}(\mathcal{O}_{K_j})$ on $[\mathscr{Y}_j(S)]$.

Proposition 4.2.1. *The group $W_0 \times \mathrm{Cl}(\mathcal{O}_{K_j})$ acts simply transitively on $[\mathscr{Y}_j(\mathbb{C})]$.*

Proof. It is shown in [15] that $W_0' \times \mathrm{Cl}(\mathcal{O}_{K_j})$ acts simply transitively on $[\mathscr{Y}_j(\mathbb{C})]$, where $W_0' \subset W_0$ is the subgroup generated by $\{w_p : p \mid d_B,\, p \text{ inert in } K_j\}$. However, we are assuming each prime $p \mid d_B$ is inert in K_j. □

Chapter 5

Deformation theory I

The main result of this chapter states that any CM false elliptic curve arises from a CM elliptic curve through the Serre tensor construction. We will use this in the next chapter to give a description, in terms of certain coordinates, of the ring $\mathrm{Hom}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ for A a CM false elliptic curve over $\overline{\mathbb{F}}_p$ for $p \mid d_B$. Another important result of this chapter that will be needed later is that the group $W_0 \times \mathrm{Cl}(\mathcal{O}_{K_j})$ acts simply transitively on the set $[\mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})]$. Fix a prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ of residue characteristic p. Let $\mathscr{W}$ be the ring of integers of the completion of the maximal unramified extension of $K_{\mathfrak{P}}$, so in particular $\mathscr{W}$ is an $\mathcal{O}_K$-algebra. Let **CLN** be the category whose objects are complete local Noetherian $\mathscr{W}$-algebras with residue field $\overline{\mathbb{F}}_{\mathfrak{P}}$, where $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$, and morphisms $R \to R'$ are local ring homomorphisms inducing the identity $\overline{\mathbb{F}}_{\mathfrak{P}} \to \overline{\mathbb{F}}_{\mathfrak{P}}$ on residue fields.

5.1 General theory

For $j \in \{1, 2\}$ and $m \geqslant 1$ an integer define $\mathscr{M}_j^m$ to be the category whose objects are triples $(\mathscr{A}, \kappa, \lambda)$, where

(1) $\mathscr{A} \to S$ is an abelian scheme of relative dimension m over an $\mathcal{O}_{K_j}$-scheme S,

(2) $\kappa : \mathcal{O}_{K_j} \to \mathrm{End}_S(\mathscr{A})$ is a ring homomorphism,

(3) $\lambda : \mathscr{A} \to \mathscr{A}^\vee$ is a principal polarization satisfying $\lambda \circ \kappa(x) = \kappa(\overline{x})^\vee \circ \lambda$ for all $x \in \mathcal{O}_{K_j}$.

We also require that the diagram

$$\begin{tikzcd}
\mathcal{O}_{K_j} \arrow[rr, "\kappa^{\mathrm{Lie}}"] \arrow[dr] & & \mathrm{End}_{\mathscr{O}_S}(\mathrm{Lie}(\mathscr{A})) \\
& \mathscr{O}_S(S) \arrow[ur] &
\end{tikzcd}$$

commute, where $\mathcal{O}_{K_j} \to \mathscr{O}_S(S)$ is the structure map. A morphism $(\mathscr{A}', \kappa', \lambda') \to (\mathscr{A}, \kappa, \lambda)$ between two such triples defined over $\mathcal{O}_{K_j}$-schemes T and S, respectively, is a morphism of $\mathcal{O}_{K_j}$-schemes $T \to S$ together with an $\mathcal{O}_{K_j}$-linear isomorphism $\varphi : \mathscr{A}' \to \mathscr{A} \times_S T$ of abelian schemes over T such that the diagram

$$\begin{tikzcd}
(\mathscr{A} \times_S T)^\vee \cong \mathscr{A}^\vee \times_S T \arrow[r, "\varphi^\vee"] & (\mathscr{A}')^\vee \\
\mathscr{A} \times_S T \arrow[u, "\lambda \times \mathrm{id}_T"] \arrow[r, "\varphi^{-1}"] & \mathscr{A}' \arrow[u, "\lambda'"']
\end{tikzcd}$$

commutes. The category $\mathscr{M}_j^m$ is a stack over $\mathrm{Spec}(\mathcal{O}_{K_j})$.

If $\widetilde{R} \to R$ is a surjection of $\mathcal{O}_{K_j}$-algebras and $x = (\mathscr{A}, \kappa, \lambda) \in \mathscr{M}_j^m(R)$, a *deformation* of x to $\widetilde{R}$ is an object $(\widetilde{\mathscr{A}}, \widetilde{\kappa}, \widetilde{\lambda}) \in \mathscr{M}_j^m(\widetilde{R})$ together with an isomorphism

$$\varphi : \widetilde{\mathscr{A}} \otimes_{\widetilde{R}} R \to \mathscr{A}$$

of abelian schemes compatible with $\kappa, \widetilde{\kappa}, \lambda, \widetilde{\lambda}$. This last condition means that the diagram

$$\begin{tikzcd}
\widetilde{\mathscr{A}} \otimes_{\widetilde{R}} R \arrow[r, "\widetilde{\kappa}(a) \otimes \mathrm{id}_R"] \arrow[d, "\varphi"'] & \widetilde{\mathscr{A}} \otimes_{\widetilde{R}} R \arrow[d, "\varphi"] \\
\mathscr{A} \arrow[r, "\kappa(a)"] & \mathscr{A}
\end{tikzcd}$$

commutes for all $a \in \mathcal{O}_{K_j}$ and the diagram

$$\begin{tikzcd}
\widetilde{\mathscr{A}} \otimes_{\widetilde{R}} R \arrow[r, "\widetilde{\lambda} \otimes \mathrm{id}_R"] & (\widetilde{\mathscr{A}})^\vee \otimes_{\widetilde{R}} R \cong (\widetilde{\mathscr{A}} \otimes_{\widetilde{R}} R)^\vee \\
\mathscr{A} \arrow[u, "\varphi^{-1}"] \arrow[r, "\lambda"] & \mathscr{A}^\vee \arrow[u, "\varphi^\vee"']
\end{tikzcd} \tag{5.1.1}$$

commutes.

Theorem 5.1.1. *If $\widetilde{R} \to R$ is a surjection of $\mathcal{O}_{K_j}$-algebras with nilpotent kernel, then*

(a) *each $\mathscr{A} \in \mathscr{M}_j^m(R)$ admits a unique deformation to $\widetilde{\mathscr{A}} \in \mathscr{M}_j^m(\widetilde{R})$,*

(b) *for any $\mathscr{A} \in \mathscr{M}_j^m(R)$ and $\mathscr{B} \in \mathscr{M}_j^n(R)$ the reduction map*

$$\mathrm{Hom}_{\mathcal{O}_{K_j}}(\widetilde{\mathscr{A}}, \widetilde{\mathscr{B}}) \to \mathrm{Hom}_{\mathcal{O}_{K_j}}(\mathscr{A}, \mathscr{B})$$

is an isomorphism.

Proof. See [12, Proposition 2.1.2]. □

Another way of stating part (a) is that the structure morphism $\mathscr{M}_j^m \to \mathrm{Spec}(\mathcal{O}_{K_j})$ is étale. This morphism is also proper, by a proof identical to that of [13, Proposition 3.3.5].

If S is an $\mathcal{O}_K$-scheme and $x = (A, i, \kappa) \in \mathscr{Y}_j(S)$ then $x \in \mathscr{M}_j^2(S)$. To see this, all we need to check is that x satisfies condition (3) above. By Proposition 2.1.12 there is some principal polarization $\lambda : A \to A^\vee$, and by definition, $\kappa(y)^t = \lambda^{-1} \circ \kappa(y)^\vee \circ \lambda$ for any $y \in \mathcal{O}_{K_j}$. But from Lemma 3.1.4, $\kappa(y)^t = \kappa(\overline{y})$, and hence $\kappa(\overline{y})^\vee \circ \lambda = \lambda \circ \kappa(y)$ for all $y \in \mathcal{O}_{K_j}$.

Definition 5.1.2. Suppose $\widetilde{R} \to R$ is a surjection of $\mathcal{O}_K$-algebras and $x = (A, i, \kappa) \in \mathscr{Y}_j(R)$. A *deformation of* x (or just a *deformation of* A) *to* $\widetilde{R}$ is an object $(\widetilde{A}, \widetilde{i}, \widetilde{\kappa}) \in \mathscr{Y}_j(\widetilde{R})$ together with an $\mathcal{O}_{K_j}$-linear isomorphism $\widetilde{A} \otimes_{\widetilde{R}} R \to A$ of false elliptic curves.

Suppose $\widetilde{R} \to R$ is a surjection of $\mathcal{O}_K$-algebras, $(A, i, \kappa) \in \mathscr{Y}_j(R)$, and $(\widetilde{A}, \widetilde{i}, \widetilde{\kappa}) \in \mathscr{Y}_j(\widetilde{R})$ is a deformation of (A, i, κ). We claim it is automatic that the principal polarizations $\widetilde{\lambda} : \widetilde{A} \to (\widetilde{A})^\vee$ and $\lambda : A \to A^\vee$ defined in Proposition 2.1.12 are compatible in the sense that a diagram such as (5.1.1) commutes, where $\varphi : \widetilde{A} \otimes_{\widetilde{R}} R \to A$ is an isomorphism. To see this, first note that $\widetilde{\lambda}$ and φ induce a principal polarization $\lambda' : A \to A^\vee$ defined by

$$\lambda' = (\varphi^\vee)^{-1} \circ (\widetilde{\lambda} \otimes \mathrm{id}_R) \circ \varphi^{-1},$$

so we have the diagram (5.1.1) with λ' in place of λ. Now, using the fact that

$$\widetilde{\lambda}_{\overline{t}}^{-1} \circ \widetilde{i}(x)^\vee \circ \widetilde{\lambda}_{\overline{t}} = \widetilde{i}(x^*)$$

for all $x \in \mathcal{O}_B$ and all geometric points $\overline{t}$ of $\mathrm{Spec}(\widetilde{R})$, and the fact that

$$i(x) \circ \varphi = \varphi \circ (\widetilde{i}(x) \otimes \mathrm{id}_R)$$

for all $x \in \mathcal{O}_B$, a computation shows

$$(\lambda')_{\overline{s}}^{-1} \circ i(x)^\vee \circ (\lambda')_{\overline{s}} = i(x^*)$$

for all $x \in \mathcal{O}_B$ and all geometric points $\overline{s}$ of $\mathrm{Spec}(R)$. By the uniqueness part of Proposition 2.1.12 we must have $\lambda' = \lambda$, which proves the claim.

Let $x = (A, i, \kappa) \in \mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})$ and define a functor $\mathrm{Def}_{\mathcal{O}_B}(A, \mathcal{O}_{K_j}) : \mathbf{CLN} \to \mathbf{Sets}$ that assigns to each object R of $\mathbf{CLN}$ the set of isomorphism classes of deformations of x to R. If $R \to R'$ is a morphism in $\mathbf{CLN}$ then the corresponding map

$$\mathrm{Def}_{\mathcal{O}_B}(A, \mathcal{O}_{K_j})(R) \to \mathrm{Def}_{\mathcal{O}_B}(A, \mathcal{O}_{K_j})(R')$$

is defined by $\widetilde{A} \mapsto \widetilde{A} \otimes_R R'$.

Corollary 5.1.3. *The functor* $\mathrm{Def}_{\mathcal{O}_B}(A, \mathcal{O}_{K_j})$ *is represented by* $\mathscr{W}$*, so there is a bijection*

$$\mathrm{Def}_{\mathcal{O}_B}(A, \mathcal{O}_{K_j})(R) \cong \mathrm{Hom}_{\mathbf{CLN}}(\mathscr{W}, R),$$

which is a one point set, for any object R *of* $\mathbf{CLN}$*. In particular, the reduction map* $[\mathscr{Y}_j(R)] \to [\mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})]$ *is a bijection for any* $R \in \mathbf{CLN}$*.*

Proof. Let R be an Artinian object of $\mathbf{CLN}$, so the reduction map $R \to \overline{\mathbb{F}}_{\mathfrak{P}}$ is surjective with nilpotent kernel, the maximal ideal of R. Since $A \in \mathscr{M}_j^2(\overline{\mathbb{F}}_{\mathfrak{P}})$, it has a unique deformation to $\widetilde{A} \in \mathscr{M}_j^2(R)$ and the reduction map $\mathrm{End}_{\mathcal{O}_{K_j}}(\widetilde{A}) \to \mathrm{End}_{\mathcal{O}_{K_j}}(A)$ is an isomorphism. Therefore we can lift the $\mathcal{O}_{K_j}$-linear action of $\mathcal{O}_B$ on A to a unique such action on $\widetilde{A}$. This shows that each object of $\mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})$ has a unique deformation to an object of $\mathscr{Y}_j(R)$ for any Artinian R in $\mathbf{CLN}$. Now let R be an arbitrary object of $\mathbf{CLN}$, so $R = \varprojlim R/\mathfrak{m}^n$, where $\mathfrak{m} \subset R$ is the maximal ideal, and $R/\mathfrak{m}^n$ is an Artinian object of $\mathbf{CLN}$. The result now follows from the Artinian case, the bijection

$$\mathrm{Hom}_{\mathbf{CLN}}(\mathscr{W}, R) \cong \varprojlim \mathrm{Hom}_{\mathbf{CLN}}(\mathscr{W}, R/\mathfrak{m}^n),$$

and the fact that the natural map

$$\mathrm{Def}_{\mathcal{O}_B}(A, \mathcal{O}_{K_j})(R) \to \varprojlim \mathrm{Def}_{\mathcal{O}_B}(A, \mathcal{O}_{K_j})(R/\mathfrak{m}^n)$$

is a bijection by Grothendieck's existence theorem ([7, Theorem 3.4]). □

Proposition 5.1.4. *The group* $W_0 \times \mathrm{Cl}(\mathcal{O}_{K_j})$ *acts simply transitively on* $[\mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})]$*.*

Proof. Let $\mathbb{C}_p$ be the metric completion of an algebraic closure of $\mathbb{Q}_p$, where p is the prime below $\mathfrak{P}$, and fix a ring embedding $\mathscr{W} \to \mathbb{C}_p$. There is a $W_0 \times \mathrm{Cl}(\mathcal{O}_{K_j})$-equivariant bijection $[\mathscr{Y}_j(\mathbb{C}_p)] \to [\mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})]$ defined as follows. Let $A \in \mathscr{Y}_j(\mathbb{C}_p)$. Since A is a CM abelian variety over $\mathbb{C}_p$, it descends to a number field, which means there is an abelian surface A_0 over L with an action of $\mathcal{O}_{K_j}$, for some number field L, and an isomorphism $A_0 \otimes_L \mathbb{C}_p \cong A$ compatible with the actions of $\mathcal{O}_{K_j}$ on each. By passing to a finite extension of L if necessary, we may assume $\mathrm{End}_{\overline{L}}(A_0) = \mathrm{End}_L(A_0)$, where $\overline{L}$ is an algebraic closure of L. Now fix a prime $\mathfrak{p} \subset \mathcal{O}_L$ lying over p. Passing to a further finite extension of L, we may assume A_0 has good reduction at $\mathfrak{p}$, since A_0 is a CM abelian variety. From [7, Theorem 2.1(1)], the natural map $\mathrm{End}_{\overline{L}}(A_0) \to \mathrm{End}_{\mathbb{C}_p}(A)$ is an isomorphism, so there is an isomorphism $\mathrm{End}_{\mathcal{O}_{K_j}}(A_0) \to \mathrm{End}_{\mathcal{O}_{K_j}}(A)$. Therefore the $\mathcal{O}_{K_j}$-linear $\mathcal{O}_B$-action on A induces such an action on A_0, which means A_0 is a CM false elliptic curve over L (the CM normalization condition descends as well as base extends). Let $\mathscr{A}_0$ be the Néron model of A_0 at $\mathfrak{p}$, so $\mathscr{A}_0$ is an abelian scheme over $\mathcal{O}_{L,\mathfrak{p}}$ satisfying $\mathscr{A}_0 \otimes_{\mathcal{O}_{L,\mathfrak{p}}} \mathrm{Frac}(\mathcal{O}_{L,\mathfrak{p}}) \cong A_0$. Since $\mathrm{End}_L(A_0) \cong \mathrm{End}_{\mathcal{O}_{L,\mathfrak{p}}}(\mathscr{A}_0)$, there are induced commuting actions of $\mathcal{O}_B$ and $\mathcal{O}_{K_j}$ on $\mathscr{A}_0$, making it into a CM false elliptic curve over $\mathcal{O}_{L,\mathfrak{p}}$. Finally, let $\widetilde{A}_0 = \mathscr{A}_0 \otimes_{\mathcal{O}_{L,\mathfrak{p}}} \mathcal{O}_L/\mathfrak{p}$, so $\widetilde{A}_0$ is a CM false elliptic curve over $\mathcal{O}_L/\mathfrak{p}$. Define $[\mathscr{Y}_j(\mathbb{C}_p)] \to [\mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})]$ by $A \mapsto \widetilde{A}_0 \otimes_{\mathcal{O}_L/\mathfrak{p}} \overline{\mathbb{F}}_{\mathfrak{P}}$. This map does not depend on the abelian surface A_0 or the number field L such that $A_0 \otimes_L \mathbb{C}_p \cong A$ since we are base extending to $\overline{\mathbb{F}}_{\mathfrak{P}}$ in the end.

Next define a map $[\mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})] \to [\mathscr{Y}_j(\mathbb{C}_p)]$ as the composition

$$[\mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})] \to [\mathscr{Y}_j(\mathscr{W})] \to [\mathscr{Y}_j(\mathbb{C}_p)],$$

where the first map is the inverse of the reduction map in Corollary 5.1.3 and the second map is base extension to $\mathbb{C}_p$. This is the inverse to the map $[\mathscr{Y}_j(\mathbb{C}_p)] \to [\mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})]$ defined above. The result now follows from Proposition 4.2.1. □

5.2 Structure of CM false elliptic curves

Our next goal is to prove there is an isomorphism as in (3.2.1). It will be a consequence of this isomorphism that any $A \in \mathscr{Y}_j(S)$ is of the form $M \otimes_{\mathcal{O}_{K_j}} E$ for some $E \in \mathscr{C}_j(S)$ and some $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_{K_j}$-module M, free of rank 4 over $\mathbb{Z}$. To prove this result, we will describe a bijection between the set of isomorphism classes of such modules M and the set $[\mathscr{Y}_j(\mathbb{C})]$.

For $j \in \{1, 2\}$ set $\mathcal{O}_j = \mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_{K_j}$ and define $\mathscr{L}_j$ to be the set of isomorphism classes of $\mathcal{O}_j$-modules that are free of rank 4 over $\mathbb{Z}$. Define $\mathscr{K}_j$ to be the set of $\mathcal{O}_B^\times$-conjugacy classes of ring embeddings $\mathcal{O}_{K_j} \hookrightarrow \mathcal{O}_B$. We begin by examining the local structure of modules in $\mathscr{L}_j$.

Lemma 5.2.1. *Fix a prime p, let Δ be the maximal order in the unique quaternion division algebra $\Delta_{\mathbb{Q}}$ over $\mathbb{Q}_p$, and fix an embedding $\mathbb{Z}_{p^2} \hookrightarrow \Delta$. There is an isomorphism of rings $\mathbb{Z}_{p^2} \otimes_{\mathbb{Z}_p} \Delta \cong R_1$, where*

$$R_1 = \begin{bmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ p\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \end{bmatrix}$$

is the standard Eichler order of level 1 *in* $\mathrm{M}_2(\mathbb{Q}_{p^2})$.

Proof. There is a ring homomorphism $f : \mathbb{Z}_{p^2} \to \mathrm{End}_{\mathbb{Z}_{p^2}}(\Delta)$ given by $f(a)(\delta) = a\delta$, and there is a ring homomorphism $g : \Delta \to \mathrm{End}_{\mathbb{Z}_{p^2}}(\Delta)$ given by $g(x)(\delta) = \delta x^\iota$, where $x \mapsto x^\iota$ is the main involution on $\Delta_{\mathbb{Q}}$. Note that g is multiplicative since $(xy)^\iota = y^\iota x^\iota$. As f and g have commuting images, there is an induced ring homomorphism

$$\Phi : \mathbb{Z}_{p^2} \otimes_{\mathbb{Z}_p} \Delta \to \mathrm{End}_{\mathbb{Z}_{p^2}}(\Delta) \cong \mathrm{M}_2(\mathbb{Z}_{p^2})$$

given by $\Phi(a \otimes x)(\delta) = a\delta x^\iota$. Tensoring this map with $\mathbb{Q}_{p^2}$ induces the natural isomorphism $\mathbb{Q}_{p^2} \otimes_{\mathbb{Q}_p} \Delta_{\mathbb{Q}} \cong \mathrm{M}_2(\mathbb{Q}_{p^2})$ (the maximal subfield $\mathbb{Q}_{p^2} \subset \Delta_{\mathbb{Q}}$ containing $\mathbb{Q}_p$ splits $\Delta_{\mathbb{Q}}$), so $\ker \Phi$ is a torsion $\mathbb{Z}_p$-module. However, $\mathbb{Z}_{p^2} \otimes_{\mathbb{Z}_p} \Delta$ is a torsion-free $\mathbb{Z}_p$-module, which means Φ is injective.

Let $\mathfrak{m}_\Delta \subset \Delta$ be the unique maximal ideal. Then $\mathrm{End}_{\mathbb{Z}_{p^2}}(\mathfrak{m}_\Delta)$ and $\mathrm{End}_{\mathbb{Z}_{p^2}}(\Delta)$ are distinct maximal orders in $\mathrm{End}_{\mathbb{Q}_{p^2}}(\Delta \otimes_{\mathbb{Z}_{p^2}} \mathbb{Q}_{p^2}) \cong \mathrm{M}_2(\mathbb{Q}_{p^2})$ and

$$\mathrm{im}\, \Phi \subset R' = \mathrm{End}_{\mathbb{Z}_{p^2}}(\Delta) \cap \mathrm{End}_{\mathbb{Z}_{p^2}}(\mathfrak{m}_\Delta).$$

Since R' is an Eichler order in $\mathrm{M}_2(\mathbb{Q}_{p^2})$, it is conjugate to

$$R_n = \begin{bmatrix} \mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \\ p^n\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2} \end{bmatrix}$$

for some $n \geqslant 1$ ([7, Lemma A.9(2)]). To show $\mathrm{im}\, \Phi = R_1$, we will consider the discriminants of the orders $\mathrm{im}\, \Phi \cong \mathbb{Z}_{p^2} \otimes_{\mathbb{Z}_p} \Delta$ and R' in $\mathrm{M}_2(\mathbb{Q}_{p^2})$. By [7, Example A.13], $\mathrm{disc}(\Delta) = p^2\mathbb{Z}_p$, and thus $\mathrm{disc}(\mathrm{im}\, \Phi) = \mathrm{disc}(\Delta)\mathbb{Z}_{p^2} = p^2\mathbb{Z}_{p^2}$. By [7, Example A.12], $\mathrm{disc}(R') = \mathrm{disc}(R_n) = p^{2n}\mathbb{Z}_{p^2}$. Now, for any $\mathbb{Z}_{p^2}$-orders $\mathcal{O} \subset \mathcal{O}'$, we have $\mathrm{disc}(\mathcal{O}') \mid \mathrm{disc}(\mathcal{O})$, with equality if and only if $\mathcal{O} = \mathcal{O}'$. As $\mathrm{im}\, \Phi \subset R'$, $p^{2n}\mathbb{Z}_{p^2} \mid p^2\mathbb{Z}_{p^2}$, so we must have $n = 1$ and $\mathrm{im}\, \Phi = R' \cong R_1$. □

Lemma 5.2.2. *Fix a prime* p *and let* Δ *be the maximal order in the unique quaternion division algebra over* $\mathbb{Q}_p$. *Fix an embedding* $\mathbb{Z}_{p^2} \hookrightarrow \Delta$ *so that there is a decomposition* $\Delta = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}\Pi$, *where* Π *is a uniformizer satisfying* $\Pi^2 = p$ *and* $\Pi a = \overline{a}\Pi$ *for all* $a \in \mathbb{Z}_{p^2}$. *Then any ring homomorphism* $f : \Delta \to \mathrm{M}_2(\mathbb{Z}_{p^2})$ *is* $\mathrm{GL}_2(\mathbb{Z}_{p^2})$*-conjugate to exactly one of the following two maps:*

$$f_1 : a + b\Pi \mapsto \begin{bmatrix} a & b \\ p\overline{b} & \overline{a} \end{bmatrix}, \quad f_2 : a + b\Pi \mapsto \begin{bmatrix} a & pb \\ \overline{b} & \overline{a} \end{bmatrix}.$$

The proof uses the general ideas of the proof of [24, Theorem 1.4].

Proof. Let $M = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$. Then M is a left $\mathbb{Z}_{p^2}$-module via componentwise multiplication, and a right Δ-module via matrix multiplication $\begin{bmatrix} a & b \end{bmatrix} f(x)$, viewing elements of M as row vectors. These actions commute, so M is a $\Delta \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$-module. By Lemma 5.2.1, $\Delta \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2} \cong R_1$ is the standard Eichler order of level 1 in $\mathrm{M}_2(\mathbb{Q}_{p^2})$ and thus a hereditary order. (A hereditary order $\mathcal{O}$ in a central simple algebra over a finite extension L of $\mathbb{Q}_p$ is an $\mathcal{O}_L$-order such that all left $\mathcal{O}$-lattices (left $\mathcal{O}$-modules that are $\mathcal{O}_L$-free of finite rank) are $\mathcal{O}$-projective; any Eichler order of squarefree level is hereditary.) Any R_1-module which is free of finite rank over $\mathbb{Z}_p$ is a direct sum of copies of Δ and $\mathfrak{m}_\Delta$, where $\mathfrak{m}_\Delta \subset \Delta$ is the unique maximal ideal ([23, Chapter 9]). By comparing $\mathbb{Z}_p$-ranks, we see that there is an isomorphism of $\Delta \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$-modules $\varphi : M \to \Delta$ or $\varphi : M \to \mathfrak{m}_\Delta$.

First suppose $\varphi : M \to \Delta$ is an isomorphism of $\Delta \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$-modules, where Δ is a right Δ-module through multiplication on the right, and a left $\mathbb{Z}_{p^2}$-module through multiplication on the left via the inclusion $\mathbb{Z}_{p^2} \hookrightarrow \Delta$. Let M' be the group M with the same left $\mathbb{Z}_{p^2}$-action, but now a right Δ-action given by

$$(x, y) \cdot (a + b\Pi) = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b \\ p\bar{b} & \bar{a} \end{bmatrix}.$$

Then there is an isomorphism $\psi : \Delta \to M'$ of $\Delta \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$-modules given by $\psi(a + b\Pi) = \begin{bmatrix} a & b \end{bmatrix}$, and thus $\gamma = \psi \circ \varphi : M \to M'$ is a $\Delta \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$-linear isomorphism. Hence $\gamma \in \mathrm{GL}_2(\mathbb{Z}_{p^2})$ and since it is Δ-linear, $\gamma(m \cdot x) = \gamma(m) \cdot x$ for all $x \in \Delta$ and $m \in M$. Therefore $f = \gamma \circ f_1 \circ \gamma^{-1}$.

Now suppose $\varphi : M \to \mathfrak{m}_\Delta$ is an isomorphism of $\Delta \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$-modules, where $\mathfrak{m}_\Delta$ is a right Δ-module through multiplication on the right, and a left $\mathbb{Z}_{p^2}$-module through $\mathbb{Z}_{p^2} \hookrightarrow \Delta$. Let M' be the group M with the same left $\mathbb{Z}_{p^2}$-action, but now a right Δ-action given by

$$(x, y) \cdot (a + b\Pi) = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & pb \\ \bar{b} & \bar{a} \end{bmatrix}.$$

Writing $\mathfrak{m}_\Delta = p\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}\Pi$, there is an isomorphism $\psi : \mathfrak{m}_\Delta \to M'$ of $\Delta \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$-modules given by $\psi(pa + b\Pi) = \begin{bmatrix} a & b \end{bmatrix}$. Similar to the first case, it follows that $f = \gamma \circ f_2 \circ \gamma^{-1}$, where $\gamma = \psi \circ \varphi \in \mathrm{GL}_2(\mathbb{Z}_{p^2})$.

To show f_1 and f_2 are not $\mathrm{GL}_2(\mathbb{Z}_{p^2})$-conjugate, first note that $f_1 = T f_2 T^{-1}$, where

$$T = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}.$$

Suppose f_1 and f_2 are conjugate, so $f_1 = X f_2 X^{-1}$ for some $X \in \mathrm{GL}_2(\mathbb{Z}_{p^2})$. Then conjugation by T on $f_2(\Delta) \subset \mathrm{M}_2(\mathbb{Z}_{p^2})$ is equal to conjugation by X, which means $X = UT$ for some U in the center of $f_2(\Delta)$. In particular, $U \in \mathrm{M}_2(\mathbb{Z}_{p^2})$. We then have

$$0 = \mathrm{ord}_p(\det(X)) = \mathrm{ord}_p(\det(U)) + 1 \geqslant 1,$$

a contradiction. □

Lemma 5.2.3. *Let p be a prime number. For $p \nmid d_B$ there is a unique isomorphism class of $\mathcal{O}_{j,p}$-modules free of rank 4 over $\mathbb{Z}_p$ and for $p \mid d_B$ there are two isomorphism classes.*

Proof. First suppose $p \nmid d_B$. In this case,

$$\mathcal{O}_{j,p} \cong \mathcal{O}_{B,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_{K_j,p} \cong \mathrm{M}_2(\mathcal{O}_{K_j,p}),$$

and any $\mathcal{O}_{j,p}$-module that is free of rank 4 over $\mathbb{Z}_p$ is isomorphic to $\mathcal{O}_{K_j,p} \oplus \mathcal{O}_{K_j,p}$, with the natural left action of $\mathrm{M}_2(\mathcal{O}_{K_j,p})$. Now suppose $p \mid d_B$, so $\mathcal{O}_{j,p} \cong \Delta \otimes_{\mathbb{Z}_p} \mathbb{Z}_{p^2}$. By the proof of Lemma 5.2.2 there are two isomorphism classes of modules over this ring that are free of rank 4 over $\mathbb{Z}_p$. □

Now we will show that the three sets $\mathscr{K}_j$, $\mathscr{L}_j$, and $[\mathscr{Y}_j(\mathbb{C})]$ are all in bijection.

Proposition 5.2.4. *There is a bijection $\mathscr{K}_j \to \mathscr{L}_j$.*

Proof. Let $\Theta : \mathcal{O}_{K_j} \to \mathcal{O}_B$ be a representative of an $\mathcal{O}_B^\times$-conjugacy class of embeddings and define $f : \mathscr{K}_j \to \mathscr{L}_j$ by sending Θ to the $\mathbb{Z}$-module $L_\Theta = \mathcal{O}_B$, viewed as a right $\mathcal{O}_{K_j}$-module through Θ (and multiplication on the right) and a left $\mathcal{O}_B$-module through multiplication on the left. The isomorphism class of this $\mathcal{O}_j$-module only depends on Θ through its $\mathcal{O}_B^\times$-conjugacy class. To show f is injective, suppose $\Theta, \Theta' : \mathcal{O}_{K_j} \to \mathcal{O}_B$ are two embeddings and suppose $\varphi : L_\Theta \to L_{\Theta'}$ is an $\mathcal{O}_j$-module isomorphism. By $\mathcal{O}_{K_j}$-linearity we have $\varphi(x\Theta(a)) = \varphi(x)\Theta'(a)$ for all $a \in \mathcal{O}_{K_j}$ and all $x \in \mathcal{O}_B$. By $\mathcal{O}_B$-linearity we have $\varphi \in \mathrm{End}_{\mathcal{O}_B}(\mathcal{O}_B)^\times$. There is an isomorphism of rings $\mathcal{O}_B^{\mathrm{op}} \to \mathrm{End}_{\mathcal{O}_B}(\mathcal{O}_B)$ defined by sending x to the endomorphism $y \mapsto yx$. Therefore there is a $u \in \mathcal{O}_B^\times$ such that $\varphi(x) = xu$ for all $x \in \mathcal{O}_B$, so $\Theta = u\Theta' u^{-1}$.

There is an action of the group $\mathrm{Cl}(\mathcal{O}_{K_j})$ on the set $\mathscr{K}_j$ given explicitly by the so-called "Shimura reciprocity law" (we describe this below; see [6, Theorem 60(b)]), and under the injection $f : \mathscr{K}_j \to \mathscr{L}_j$, this action corresponds to the action $\mathfrak{a} \cdot M = \mathfrak{a}^{-1} \otimes_{\mathcal{O}_{K_j}} M$ of $\mathrm{Cl}(\mathcal{O}_{K_j})$ on $\mathscr{L}_j$. To show f is surjective, let $M \in \mathscr{L}_j$ and let $\Theta : \mathcal{O}_{K_j} \to \mathcal{O}_B$ be an embedding such that $(L_\Theta)_\ell \cong M_\ell$ as $\mathcal{O}_{j,\ell}$-modules for all primes ℓ (such a Θ exists for any M; see the discussion below). Then there is an $\mathcal{O}_j$-linear isomorphism

$$L_\Theta \otimes_{\mathcal{O}_{K_j}} \mathrm{Hom}_{\mathcal{O}_j}(L_\Theta, M) \to M$$

given by $x \otimes \varphi \mapsto \varphi(x)$, where the module on the left has the obvious left $\mathcal{O}_B$-action through its action on L_Θ, and $\mathrm{Hom}_{\mathcal{O}_j}(L_\Theta, M)$ is an $\mathcal{O}_{K_j}$-module via the pointwise action on the images of the homomorphisms (that this map is an isomorphism can be checked by proving it is an isomorphism after completion at each prime number, and using the following fact). The $\mathcal{O}_{K_j}$-module $\mathfrak{a} = \mathrm{Hom}_{\mathcal{O}_j}(L_\Theta, M)$ is a fractional ideal: for any prime number ℓ, there is an isomorphism of $\mathcal{O}_{K_j,\ell}$-modules $\mathfrak{a} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathcal{O}_{K_j,\ell}$. Hence $M \cong L_\Theta \otimes_{\mathcal{O}_{K_j}} \mathfrak{a} = \mathfrak{a}^{-1} \cdot L_\Theta$ is in the image of f, as $\mathrm{Cl}(\mathcal{O}_{K_j})$ acts on $f(\mathscr{K}_j) \cong \mathscr{K}_j$. □

Proposition 5.2.5. *There is a bijection* $\mathscr{L}_j \to [\mathscr{Y}_j(\mathbb{C})]$.

Proof. Let $M \in \mathscr{L}_j$. Then $V = M \otimes_{\mathbb{Z}} \mathbb{R}$ is a 4-dimensional $\mathbb{R}$-vector space with M a $\mathbb{Z}$-lattice in V. The action of $\mathcal{O}_{K_j}$ on M induces a map $K_j \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{C} \to \mathrm{End}(V)$, turning V into a $\mathbb{C}$-vector space. Define a function $\mathscr{L}_j \to [\mathscr{Y}_j(\mathbb{C})]$ by sending M to the CM false elliptic curve with complex points V/M. The inverse $[\mathscr{Y}_j(\mathbb{C})] \to \mathscr{L}_j$ is given by $A \mapsto H_1(A(\mathbb{C}), \mathbb{Z})$, the first homology of $A(\mathbb{C})$. □

Next we will describe further refinements of the sets $\mathscr{K}_j$ and $\mathscr{L}_j$, and how the elements $\Theta \in \mathscr{K}_j$ relate to homomorphisms $\theta_j : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_B$. Define an equivalence relation on the set $\mathscr{K}_j$ according to $\Theta \sim \Theta'$ if and only if the induced maps $\widetilde{\Theta}, \widetilde{\Theta}' : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_B$ are equal. Let $\mathscr{K}_j'$ be the set of equivalence classes under this relation. Under the bijection $\mathscr{K}_j \to \mathscr{L}_j$, this equivalence relation corresponds to the following equivalence relation on $\mathscr{L}_j$: $M \sim M'$ if and only if $M_\ell \cong M_\ell'$ as $\mathcal{O}_{j,\ell}$-modules for all primes ℓ (note by Lemma 5.2.3 that this really is only a condition at each prime dividing d_B). Let $\mathscr{L}_j'$ be the set of equivalence classes under this relation.

We know that the group $W_0 \times \mathrm{Cl}(\mathcal{O}_{K_j})$ acts simply transitively on the set $[\mathscr{Y}_j(\mathbb{C})]$, so its natural actions on $\mathscr{K}_j$ and $\mathscr{L}_j$ are also simply transitive (the above bijections are both equivariant with respect to this group). Explicitly, the action of W_0 on $\mathscr{K}_j$ is given by $w \cdot \Theta = \Theta'$, where $\Theta'(a) = w\Theta(a)w^{-1}$, and the action on $\mathscr{L}_j$ is given by $w \cdot L_\Theta = L_{w\cdot\Theta}$. The action of $\mathrm{Cl}(\mathcal{O}_{K_j})$ on $\mathscr{L}_j$ is given by $\mathfrak{a} \cdot M = \mathfrak{a}^{-1} \otimes_{\mathcal{O}_{K_j}} M$ and the action on $\mathscr{K}_j$ is defined as follows, according to the Shimura reciprocity law. Let $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{K_j})$ and let $\Theta : \mathcal{O}_{K_j} \to \mathcal{O}_B$. Then $\Theta(\mathfrak{a})\mathcal{O}_B = x\mathcal{O}_B$ for some $x \in \mathcal{O}_B$ and $\mathfrak{a} \cdot \Theta = \Theta'$, where $\Theta'(a) = x^{-1}\Theta(a)x$.

The elements of $\mathscr{L}_j'$ can be thought of as collections of $\mathcal{O}_{j,\ell}$-modules $\{M_\ell\}_\ell$ indexed by the prime numbers. The action of W_0 on $\mathscr{L}_j$ induces an action on $\mathscr{L}_j'$. Explicitly, for $\ell \mid d_B$, the Atkin-Lehner operator $w_\ell \in W_0$ interchanges the two isomorphism classes of modules M_ℓ over $\mathcal{O}_{j,\ell}$ (see Proposition 7.2.7 below). It follows that under the action of $W_0 \times \mathrm{Cl}(\mathcal{O}_{K_j})$ on $\mathscr{L}_j$, the group $\mathrm{Cl}(\mathcal{O}_{K_j})$ acts simply transitively on each equivalence class under $\sim$ and the group W_0 acts simply transitively on the set of equivalence classes $\mathscr{L}_j'$. The corresponding results hold for the set $\mathscr{K}_j$, so in particular $\#\mathscr{K}_j' = |W_0| = 2^r$, where r is the number of primes dividing d_B. Since there are two ring homomorphisms $\mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_p \cong \mathbb{F}_{p^2}$ for each $p \mid d_B$, there are 2^r ring homomorphisms $\mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_B$, which shows that each such homomorphism arises as the reduction of a homomorphism $\mathcal{O}_{K_j} \to \mathcal{O}_B$.

The equivalence relation $\sim$ on $\mathscr{K}_j$ induces an equivalence relation on the set $[\mathscr{Y}_j(\mathbb{C})]$ determined by the following: if $[\Theta]$ is the equivalence class of $\Theta \in \mathscr{K}_j$, then $[\Theta]$ is in bijection with $[\mathscr{Y}_j^{\widetilde{\Theta}}(\mathbb{C})]$, where $\widetilde{\Theta} : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_B$ is the map induced by $\Theta : \mathcal{O}_{K_j} \to \mathcal{O}_B$. It follows that the natural action of $\mathrm{Cl}(\mathcal{O}_{K_j})$ on $[\mathscr{Y}_j^{\widetilde{\Theta}}(\mathbb{C})]$ is simply transitive. The same statements hold with $[\mathscr{Y}_j^{\widetilde{\Theta}}(\overline{\mathbb{F}}_{\mathfrak{P}})]$ in place of $[\mathscr{Y}_j^{\widetilde{\Theta}}(\mathbb{C})]$.

Suppose (E,κ) is an elliptic curve over an $\mathcal{O}_K$-scheme S with CM by $\mathcal{O}_{K_j}$ and suppose $M \in \mathscr{L}_j$. The ring homomorphism $\kappa : \mathcal{O}_{K_j} \to \mathrm{End}_S(E)$ gives E the structure of an $\mathcal{O}_{K_j}$-module scheme over S, so from M being a finitely generated projective $\mathcal{O}_{K_j}$-module, locally free of rank 2, there is an abelian scheme $M \otimes_{\mathcal{O}_{K_j}} E \to S$ of relative dimension 2 with $(M \otimes_{\mathcal{O}_{K_j}} E)(X) = M \otimes_{\mathcal{O}_{K_j}} E(X)$ for any S-scheme X. There are commuting actions

$$i_M : \mathcal{O}_B \to \mathrm{End}_S(M \otimes_{\mathcal{O}_{K_j}} E), \quad \kappa_M : \mathcal{O}_{K_j} \to \mathrm{End}_S(M \otimes_{\mathcal{O}_{K_j}} E)$$

given on points by

$$i_M(x)(m \otimes z) = x \cdot m \otimes z, \quad \kappa_M(a)(m \otimes z) = m \otimes \kappa(a)(z).$$

As above, $M \otimes_{\mathcal{O}_{K_j}} E$ inherits the CM normalization condition from E, so $M \otimes_{\mathcal{O}_{K_j}} E$ is a false elliptic curve over S with complex multiplication by $\mathcal{O}_{K_j}$.

If $\Theta : \mathcal{O}_{K_j} \to \mathcal{O}_B$ is a ring homomorphism and $\widetilde{\Theta} : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_B$ is its reduction modulo $\mathfrak{m}_B$, we will sometimes write $\mathscr{Y}_j^{[\Theta]}$ for the category $\mathscr{Y}_j^{\widetilde{\Theta}}$.

Theorem 5.2.6. *Fix representatives $\Theta_1, \ldots, \Theta_m \in \mathscr{K}_j$ of the $m = 2^r$ classes in $\mathscr{K}_j'$. There is an isomorphism of stacks over* $\mathrm{Spec}(\mathcal{O}_K)$

$$f : \bigsqcup_{d=1}^{m} \mathscr{C}_j \to \mathscr{Y}_j$$

defined by $(E,d) \mapsto L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} E$. This isomorphism induces an equivalence of categories $\mathscr{C}_j \to \mathscr{Y}_j^{[\Theta]}$ for any $[\Theta] \in \mathscr{K}_j'$.

The notation (E,d) means E is an object of the d-th copy of $\mathscr{C}_j$ in the disjoint union. Therefore we obtain an isomorphism

$$\bigsqcup_{\theta_j : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_B} \mathscr{Y}_j^{\theta_j} \to \mathscr{Y}_j.$$

In particular, any $A \in \mathscr{Y}_j(S)$ is isomorphic to $L_\Theta \otimes_{\mathcal{O}_{K_j}} E$ for some $\Theta : \mathcal{O}_{K_j} \to \mathcal{O}_B$ and some $E \in \mathscr{C}_j(S)$. The theorem states that Θ is unique up to the equivalence relation $\sim$, but E and L_Θ are not necessarily unique up to isomorphism: for any nontrivial $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{K_j})$,

$$L_\Theta \otimes_{\mathcal{O}_{K_j}} E \cong (\mathfrak{a}^{-1} \otimes_{\mathcal{O}_{K_j}} L_\Theta) \otimes_{\mathcal{O}_{K_j}} (\mathfrak{a} \otimes_{\mathcal{O}_{K_j}} E),$$

with $\mathfrak{a}^{-1} \otimes_{\mathcal{O}_{K_j}} L_\Theta \ncong L_\Theta$, by what we showed above, and $\mathfrak{a} \otimes_{\mathcal{O}_{K_j}} E \ncong E$ by the elliptic curve analogue of Lemma 4.1.3.

Note that if $S = \mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{P}})$, then $A = L_\Theta \otimes_{\mathcal{O}_{K_j}} E \sim (E')^2$ for some elliptic curve E' over $\overline{\mathbb{F}}_{\mathfrak{P}}$ with E' supersingular if and only if E is supersingular. Indeed, by Theorem 4.1.1(c) there is an isomorphism of $\mathcal{O}_{K_j}$-modules

$$\mathrm{End}(A) \cong L_\Theta \otimes_{\mathcal{O}_{K_j}} \mathrm{End}(E) \otimes_{\mathcal{O}_{K_j}} L_\Theta^\vee \cong \mathrm{End}_{\mathcal{O}_{K_j}}(L_\Theta) \otimes_{\mathcal{O}_{K_j}} \mathrm{End}(E),$$

and thus there are isomorphisms of $\mathbb{Q}$-algebras

$$\mathrm{M}_2(\mathrm{End}^0(E')) \cong \mathrm{End}^0(A) \cong \mathrm{End}_{K_j}(B) \otimes_{K_j} \mathrm{End}^0(E) \cong \mathrm{M}_2(\mathrm{End}^0(E)).$$

Proof of Theorem 5.2.6. The idea of the proof is to introduce level structure to the stacks $\mathscr{C}_j$ and $\mathscr{Y}_j$, show that these new spaces are schemes, and then show f induces an isomorphism between these schemes. We begin by showing f induces a bijection on geometric points. Let $k = \mathbb{C}$ or $k = \overline{\mathbb{F}}_{\mathfrak{P}}$ and let $X \subset [\mathscr{Y}_j(k)]$ be the image of the map

$$f_k : \bigsqcup_{d=1}^{m} [\mathscr{C}_j(k)] \to [\mathscr{Y}_j(k)]$$

on k-points determined by f. The group $W_0 \times \mathrm{Cl}(\mathcal{O}_{K_j})$ acts simply transitively on the set $[\mathscr{Y}_j(k)]$ and this action preserves the subset X. Indeed,

$$\mathfrak{a} \otimes_{\mathcal{O}_{K_j}} (L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} E) \cong L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} (\mathfrak{a} \otimes_{\mathcal{O}_{K_j}} E) \in X$$

for any $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{K_j})$. Next, for any $w \in W_0$,

$$w \cdot (L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} E, i_{L_{\Theta_d}}, \kappa_{L_{\Theta_d}}) = (M \otimes_{\mathcal{O}_{K_j}} E, i_M, \kappa_M),$$

where $M = \mathcal{O}_B \in \mathscr{L}_j$, viewed as a left $\mathcal{O}_B$-module via $x \cdot y = wxw^{-1}y$ and a right $\mathcal{O}_{K_j}$-module through Θ_d. By the proof of Proposition 5.2.4, $M \cong L_{\Theta'}$ for some Θ'. Let d' be the integer such that $[\Theta'] = [\Theta_{d'}]$. Then $\Theta' = \mathfrak{a} \cdot \Theta_{d'}$ for some $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{K_j})$, so

$$w \cdot (L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} E, i_{L_{\Theta_d}}, \kappa_{L_{\Theta_d}}) \cong \mathfrak{a}^{-1} \cdot (L_{\Theta_{d'}} \otimes_{\mathcal{O}_{K_j}} E, i_{L_{\Theta_{d'}}}, \kappa_{L_{\Theta_{d'}}}) \in X.$$

This shows $X = [\mathscr{Y}_j(k)]$, so f_k is surjective. Now, it is well-known that $\mathrm{Cl}(\mathcal{O}_{K_j})$ acts simply transitively on $[\mathscr{C}_j(k)]$, and thus f_k is a bijection since

$$\# \bigsqcup_{d=1}^{m} [\mathscr{C}_j(k)] = m \cdot \#[\mathscr{C}_j(k)] = |W_0| \cdot |\,\mathrm{Cl}(\mathcal{O}_{K_j})| = \#[\mathscr{Y}_j(k)].$$

Fix an integer $n \geqslant 1$ and set $S = \mathrm{Spec}(\mathcal{O}_K)$ and $S_n = \mathrm{Spec}(\mathcal{O}_K[n^{-1}])$. For n prime to d_B define $\mathscr{Y}_j(n)$ to be the category fibered in groupoids over S_n with $\mathscr{Y}_j(n)(T)$ the category of quadruples (A, i, κ, ν) where $(A, i, \kappa) \in \mathscr{Y}_j(T)$ and

$$\nu : (\mathcal{O}_B/(n))_T \to A[n]$$

is an $\mathcal{O}_j$-linear isomorphism of schemes, where $(\mathcal{O}_B/(n))_T$ is the constant group scheme over the S_n-scheme T associated with $\mathcal{O}_B/(n)$. Here we are viewing $\mathcal{O}_B/(n)$ as a left $\mathcal{O}_B$-module through multiplication on the left and a right $\mathcal{O}_{K_j}$-module through a fixed inclusion $\mathcal{O}_{K_j} \hookrightarrow \mathcal{O}_B$ and multiplication on the right. Forgetting ν defines a finite étale representable morphism $\mathscr{Y}_j(n) \to \mathscr{Y}_j \times_S S_n$, so $\mathscr{Y}_j(n)$ is a stack, finite étale over S_n (since $\mathscr{Y}_j \times_S S_n$ is).

We claim that for $n \geqslant 3$ prime to d_B, any object of $\mathscr{Y}_j(n)$ has no nontrivial automorphisms. Let T be an S_n-scheme, let $(A, i, \kappa, \nu) \in \mathscr{Y}_j(n)(T)$, and suppose $g \in \mathrm{Aut}(A, i, \kappa, \nu)$. Set $g' = g - \mathrm{id}_A$. Since $g = \kappa(a)$ for some $a \in \mathcal{O}_{K_j}^\times$, the morphism $g' = \kappa(a-1)$ is an isogeny of false elliptic curves. Then

$$[\deg^*(g')] = (g')^t \circ g' = g^t \circ g - g^t - g + \mathrm{id}_A = 2 \cdot \mathrm{id}_A - (g^t + g),$$

so $g^t + g = [m]$, where $m = 2 - \deg^*(g')$. Hence g is a root of the polynomial $x^2 - mx + 1$ in $\mathrm{End}_T(A)[x]$. But g is a root of unity, which means $|m| \leqslant 2$ and thus $1 \leqslant \deg^*(g') \leqslant 4$. By definition of g being an automorphism of (A, i, κ, ν), the endomorphism g' kills $A[n]$, so $g' = g'' \circ [n]$ for some $g'' \in \mathrm{End}_{\mathcal{O}_B}(A)$. Then $|n^2 \deg^*(g'')| \leqslant 4$ and since $n \geqslant 3$, we must have $\deg^*(g'') = 0$ and thus $g = \mathrm{id}_A$. It follows from this fact, as in [4, proof of Corollary 2.3], that $\mathscr{Y}_j(n)$ is a scheme.

For any $n \geqslant 1$ define $\mathscr{C}_j(n)$ to be the category fibered in groupoids over S_n with $\mathscr{C}_j(n)(T)$ the category of triples (E, κ, ν) where $(E, \kappa) \in \mathscr{C}_j(T)$ and

$$\nu : (\mathcal{O}_{K_j}/(n))_T \to E[n]$$

is an $\mathcal{O}_{K_j}$-linear isomorphism of schemes. The same argument as above shows $\mathscr{C}_j(n)$ is a scheme, finite étale over S_n. Let $G_n = \mathrm{Aut}_{\mathcal{O}_{K_j}}(\mathcal{O}_{K_j}/(n)) \cong (\mathcal{O}_{K_j}/(n))^\times$. There is an action of the finite group scheme $(G_n)_{S_n}$ on the scheme $\mathscr{C}_j(n)$, defined on T-points, for any connected S_n-scheme T, by

$$g \cdot (E, \kappa, \nu) = (E, \kappa, \nu \circ g^{-1}).$$

There is an associated quotient stack $\mathscr{C}_j(n)/(G_n)_{S_n} \to S_n$, defined in [27, Example 7.17], and there is an isomorphism of stacks $\mathscr{C}_j(n)/(G_n)_{S_n} \to \mathscr{C}_j \times_S S_n$ such that the composition

$$\mathscr{C}_j(n) \to \mathscr{C}_j(n)/(G_n)_{S_n} \xrightarrow{\cong} \mathscr{C}_j \times_S S_n$$

is the morphism defined by forgetting the level structure.

Note that there is an isomorphism of groups

$$\mathrm{Aut}_{\mathcal{O}_j}(\mathcal{O}_B/(n)) \cong (\mathcal{O}_{K_j}/(n))^\times,$$

so $(G_n)_{S_n}$ also acts on $\mathscr{Y}_j(n)$, the action defined in the same way as above. As before there is an isomorphism of stacks $\mathscr{Y}_j(n)/(G_n)_{S_n} \to \mathscr{Y}_j \times_S S_n$ such that the composition

$$\mathscr{Y}_j(n) \to \mathscr{Y}_j(n)/(G_n)_{S_n} \xrightarrow{\cong} \mathscr{Y}_j \times_S S_n$$

is the forgetful morphism. The base change

$$f_n = f \times \mathrm{id} : \bigsqcup_{d=1}^{m} \mathscr{C}_j \times_S S_n \to \mathscr{Y}_j \times_S S_n$$

induces a morphism of schemes over S_n

$$f'_n : \bigsqcup_{d=1}^{m} \mathscr{C}_j(n) \to \mathscr{Y}_j(n)$$

given on T-points by $(E, \nu, d) \mapsto (L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} E, \nu')$, where ν' is the composition

$$(\mathcal{O}_B/(n))_T \cong L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} (\mathcal{O}_{K_j}/(n))_T \xrightarrow{\mathrm{id} \otimes \nu} L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} E[n] \cong (L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} E)[n]. \tag{5.2.1}$$

Let $k = \mathbb{C}$ or $k = \overline{\mathbb{F}}_{\mathfrak{P}}$ and fix a triple $(A, i, \kappa) \in \mathscr{Y}_j(k)$, so $A \cong L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} E$ for some d and some $E \in \mathscr{C}_j(k)$, by the first part of the proof. Let X be the set of all $\mathcal{O}_j$-linear isomorphisms of schemes $\nu : (\mathcal{O}_B/(n))_k \to A[n]$, where two such isomorphisms ν and ν' are considered equal in X if the objects (A, i, κ, ν) and (A, i, κ, ν') are isomorphic in $\mathscr{Y}_j(n)(k)$. The group G_n acts simply transitively on X, the action as above, and this action preserves the subset of X consisting of all ν' of the form (5.2.1) for some $\mathcal{O}_{K_j}$-linear isomorphism $\nu : (\mathcal{O}_{K_j}/(n))_k \to E[n]$ since $a \cdot (\mathrm{id} \otimes \nu) = \mathrm{id} \otimes (\nu \circ m_{a^{-1}})$ for any $a \in (\mathcal{O}_{K_j}/(n))^\times$, where $m_{a^{-1}}$ is left multiplication by a^{-1}. Combining this with the first paragraph of the proof, it follows that f'_n defines a bijection

$$(f'_n)_k : \bigsqcup_{d=1}^{m} [\mathscr{C}_j(n)(k)] \to [\mathscr{Y}_j(n)(k)].$$

(Injectivity follows from the injectivity of f_k and the fact that f is a fully faithful functor.) The morphism f'_n is $(G_n)_{S_n}$-equivariant, so there is a morphism of stacks

$$\bigsqcup_{d=1}^{m} \mathscr{C}_j(n)/(G_n)_{S_n} \to \mathscr{Y}_j(n)/(G_n)_{S_n}$$

making the diagram

$$\begin{tikzcd}
\bigsqcup_{d=1}^{m} \mathscr{C}_j(n) \arrow[r, "f'_n"] \arrow[d] & \mathscr{Y}_j(n) \arrow[d] \\
\bigsqcup_{d=1}^{m} \mathscr{C}_j(n)/(G_n)_{S_n} \arrow[r] \arrow[d, "\cong"'] & \mathscr{Y}_j(n)/(G_n)_{S_n} \arrow[d, "\cong"] \\
\bigsqcup_{d=1}^{m} \mathscr{C}_j \times_S S_n \arrow[r, "f_n"] & \mathscr{Y}_j \times_S S_n
\end{tikzcd}$$

commute. It follows that to show f_n is an isomorphism, it suffices to show f'_n is an isomorphism. The morphism f_n is finite étale since $\mathscr{C}_j$ and $\mathscr{Y}_j$ are finite étale over S. The vertical arrows in the above diagram are finite étale, so the same is true of f'_n. As f'_n is a finite étale morphism of S_n-schemes inducing a bijection on geometric points, it is an isomorphism by Lemma 5.2.7 below. Choosing relatively prime integers $n, n' \geqslant 3$ prime to d_B, the morphisms f_n and $f_{n'}$ being isomorphisms implies f is an isomorphism.

For the final statement of the theorem, let S be any $\mathcal{O}_K$-scheme and fix an integer $1 \leqslant d \leqslant m$. It follows directly from the definitions that any CM false elliptic curve of the form $L_{\Theta_d} \otimes_{\mathcal{O}_{K_j}} E$ for some $E \in \mathscr{C}_j(S)$ lies in $\mathscr{Y}_j^{[\Theta_d]}(S)$. Conversely, suppose $(A, i, \kappa) \in \mathscr{Y}_j^{[\Theta_d]}(S)$. Then $A \cong L_{\Theta_{d'}} \otimes_{\mathcal{O}_{K_j}} E$ for some $E \in \mathscr{C}_j(S)$ and a unique $1 \leqslant d' \leqslant m$ as f is an isomorphism, so the diagram

$$\begin{tikzcd}
\mathcal{O}_{K_j} \arrow[rr, "\kappa^{\mathfrak{m}_B}"] \arrow[dr, "\eta"'] & & \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(A[\mathfrak{m}_B]) \\
& \mathcal{O}_B/\mathfrak{m}_B \arrow[ur] &
\end{tikzcd}$$

commutes for $\eta = \widetilde{\Theta}_d$ and $\eta = \widetilde{\Theta}_{d'}$. Picking any geometric point $\overline{s} : \mathrm{Spec}(k) \to S$, the above diagram still commutes with A replaced with $A_{\overline{s}}$. But the map

$$\mathcal{O}_B/\mathfrak{m}_B \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(A_{\overline{s}}[\mathfrak{m}_B])$$

is an isomorphism by Corollary 7.2.9, proved below only using the first paragraph of this proof (that f is a bijection on geometric points). Therefore $\widetilde{\Theta}_d = \widetilde{\Theta}_{d'}$, so $d = d'$, which shows f defines an equivalence of categories $\mathscr{C}_j \to \mathscr{Y}_j^{[\Theta_d]}$. □

Lemma 5.2.7. *Let S be a scheme, let X and Y be S-schemes, and suppose $f : X \to Y$ is a finite étale S-morphism such that the induced map $X(k) \to Y(k)$ is a bijection for any geometric point* $\mathrm{Spec}(k) \to S$. *Then f is an isomorphism.*

Proof. Since f is surjective on geometric points, $f(X)$ has a nonempty intersection with every connected component of Y. As f is finite flat, the set $f(X) \subset Y$ is both open and closed, so $f(X) = Y$. Also, there is the usual notion of the degree of f, defined as the rank of the locally free $\mathscr{O}_Y$-module $f_*\mathscr{O}_X$. To show $\deg(f) = 1$, we can check this at a geometric point in each connected component of S, so we may assume $S = \mathrm{Spec}(k)$ for k an algebraically closed field. If $y \in Y(k)$, viewed as a closed point of Y, then since $X(k) \to Y(k)$ is injective, there is a unique point $x \in X(k)$ in the fiber $f^{-1}(y)$. As f is unramified and $k(x) = k(y) = k$, we have $\deg(f) = 1$ ([9, Proposition 12.21]) and therefore f is an isomorphism. □

Corollary 5.2.8. *Suppose S is an $\mathcal{O}_K$-scheme and let $(A, i, \kappa) \in \mathscr{Y}_j(S)$. Then the trace of $i(x)$ acting on* $\mathrm{Lie}(A)$ *is equal to* $\mathrm{Trd}(x)$ *for any $x \in \mathcal{O}_B$.*

What this means is that each point of S has an affine open neighborhood $\mathrm{Spec}(R) \to S$ such that the trace of $i(x)$ acting on the free R-module $\mathrm{Lie}(A_{/R})$ is equal to $\mathrm{Trd}(x)$ for any $x \in \mathcal{O}_B$.

Proof. We have $A \cong M \otimes_{\mathcal{O}_{K_j}} E$ for some $\mathcal{O}_j$-module M and $E \in \mathscr{C}_j(S)$. Then $\mathrm{Lie}(A) \cong M \otimes_{\mathcal{O}_{K_j}} \mathrm{Lie}(E)$ as $\mathcal{O}_j$-modules, with $\mathcal{O}_B$ acting on $M \otimes_{\mathcal{O}_{K_j}} \mathrm{Lie}(E)$ through its action on M. As $M \cong \mathcal{O}_B$ as a left $\mathcal{O}_B$-module, the result easily follows. □

Corollary 5.2.9. *Suppose $\widetilde{R} \to R$ is a surjection of $\mathcal{O}_K$-algebras, $x = (A, i, \kappa) \in \mathscr{Y}_j(R)$, and $\widetilde{x} = (\widetilde{A}, \widetilde{i}, \widetilde{\kappa}) \in \mathscr{Y}_j(\widetilde{R})$ is a deformation of x. Then $x \in \mathscr{Y}_j^{\theta_j}(R)$ if and only if $\widetilde{x} \in \mathscr{Y}_j^{\theta_j}(\widetilde{R})$.*

Proof. First suppose $x \in \mathscr{Y}_j^{\theta_j}(R)$. We know $\widetilde{x} \in \mathscr{Y}_j^{\eta}(\widetilde{R})$ for a unique $\eta : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_B$, so the diagram

$$\begin{tikzcd}
\mathcal{O}_{K_j} \arrow[rr, "\widetilde{\kappa}^{\mathfrak{m}_B}"] \arrow[dr, "\eta"'] & & \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(\widetilde{A}[\mathfrak{m}_B]) \\
& \mathcal{O}_B/\mathfrak{m}_B \arrow[ur, "\widetilde{i}^{\mathfrak{m}_B}"'] &
\end{tikzcd} \tag{5.2.2}$$

commutes, where $\widetilde{\kappa}^{\mathfrak{m}_B}$ and $\widetilde{i}^{\mathfrak{m}_B}$ are the maps induced by $\widetilde{\kappa}$ and $\widetilde{i}$. Since $\widetilde{x}$ is a deformation of x, it follows that the diagram

$$\begin{tikzcd}
\mathcal{O}_{K_j} \arrow[rr, "\kappa^{\mathfrak{m}_B}"] \arrow[dr, "\eta"'] & & \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(A[\mathfrak{m}_B]) \\
& \mathcal{O}_B/\mathfrak{m}_B \arrow[ur, "i^{\mathfrak{m}_B}"'] &
\end{tikzcd} \tag{5.2.3}$$

commutes. But $x \in \mathscr{Y}_j^{\theta_j}(R)$ implies this diagram also commutes with θ_j in place of η, so $\eta = \theta_j$ as in the last part of the proof of Theorem 5.2.6. Conversely, if $\widetilde{x} \in \mathscr{Y}_j^{\theta_j}(\widetilde{R})$ then (5.2.2) commutes with θ_j in place of η, so as before it follows that (5.2.3) commutes with θ_j in place of η and hence $x \in \mathscr{Y}_j^{\theta_j}(R)$. □

Chapter 6

Tate and Dieudonné modules

6.1 The Tate module

Let A be a false elliptic curve over a field k and let $\ell \neq \mathrm{char}(k)$ be a prime number. For any $x \in \mathcal{O}_B$ the endomorphism $i(x) \in \mathrm{End}(A)$ induces an endomorphism $i(x)_n : A[\ell^n] \to A[\ell^n]$ for each $n \geqslant 1$, and these maps are compatible with the maps $[\ell] : A[\ell^{n+1}] \to A[\ell^n]$. Hence there is an induced endomorphism $i(x) : T_\ell(A) \to T_\ell(A)$ on ℓ-adic Tate modules, and thus $T_\ell(A)$ is a left $\mathcal{O}_B$-module.

Lemma 6.1.1. *Let ℓ be a prime number and suppose A_1 and A_2 are false elliptic curves over $\overline{\mathbb{F}}_p$ for $p \neq \ell$.*
(a) *Suppose $\ell \nmid d_B$ and set*

$$\varepsilon = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \varepsilon' = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

in $\mathrm{M}_2(\mathbb{Z}_\ell) \cong \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. There are isomorphisms of $\mathbb{Z}_\ell$-modules

$$\mathrm{Hom}_{\mathcal{O}_B}(T_\ell(A_1), T_\ell(A_2)) \cong \mathrm{Hom}_{\mathbb{Z}_\ell}(\varepsilon T_\ell(A_1), \varepsilon T_\ell(A_2)) \cong \mathrm{M}_2(\mathbb{Z}_\ell),$$

where $\mathrm{Hom}_{\mathcal{O}_B}(T_\ell(A_1), T_\ell(A_2))$ is the set of $\mathbb{Z}_\ell$-linear maps $T_\ell(A_1) \to T_\ell(A_2)$ that are also $\mathcal{O}_B$-linear. If $A_1 = A_2$ then these are isomorphisms of rings.
(b) *If $\ell \mid d_B$ then there is an isomorphism of $\mathbb{Z}_\ell$-modules*

$$\mathrm{Hom}_{\mathcal{O}_B}(T_\ell(A_1), T_\ell(A_2)) \cong \mathcal{O}_{B,\ell},$$

which is an isomorphism of rings if $A_1 = A_2$.

Proof. (a) For $j = 1, 2$ write T_j for $T_\ell(A_j)$. From $T_j = \varepsilon T_j \oplus \varepsilon' T_j$, there is an inclusion

$$\mathrm{Hom}_{\mathcal{O}_B}(T_1, T_2) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(\varepsilon T_1, \varepsilon T_2) \oplus \mathrm{Hom}_{\mathbb{Z}_\ell}(\varepsilon' T_1, \varepsilon' T_2)$$

since any $f \in \mathrm{Hom}_{\mathcal{O}_B}(T_1, T_2)$ is $\mathrm{M}_2(\mathbb{Z}_\ell)$-linear and hence satisfies $f(\varepsilon x) = \varepsilon f(x)$ and $f(\varepsilon' x) = \varepsilon' f(x)$ for all $x \in T_1$. Denote the above map by $f \mapsto (f_\varepsilon, f_{\varepsilon'})$. Now let

$$w = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}_\ell),$$

so $w\varepsilon w = \varepsilon'$. Then for any $x \in T_1$,

$$f_{\varepsilon'}(\varepsilon' x) = f(\varepsilon' x) = f(w\varepsilon w x) = w f(\varepsilon w x) = w f_\varepsilon(\varepsilon w x),$$

which shows f_ε determines $f_{\varepsilon'}$. Therefore the above map is really an inclusion

$$\mathrm{Hom}_{\mathcal{O}_B}(T_1, T_2) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(\varepsilon T_1, \varepsilon T_2).$$

To show this map is surjective, let $f_\varepsilon \in \mathrm{Hom}_{\mathbb{Z}_\ell}(\varepsilon T_1, \varepsilon T_2)$. Define $f_{\varepsilon'} \in \mathrm{Hom}_{\mathbb{Z}_\ell}(\varepsilon' T_1, \varepsilon' T_2)$ by $f_{\varepsilon'}(\varepsilon' x) = w f_\varepsilon(\varepsilon w x)$, and define $f : T_1 \to T_2$ by $f = f_\varepsilon \oplus f_{\varepsilon'}$. By construction f is $\mathbb{Z}_\ell$-linear. To see that f is $\mathrm{M}_2(\mathbb{Z}_\ell)$-linear, first note that since $\varepsilon^2 = \varepsilon$, $(\varepsilon')^2 = \varepsilon'$, and $\varepsilon\varepsilon' = \varepsilon'\varepsilon = 0$, we have $f(\varepsilon x) = \varepsilon f(x)$ and $f(\varepsilon' x) = \varepsilon' f(x)$ for all $x \in T_1$. Next,

$$\begin{aligned} f(\varepsilon' x) = \varepsilon' f(x) &\implies f(\varepsilon' x) = w\varepsilon w f(x) \\ &\implies w f(\varepsilon' x) = \varepsilon w f(x) \\ &\implies f(\varepsilon w x) = \varepsilon w f(x) \end{aligned}$$

and

$$f(\varepsilon' w x) = w f(\varepsilon x) = w\varepsilon f(x) = \varepsilon' w f(x).$$

As

$$\varepsilon w = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad \varepsilon' w = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},$$

this shows that f is $\mathrm{M}_2(\mathbb{Z}_\ell)$-linear, and maps to f_ε in the above inclusion. The isomorphism $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_1, T_2) \cong \mathrm{M}_2(\mathbb{Z}_\ell)$ comes from choosing $\mathbb{Z}_\ell$-bases for εT_1 and εT_2.

(b) Since $\ell \mid d_B$, B_ℓ is a quaternion division algebra over $\mathbb{Q}_\ell$, and from $T_j = T_\ell(A_j)$ being free of rank 4 as a $\mathbb{Z}_\ell$-module, $T_j \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a free B_ℓ-module of rank 1. Choosing a generator, we obtain an isomorphism of B_ℓ-modules $T_j \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong B_\ell$, which identifies T_j with a finitely generated $\mathcal{O}_{B,\ell}$-

submodule of B_ℓ. Multiplying T_j by a suitably large power of ℓ gives an isomorphism of T_j with a finitely generated $\mathcal{O}_{B,\ell}$-submodule of $\mathcal{O}_{B,\ell}$, that is, a left ideal in $\mathcal{O}_{B,\ell}$. Since all ideals of $\mathcal{O}_{B,\ell}$ are principal, $T_j \cong \mathcal{O}_{B,\ell}$ as a left $\mathcal{O}_{B,\ell}$-module. Hence

$$\mathrm{Hom}_{\mathcal{O}_B}(T_1, T_2) \cong \mathrm{End}_{\mathcal{O}_{B,\ell}}(\mathcal{O}_{B,\ell}) \cong \mathcal{O}_{B,\ell}^{\mathrm{op}} \cong \mathcal{O}_{B,\ell}$$

as $\mathbb{Z}_\ell$-modules, where the isomorphism $\mathcal{O}_{B,\ell} \to \mathcal{O}_{B,\ell}^{\mathrm{op}}$ is given by the main involution. □

Lemma 6.1.2. *Let A_1 and A_2 be supersingular false elliptic curves over $\overline{\mathbb{F}}_p$. For any prime $\ell \neq p$ the natural map*

$$\Phi : \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathcal{O}_B}(T_\ell(A_1), T_\ell(A_2))$$

is an isomorphism of $\mathbb{Z}_\ell$-modules, and is an isomorphism of rings if $A_1 = A_2$.

Proof. For $j = 1, 2$ write T_j for $T_\ell(A_j)$, and let $M = \mathrm{im}(\Phi)$. We claim $\mathrm{Hom}_{\mathcal{O}_B}(T_1, T_2)/M$ is a torsion-free $\mathbb{Z}_\ell$-module. Suppose $f \in \mathrm{Hom}_{\mathcal{O}_B}(T_1, T_2)$ satisfies $\ell f \in M$. Then $\ell f = \Phi(\varphi)$ for some $\varphi \in \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, which means φ vanishes on $A_1[\ell](\overline{\mathbb{F}}_p)$. Hence $(\ker \varphi)(\overline{\mathbb{F}}_p) \supset (\ker [\ell])(\overline{\mathbb{F}}_p)$, and thus there is a $\varphi' \in \mathrm{Hom}(A_1, A_2)$ such that $\varphi = \varphi' \circ [\ell] = \ell\varphi'$. (This comes from viewing A_1 as the quotient $A_1/\ker([\ell])$, either in the sense of [19, §12, Corollary 1] or viewing it in the category of *fppf* sheaves of abelian groups on $\mathbf{Sch}/\overline{\mathbb{F}}_p$.) Note that φ being $\mathcal{O}_B$-linear implies φ' is also $\mathcal{O}_B$-linear. Then $\ell\Phi(\varphi') = \Phi(\ell\varphi') = \Phi(\varphi) = \ell f$, so $f = \Phi(\varphi') \in M$ since $\mathrm{Hom}_{\mathcal{O}_B}(T_1, T_2)$ is a torsion-free $\mathbb{Z}_\ell$-module.

As A_1 and A_2 are supersingular, $\mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is a free $\mathbb{Z}_\ell$-module of rank 4 (it is a lattice in $\mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \cong \mathrm{End}_{\mathcal{O}_B}(A_1) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \cong B_\ell^{(p)}$, where the first isomorphism comes from choosing an isogeny $A_1 \to A_2$ of false elliptic curves). By Lemma 6.1.1 we see that the same is true of $\mathrm{Hom}_{\mathcal{O}_B}(T_1, T_2)$, and therefore Φ is an isomorphism. □

6.2 The Dieudonné module

Fix a prime number p and let $W = W(\overline{\mathbb{F}}_p)$ be the ring of Witt vectors over $\overline{\mathbb{F}}_p$, so W is the ring of integers in the completion of the maximal unramified extension of $\mathbb{Q}_p$. If A is a false elliptic curve over $\overline{\mathbb{F}}_p$, we write $D(A)$ for the covariant Dieudonné module of A (that is, the Dieudonné module of $A[p^\infty]$), which is a module over the Dieudonné ring $\mathscr{D}$, free of rank 4 over W. Recall that there is a unique continuous ring automorphism σ of W inducing the absolute Frobenius $x \mapsto x^p$ on $W/pW \cong \overline{\mathbb{F}}_p$, and $\mathscr{D} = W\{\mathscr{F}, \mathscr{V}\}/(\mathscr{F}\mathscr{V} - p)$ where $W\{\mathscr{F}, \mathscr{V}\}$ is the non-commutative polynomial ring in two commuting variables $\mathscr{F}$ and $\mathscr{V}$ satisfying $\mathscr{F}x = \sigma(x)\mathscr{F}$ and $\mathscr{V}x = \sigma^{-1}(x)\mathscr{V}$ for all $x \in W$. The action of $\mathcal{O}_B$ on A induces an action of $\mathcal{O}_B$ on $D(A)$ which commutes with the action of $\mathscr{D}$. For any false elliptic curves A_1 and A_2 over $\overline{\mathbb{F}}_p$ there is an isomorphism of $\mathbb{Z}$-modules

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) \cong \mathrm{Hom}_{\mathcal{O}_B}(A_1[p^\infty], A_2[p^\infty]),$$

which is an isomorphism of rings if $A_1 = A_2$.

If E is an elliptic curve over $\overline{\mathbb{F}}_p$ then its covariant Dieudonné module $D(E)$ is a $\mathscr{D}$-module, free of rank 2 over W, and there is an isomorphism

$$\mathrm{Hom}_{\mathscr{D}}(D(E_1), D(E_2)) \cong \mathrm{Hom}(E_1[p^\infty], E_2[p^\infty])$$

for any E_1 and E_2 over $\overline{\mathbb{F}}_p$. If E is a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ then the natural map

$$\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathrm{End}_{\mathscr{D}}(D(E)) \cong \Delta$$

is an isomorphism of $\mathbb{Z}_p$-algebras, where Δ is the unique maximal order in the quaternion division algebra over $\mathbb{Q}_p$, by a proof very similar to that of Lemma 6.1.2.

Lemma 6.2.1. *Let A_1 and A_2 be false elliptic curves over $\overline{\mathbb{F}}_p$. Suppose $p \nmid d_B$ and set*

$$\varepsilon = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

in $\mathrm{M}_2(W) \cong \mathrm{M}_2(\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} W \cong \mathcal{O}_B \otimes_{\mathbb{Z}} W$. There is an isomorphism of W-modules

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W}(D(A_1), D(A_2)) \cong \mathrm{Hom}_W(\varepsilon D(A_1), \varepsilon D(A_2)) \cong \mathrm{M}_2(W),$$

which is an isomorphism of rings if $A_1 = A_2$. In particular, if A_1 and A_2 are supersingular, then

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) \cong \Delta.$$

Proof. The proof of the first part is identical to that of Lemma 6.1.1(a), replacing $\mathbb{Z}_\ell$-linearity with W-linearity. For the in particular statement, note that

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) = \{\varphi \in \mathrm{M}_2(W) : \mathscr{F}\varphi = \varphi^\sigma \mathscr{F},\ \mathscr{V}\varphi = \varphi^{\sigma^{-1}} \mathscr{V}\},$$

where φ^σ is the matrix obtained by applying σ to all of the entries. Since A_j is supersingular, $\varepsilon D(A_j)$ is free of rank of 2 over W with basis $\{e_1, e_2\}$ satisfying $\mathscr{F}(e_1) = \mathscr{V}(e_1) = e_2$ and $\mathscr{F}(e_2) =$

$\mathscr{V}(e_2) = pe_1$. A computation in coordinates then shows

$$\{\varphi \in \mathrm{M}_2(W) : \mathscr{F}\varphi = \varphi^\sigma \mathscr{F},\ \mathscr{V}\varphi = \varphi^{\sigma^{-1}}\mathscr{V}\} = \left\{ \begin{bmatrix} a & pb \\ \bar{b} & \bar{a} \end{bmatrix} : a, b \in \mathbb{Z}_{p^2} \right\} \cong \Delta. \qquad \square$$

Lemma 6.2.2. *If A_1 and A_2 are supersingular false elliptic curves over $\overline{\mathbb{F}}_p$, then the natural map*

$$\mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2))$$

is an isomorphism of $\mathbb{Z}_p$-modules, and is an isomorphism of rings if $A_1 = A_2$.

Proof. The proof is very similar to that of Lemma 6.1.2, using the following fact: the group $H = \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2))$ is a free $\mathbb{Z}_p$-module of rank 4. To see this, consider the $\mathbb{Q}_p$-vector space $H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Since $D(A_1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong D(A_2) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ as $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}$-modules,

$$H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

As $A_1 \sim E_1^2$ for some supersingular elliptic curve E_1, we have $D(A_1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong D(E_1)^2 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ as $\mathscr{D}$-modules and thus there are isomorphisms

$$\begin{aligned} \mathrm{End}_{\mathscr{D}}(D(A_1)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p &\cong \mathrm{M}_2(\mathrm{End}_{\mathscr{D}}(D(E_1))) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathrm{M}_2(\mathrm{End}(E_1)) \otimes_{\mathbb{Z}} \mathbb{Q}_p \\ &\cong \mathrm{End}(A_1) \otimes_{\mathbb{Z}} \mathbb{Q}_p. \end{aligned}$$

Taking centralizers of $\mathcal{O}_B$ in each ring shows $H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathrm{End}_{\mathcal{O}_B}(A_1) \otimes_{\mathbb{Z}} \mathbb{Q}_p$ has dimension 4 as a $\mathbb{Q}_p$-vector space. □

6.3 CM false elliptic curves

Within the context of CM false elliptic curves we can be more specific about the Tate and Dieudonné modules. Let $A \in \mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})$, so $A \cong M \otimes_{\mathcal{O}_{K_j}} E$ for some $E \in \mathscr{C}_j(\overline{\mathbb{F}}_{\mathfrak{P}})$ and some module M over $\mathcal{O}_j = \mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_{K_j}$, free of rank 4 over $\mathbb{Z}$. Let p be the rational prime below $\mathfrak{P}$. For any prime $\ell \neq p$ there is an isomorphism of $\mathcal{O}_{j,\ell}$-modules

$$T_\ell(A) \cong M_\ell \otimes_{\mathcal{O}_{K_j,\ell}} T_\ell(E),$$

where $\mathcal{O}_{j,\ell}$ acts through its action on M_ℓ. Similarly, there is an isomorphism of $W \otimes_{\mathbb{Z}_p} \mathcal{O}_{j,p}$-modules

$$D(A) \cong M_p \otimes_{\mathcal{O}_{K_j,p}} D(E).$$

However, $M_p \cong \mathcal{O}_{K_j,p} \oplus \mathcal{O}_{K_j,p}$ as $\mathcal{O}_{K_j,p}$-modules and thus $D(A) \cong D(E) \oplus D(E)$ as modules over $W \otimes_{\mathbb{Z}_p} \mathcal{O}_{K_j,p}$, where $\mathcal{O}_{K_j,p}$ acts on $D(E) \oplus D(E)$ diagonally through its action on $D(E)$. We still have to determine the possibilities for the actions of $\mathcal{O}_{B,p}$ and $\mathscr{D}$ on $D(A)$. The next proposition does this for $\mathcal{O}_{B,p}$, where $p \mid d_B$.

Proposition 6.3.1. *Suppose $A \in \mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})$ for $p \mid d_B$, with $A \cong M \otimes_{\mathcal{O}_{K_j}} E$ for some supersingular E. Fix an isomorphism $\mathcal{O}_{B,p} \cong \Delta$ and a uniformizer $\Pi \in \Delta$ satisfying $\Pi^2 = p$ and $\Pi a = \overline{a}\Pi$ for all $a \in \mathbb{Z}_{p^2}$, where we are viewing $\mathbb{Z}_{p^2} \hookrightarrow \Delta$ through the CM action $\mathcal{O}_{K_j,p} \to \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Then there is an isomorphism of rings $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong R_{11}$, where*

$$R_{11} = \left\{ \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix} : x, y \in \mathbb{Z}_{p^2} \right\} \subset \mathrm{M}_2(\Delta).$$

Proof. We have the Δ-action on $D(A)$

$$D(i) : \Delta \to \mathrm{End}_{\mathcal{O}_{K_j} \otimes_{\mathbb{Z}} \mathscr{D}}(D(A)) \cong \mathrm{M}_2(\mathrm{End}_{\mathcal{O}_{K_j} \otimes_{\mathbb{Z}} \mathscr{D}}(D(E))) \cong \mathrm{M}_2(\mathcal{O}_{K_j,p}) = \mathrm{M}_2(\mathbb{Z}_{p^2}).$$

Here we are viewing $\mathrm{M}_2(\mathbb{Z}_{p^2}) \subset \mathrm{M}_2(\Delta)$ through the inclusion $\mathbb{Z}_{p^2} \hookrightarrow \Delta$. By Lemma 5.2.2 there are two possibilities for $D(i)$ up to $\mathrm{GL}_2(\mathbb{Z}_{p^2})$-conjugacy, f_1 and f_2, and we may assume $D(i)$ is equal to f_1 or f_2 in computing

$$\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A)) \cong C_{\mathrm{M}_2(\Delta)}(\Delta).$$

First suppose $D(i) = f_1$. Then a computation shows

$$\begin{bmatrix} a_1 + b_1\Pi & a_2 + b_2\Pi \\ a_3 + b_3\Pi & a_4 + b_4\Pi \end{bmatrix} \in \mathrm{M}_2(\Delta)$$

commutes with $f_1(x)$ for all $x \in \Delta$ if and only if $a_1 = a_4, b_1 = b_4 = a_2 = a_3 = 0$, and $pb_2 = b_3$, giving $C_{\mathrm{M}_2(\Delta)}(\Delta) = R_{11}$.

Now suppose $D(i) = f_2$. Then a computation shows

$$\begin{bmatrix} a_1 + b_1\Pi & a_2 + b_2\Pi \\ a_3 + b_3\Pi & a_4 + b_4\Pi \end{bmatrix} \in \mathrm{M}_2(\Delta)$$

commutes with $f_2(x)$ for all $x \in \Delta$ if and only if $a_1 = a_4, b_1 = b_4 = a_2 = a_3 = 0$, and $pb_3 = b_2$, giving $C_{\mathrm{M}_2(\Delta)}(\Delta) = R_{22}$, where

$$R_{22} = \left\{ \begin{bmatrix} x & py\Pi \\ y\Pi & x \end{bmatrix} : x, y \in \mathbb{Z}_{p^2} \right\}.$$

However,

$$T\begin{bmatrix} x & py\Pi \\ y\Pi & x \end{bmatrix}T^{-1} = \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix}$$

with

$$T = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Q}_{p^2})$$

and therefore $R_{22} \cong R_{11}$ as rings. □

We know that for $p \mid d_B$ there are two isomorphism classes of modules over $W \otimes_{\mathbb{Z}_p} \mathcal{O}_{j,p}$ that are free of rank 4 over W, and the proof of the previous proposition gives us explicit coordinates for each of these modules (which we will use for the $W \otimes_{\mathbb{Z}_p} \mathcal{O}_{j,p}$-module $D(A)$). To describe this, identify Δ with a subring of $\mathrm{M}_2(\mathbb{Z}_{p^2}) \subset \mathrm{M}_2(W)$ by

$$a + b\Pi \mapsto \begin{bmatrix} a & pb \\ \overline{b} & \overline{a} \end{bmatrix}, \tag{6.3.1}$$

and use this to view $\mathbb{Z}_{p^2} \subset \Delta$ inside $\mathrm{M}_2(\mathbb{Z}_{p^2})$. Then there is a basis $\{e_n\}$ for the free of rank 4 W-module $D(A) \cong D(E) \oplus D(E)$ relative to which the Δ-action on $D(A)$ is given by one of the two maps $f_1, f_2 : \Delta \to \mathrm{End}_W(D(A)) \cong \mathrm{M}_4(W)$ of Lemma 5.2.2:

$$f_1(a + b\Pi) = \begin{bmatrix} a & 0 & b & 0 \\ 0 & \overline{a} & 0 & \overline{b} \\ p\overline{b} & 0 & \overline{a} & 0 \\ 0 & pb & 0 & a \end{bmatrix}, \quad f_2(a + b\Pi) = \begin{bmatrix} a & 0 & pb & 0 \\ 0 & \overline{a} & 0 & p\overline{b} \\ \overline{b} & 0 & \overline{a} & 0 \\ 0 & b & 0 & a \end{bmatrix}. \tag{6.3.2}$$

Note that (6.3.1) comes from choosing a basis $\{v_1, v_2\}$ of $D(E)$ with $\mathscr{F} = \mathscr{V}$ satisfying $\mathscr{F}(v_1) = v_2$ and $\mathscr{F}(v_2) = pv_1$, so $\mathscr{F} = \mathscr{V}$ on $D(A)$ and

$$\mathscr{F}(e_1) = e_2, \quad \mathscr{F}(e_2) = pe_1, \quad \mathscr{F}(e_3) = e_4, \quad \mathscr{F}(e_4) = pe_3.$$

The action of $\mathcal{O}_{K_j,p} \cong \mathbb{Z}_{p^2}$ on $D(A)$ is necessarily given in this basis by

$$a \mapsto \mathrm{diag}(a, \overline{a}, a, \overline{a}). \tag{6.3.3}$$

Furthermore, using the basis $\{e_n\}$ to view

$$R_{11} \cong \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A)) \subset \mathrm{M}_4(W),$$

we can express any

$$f = \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix} \in R_{11}$$

as an element of $\mathrm{M}_4(W)$ by

$$f = \begin{bmatrix} x & 0 & 0 & py \\ 0 & \overline{x} & \overline{y} & 0 \\ 0 & p^2 y & x & 0 \\ p\overline{y} & 0 & 0 & \overline{x} \end{bmatrix}. \tag{6.3.4}$$

Combining everything, we have proved the following.

Proposition 6.3.2. *With notation as above, there is a W-basis $\{e_1, e_2, e_3, e_4\}$ for $D(A)$ relative to which the action of Δ on $D(A)$ is given by one of the matrices* (6.3.2)*, the action of $\mathcal{O}_{K_j,p}$ is given by* (6.3.3)*, the action of $\mathscr{F} = \mathscr{V}$ is determined by*

$$\mathscr{F}(e_1) = e_2, \quad \mathscr{F}(e_2) = pe_1, \quad \mathscr{F}(e_3) = e_4, \quad \mathscr{F}(e_4) = pe_3,$$

and any $f \in \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A))$ is given by a matrix of the form (6.3.4)*.*

Proposition 6.3.1 gives a description of $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ in terms of coordinates, which is best suited for computations. The next result gives the abstract structure of this ring.

Proposition 6.3.3. *There is an isomorphism of rings $R_{11} \cong R_2$, where*

$$R_2 = \begin{bmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^2\mathbb{Z}_p & \mathbb{Z}_p \end{bmatrix}$$

is the standard Eichler order of level 2 *in* $\mathrm{M}_2(\mathbb{Q}_p)$*.*

Proof. This proof is identical to a calculation carried out in [8, pp. 26-27]. We will explain the main case. For $p \neq 2$ write $\mathbb{Z}_{p^2} = \mathbb{Z}_p + \mathbb{Z}_p t$ where $t^2 \in \mathbb{Z}_p^\times$ and $\overline{t} = -t$. Then R_{11} has a $\mathbb{Z}_p$-basis $\{e_1, e_2, e_3, e_4\}$, where

$$e_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad e_2 = \begin{bmatrix} t & 0 \\ 0 & t \end{bmatrix}, \quad e_3 = \begin{bmatrix} 0 & \Pi \\ p\Pi & 0 \end{bmatrix}, \quad e_4 = \begin{bmatrix} 0 & t\Pi \\ pt\Pi & 0 \end{bmatrix},$$

so $e_2^2 = t^2 I$, $e_3^2 = p^2 I$, and $e_2 e_3 = -e_3 e_2 = e_4$. Using this basis, one shows $\mathrm{disc}(R_{11}) = p^4$. Now let $R = \mathbb{Z}_p[E_j]$ where $E_1 = e_1, E_2 = e_2, E_3 = p^{-1}e_3, E_4 = p^{-1}e_4$, so $E_2^2 = t^2 I$, $E_3^2 = I$, and $E_2 E_3 = -E_3 E_2 = E_4$. Then R is an order in $\mathrm{M}_2(\mathbb{Q}_p)$ and there is an isomorphism of rings $R \to \mathrm{M}_2(\mathbb{Z}_p)$ given by

$$E_2 \mapsto \begin{bmatrix} 0 & t^2 \\ 1 & 0 \end{bmatrix}, \quad E_3 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad E_4 \mapsto \begin{bmatrix} 0 & t^2 \\ -1 & 0 \end{bmatrix}.$$

Under this map R_{11} is mapped isomorphically to the order in $\mathrm{M}_2(\mathbb{Q}_p)$ with $\mathbb{Z}_p$-basis

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \quad \begin{bmatrix}0 & t^2\\ 1 & 0\end{bmatrix}, \quad \begin{bmatrix}p & 0\\ 0 & -p\end{bmatrix}, \quad \begin{bmatrix}0 & pt^2\\ -p & 0\end{bmatrix},$$

which means

$$R_{11} \cong \left\{ \begin{bmatrix}a & b\\ c & d\end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}_p) : p \mid (a-d), p \mid (b-t^2c) \right\}.$$

For

$$M = \begin{bmatrix}1 & t\\ t^{-1} & -1\end{bmatrix}$$

we have

$$2M^{-1}\begin{bmatrix}a & b\\ c & d\end{bmatrix}M = \begin{bmatrix}a+t^{-1}b+tc+d & t(a-d)+t^2c-b\\ t^{-1}(a-d)+t^{-2}(b-t^2c) & a-t^{-1}b-tc+d\end{bmatrix},$$

so, as $2 \in \mathbb{Z}_p^\times$, R_{11} embeds as a subring of

$$\begin{bmatrix}\mathbb{Z}_{p^2} & p\mathbb{Z}_{p^2}\\ p\mathbb{Z}_{p^2} & \mathbb{Z}_{p^2}\end{bmatrix}.$$

However, R_{11} is already a suborder of $\mathrm{M}_2(\mathbb{Z}_p)$, so R_{11} must be isomorphic to a suborder of

$$R' = \begin{bmatrix}\mathbb{Z}_p & p\mathbb{Z}_p\\ p\mathbb{Z}_p & \mathbb{Z}_p\end{bmatrix}.$$

But $\mathrm{disc}(R_{11}) = p^4 = \mathrm{disc}(R')$, and thus $R_{11} \cong R'$. Conjugating by the matrix

$$\begin{bmatrix}0 & p^{-1}\\ 1 & 0\end{bmatrix}$$

then shows $R_{11} \cong R_2$. The case $p = 2$ is similar; see [8, p. 27] for the details. □

Chapter 7

Local quadratic spaces

This chapter and the next form the technical core of this thesis. In this chapter we (essentially) count the number of geometric points of $\mathscr{X}_{\theta,\alpha}$. This comes from a careful examination of the quadratic spaces $(V_\ell(\mathbf{A}_1, \mathbf{A}_2), \deg_{\mathrm{CM}})$ for each prime ℓ. The methods of the proofs follow [14] quite closely.

Fix a prime ideal $\mathfrak{P} \subset \mathcal{O}_K$ of residue characteristic p, where p is nonsplit in K_1 and K_2, a ring homomorphism $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$, and a CM pair $(\mathbf{A}_1, \mathbf{A}_2) \in \mathscr{X}_\theta(\overline{\mathbb{F}}_\mathfrak{P})$ (necessarily supersingular), where $\mathbb{F}_\mathfrak{P} = \mathcal{O}_K/\mathfrak{P}$. For $j \in \{1, 2\}$ recall that $\kappa_j : \mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B}(A_j)$ is the CM action. Suppose ℓ is a prime dividing d_B and let $\mathfrak{m}_\ell$ be the unique maximal ideal of $\mathcal{O}_B$ with residue characteristic ℓ, so $\mathcal{O}_B/\mathfrak{m}_\ell$ is a finite field with ℓ^2 elements. Define the $\mathfrak{m}_\ell$-torsion $A_j[\mathfrak{m}_\ell]$ as the group scheme

$$A_j[\mathfrak{m}_\ell] = \ker(i_j(x_\ell) : A_j[\ell] \to A_j[\ell]),$$

where x_ℓ is any element of $\mathfrak{m}_\ell$ whose image generates the principal ideal $\mathfrak{m}_\ell/\ell\mathcal{O}_B \subset \mathcal{O}_B/\ell\mathcal{O}_B$. This is a finite flat commutative group scheme over $\mathrm{Spec}(\overline{\mathbb{F}}_\mathfrak{P})$ of order

$$\deg(i_j(x_\ell) : A_j[\ell] \to A_j[\ell]) = \deg(i_j(\Pi) : A_j \to A_j) = \mathrm{Nrd}(\Pi)^2 = \ell^2,$$

where $\Pi \in \mathcal{O}_{B,\ell}$ is any uniformizer. There is a natural action of $\mathcal{O}_B/\mathfrak{m}_\ell$ on $A_j[\mathfrak{m}_\ell]$ given on points by $\overline{x} \cdot a = i_j(x)(a)$ for $\overline{x} \in \mathcal{O}_B/\mathfrak{m}_\ell$ and $a \in A_j[\mathfrak{m}_\ell](T)$ for any $\overline{\mathbb{F}}_\mathfrak{P}$-scheme T.

7.1 The case of $\ell \neq p$

Lemma 7.1.1. *Suppose $(A, i) \in \mathscr{Y}_j(k)$ for $k = \mathbb{C}$ or $k = \overline{\mathbb{F}}_p$ and $\ell \neq p$ is a prime dividing d_B. There is an isomorphism of $\mathcal{O}_B/\mathfrak{m}_\ell$-algebras $\mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_\ell}(A[\mathfrak{m}_\ell]) \cong \mathcal{O}_B/\mathfrak{m}_\ell$.*

Proof. Since $\ell \neq p$, the group scheme $A[\ell]$ is étale over k, so the k-morphism $i(x_\ell) : A[\ell] \to A[\ell]$ is étale. It follows that $A[\mathfrak{m}_\ell]$ is étale over k and in particular $A[\mathfrak{m}_\ell]$ is reduced. As $A[\mathfrak{m}_\ell]$ is reduced, and separated and finite over k, the natural map

$$\mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_\ell}(A[\mathfrak{m}_\ell]) \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_\ell}(A[\mathfrak{m}_\ell](k))$$

is injective. The group $A[\mathfrak{m}_\ell](k)$ is a vector space over $\mathcal{O}_B/\mathfrak{m}_\ell$, and with Π and x_ℓ as above,

$$|A[\mathfrak{m}_\ell](k)| = \deg(i(x_\ell) : A[\ell] \to A[\ell]) = \mathrm{Nrd}(\Pi)^2 = \ell^2,$$

so $A[\mathfrak{m}_\ell](k)$ is of dimension 1 over $\mathcal{O}_B/\mathfrak{m}_\ell$. Therefore the injection of $\mathcal{O}_B/\mathfrak{m}_\ell$-algebras

$$\mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_\ell}(A[\mathfrak{m}_\ell]) \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_\ell}(A[\mathfrak{m}_\ell](k)) \cong \mathcal{O}_B/\mathfrak{m}_\ell$$

must be an isomorphism. □

Proposition 7.1.2. *Let $\ell \neq p$ be a prime. There is a K_ℓ-linear isomorphism of F_ℓ-quadratic spaces*

$$(V_\ell(\mathbf{A}_1, \mathbf{A}_2), \deg_{\mathrm{CM}}) \cong (K_\ell, \beta_\ell \cdot \mathrm{N}_{K_\ell/F_\ell})$$

for some $\beta_\ell \in F_\ell^\times$ satisfying $\beta_\ell \mathcal{O}_{F,\ell} = \mathfrak{D}_\ell^{-1} = \mathfrak{D}^{-1}\mathcal{O}_{F,\ell}$ if $\ell \nmid d_B$ and $\beta_\ell \mathcal{O}_{F,\ell} = \mathfrak{l}\mathfrak{D}_\ell^{-1}$ if $\ell \mid d_B$, where $\mathfrak{l}$ is the prime over ℓ dividing $\ker(\theta) \cap \mathcal{O}_F$. This map takes $L_\ell(\mathbf{A}_1, \mathbf{A}_2)$ isomorphically to $\mathcal{O}_{K,\ell}$.

Proof. We will write L_ℓ and V_ℓ for $L_\ell(\mathbf{A}_1, \mathbf{A}_2)$ and $V_\ell(\mathbf{A}_1, \mathbf{A}_2)$. The isomorphism of quadratic spaces for some $\beta_\ell \in F_\ell^\times$ follows from Proposition 3.2.7(b). Under this isomorphism, L_ℓ is sent to a finitely generated $\mathcal{O}_{K,\ell}$-submodule of K_ℓ, that is, a fractional $\mathcal{O}_{K,\ell}$-ideal. Then since every ideal of $\mathcal{O}_{K,\ell}$ is principal, there is an isomorphism $V_\ell \cong K_\ell$ inducing an isomorphism $L_\ell \cong \mathcal{O}_{K,\ell}$. The $\mathcal{O}_{F,\ell}$-bilinear form

$$[\cdot\,,\cdot]_{\mathrm{CM}} : L_\ell \times L_\ell \to \mathfrak{D}_\ell^{-1}$$

induces an $\mathcal{O}_{F,\ell}$-bilinear form

$$\mathcal{O}_{K,\ell} \times \mathcal{O}_{K,\ell} \to \mathfrak{D}_\ell^{-1}$$

given by

$$(x, y) \mapsto \beta_\ell \mathrm{N}_{K_\ell/F_\ell}(x + y) - \beta_\ell \mathrm{N}_{K_\ell/F_\ell}(x) - \beta_\ell \mathrm{N}_{K_\ell/F_\ell}(y) = \beta_\ell \,\mathrm{Tr}_{K_\ell/F_\ell}(x\overline{y}).$$

The dual lattice of $\mathcal{O}_{K,\ell}$ with respect to this pairing is

$$\mathcal{O}_{K,\ell}^{\vee} = \{x \in K_\ell : \beta_\ell \operatorname{Tr}_{K_\ell/F_\ell}(x\overline{y}) \in \mathfrak{D}_\ell^{-1} \text{ for all } y \in \mathcal{O}_{K,\ell}\},$$

so

$$\begin{aligned} \beta_\ell \mathcal{O}_{K,\ell}^{\vee} &= \{x \in K_\ell : \operatorname{Tr}_{K_\ell/F_\ell}(xy) \in \mathfrak{D}_\ell^{-1} \text{ for all } y \in \mathcal{O}_{K,\ell}\} \\ &= \{x \in K_\ell : \operatorname{Tr}_{K_\ell/\mathbb{Q}_\ell}(xy) \in \mathbb{Z}_\ell \text{ for all } y \in \mathcal{O}_{K,\ell}\} \\ &= \mathfrak{D}_{K/\mathbb{Q}}^{-1} \mathcal{O}_{K,\ell}. \end{aligned}$$

Since K/F is unramified at any prime of F over ℓ,

$$\mathfrak{D}_{K/\mathbb{Q}} \mathcal{O}_{K,\ell} = \mathfrak{D}_{K/F} \mathcal{O}_{K,\ell} \cdot \mathfrak{D}_{F/\mathbb{Q}} \mathcal{O}_{K,\ell} = \mathfrak{D} \mathcal{O}_{K,\ell},$$

where $\mathfrak{D}$ is the different of $F/\mathbb{Q}$. Therefore $\beta_\ell \mathcal{O}_{K,\ell}^{\vee} = \mathfrak{D}^{-1}\mathcal{O}_{K,\ell}$, which shows that the dual of L_ℓ with respect to $\deg_{\mathrm{CM}}$ is $L_\ell^{\vee} \cong \mathcal{O}_{K,\ell}^{\vee} = \beta_\ell^{-1}\mathfrak{D}^{-1}\mathcal{O}_{K,\ell}$.

We claim that the dual lattice

$$\{f \in V_\ell : [f, f']_{\mathrm{CM}} \in \mathfrak{D}_\ell^{-1} \text{ for all } f' \in L_\ell\}$$

of L_ℓ with respect to the $\mathcal{O}_{F,\ell}$-bilinear form $[\cdot\,,\cdot]_{\mathrm{CM}} : L_\ell \times L_\ell \to \mathfrak{D}_\ell^{-1}$ (corresponding to $\deg_{\mathrm{CM}}$) is equal to the dual lattice

$$\{f \in V_\ell : [f, f'] \in \mathbb{Z}_\ell \text{ for all } f' \in L_\ell\}$$

of L_ℓ with respect to the $\mathbb{Z}_\ell$-bilinear form $[\cdot\,,\cdot] : L_\ell \times L_\ell \to \mathbb{Z}_\ell$ (corresponding to $\deg^*$). Since $[\cdot\,,\cdot] = \operatorname{Tr}_{F_\ell/\mathbb{Q}_\ell}[\cdot\,,\cdot]_{\mathrm{CM}}$, this can be checked by proving the corresponding result for the pairings

$$\mathcal{O}_{K,\ell} \times \mathcal{O}_{K,\ell} \to \mathfrak{D}_\ell^{-1}, \quad (x, y) \mapsto \beta_\ell \operatorname{Tr}_{K_\ell/F_\ell}(x\overline{y}) = \operatorname{Tr}_{K_\ell/F_\ell}(\beta_\ell x\overline{y})$$

and

$$\mathcal{O}_{K,\ell} \times \mathcal{O}_{K,\ell} \to \mathbb{Z}_\ell, \quad (x, y) \mapsto \operatorname{Tr}_{F_\ell/\mathbb{Q}_\ell}(\operatorname{Tr}_{K_\ell/F_\ell}(\beta_\ell x\overline{y})) = \operatorname{Tr}_{K_\ell/\mathbb{Q}_\ell}(\beta_\ell x\overline{y}).$$

This is clear from what we showed above since the dual of $\mathcal{O}_{K,\ell}$ with respect to both pairings is $\beta_\ell^{-1}\mathfrak{D}_{K/\mathbb{Q}}^{-1}\mathcal{O}_{K,\ell}$.

First suppose $\ell \nmid d_B$, and write T_j for $T_\ell(A_j)$. By Lemmas 6.1.1 and 6.1.2 there are isomorphisms of $\mathbb{Z}_\ell$-modules

$$L_\ell \cong \operatorname{Hom}_{\mathcal{O}_B}(T_1, T_2) \cong \mathrm{M}_2(\mathbb{Z}_\ell).$$

We claim that under this isomorphism the quadratic form $\deg^*$ on L_ℓ is identified with the quadratic form $u \cdot \det$ on $\mathrm{M}_2(\mathbb{Z}_\ell)$ for some $u \in \mathbb{Z}_\ell^\times$. If we choose an $\mathcal{O}_B$-linear isomorphism of $\mathbb{Z}_\ell$-modules $\gamma : T_1 \to T_2$ (which is possible since the idempotents $\varepsilon, \varepsilon' \in \mathrm{M}_2(\mathbb{Z}_\ell) \cong \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ provide a splitting $T_j \cong \varepsilon T_j \oplus \varepsilon' T_j$), there is an isomorphism of $\mathbb{Z}_\ell$-modules

$$\mathrm{Hom}_{\mathcal{O}_B}(T_1, T_2) \to \mathrm{End}_{\mathcal{O}_B}(T_1)$$

given by $f \mapsto \gamma^{-1} \circ f$. Writing $\deg^*$ for the quadratic form on $\mathrm{Hom}_{\mathcal{O}_B}(T_1, T_2)$ induced by $\deg^*$ on L_ℓ, we have $\deg^*(\gamma^{-1} \circ f) = \deg^*(\gamma^{-1}) \deg^*(f)$ with $\deg^*(\gamma^{-1}) \in \mathbb{Z}_\ell^\times$, so it suffices to assume $A_1 = A_2 = A$ and show that under the isomorphism

$$L_\ell \to \mathrm{End}_{\mathcal{O}_B}(T_\ell(A)) \to \mathrm{M}_2(\mathbb{Z}_\ell)$$

given above, $\deg^*$ on L_ℓ is identified with $\det$ on $\mathrm{M}_2(\mathbb{Z}_\ell)$. It is enough to show that after tensoring this map with $\mathbb{Q}_\ell$, we obtain an isomorphism of $\mathbb{Q}_\ell$-quadratic spaces

$$\Phi : (V_\ell, \deg^*) \to (\mathrm{M}_2(\mathbb{Q}_\ell), \det).$$

Let Q be the quadratic form on $\mathrm{M}_2(\mathbb{Q}_\ell)$ induced by Φ. By Proposition 3.2.7(c) there is some isomorphism of $\mathbb{Q}_\ell$-quadratic spaces

$$\Psi : (V_\ell, \deg^*) \to (B_\ell^{(p)}, \mathrm{Nrd}) \cong (\mathrm{M}_2(\mathbb{Q}_\ell), \det).$$

Note that Φ and Ψ are both ring homomorphisms. Then by Noether-Skolem there is a $b \in \mathrm{M}_2(\mathbb{Q}_\ell)^\times$ such that $\Psi(v) = b\Phi(v)b^{-1}$ for all $v \in V_\ell$. Hence

$$Q(\Phi(v)) = \deg^*(v) = \det(\Psi(v)) = \det(b\Phi(v)b^{-1}) = \det(\Phi(v)),$$

so $Q = \det$.

A calculation shows that the lattice $\mathrm{M}_2(\mathbb{Z}_\ell) \subset \mathrm{M}_2(\mathbb{Q}_\ell)$ is self dual relative to det, which means L_ℓ is self dual relative to $\deg^*$. From the isomorphism

$$L_\ell^\vee / L_\ell \cong \beta_\ell^{-1} \mathfrak{D}^{-1} \mathcal{O}_{K,\ell} / \mathcal{O}_{K,\ell},$$

we find that $\beta_\ell \mathcal{O}_{K,\ell} = \mathfrak{D}^{-1} \mathcal{O}_{K,\ell}$, and thus $\beta_\ell \mathcal{O}_{F,\ell} = \mathfrak{D}_\ell^{-1}$ as K/F is unramified over ℓ.

Now suppose $\ell \mid d_B$. In the proof of Lemma 6.1.1(b) we showed that $T_\ell(A_j) \cong \mathcal{O}_{B,\ell}$ as $\mathcal{O}_{B,\ell}$-modules, so $T_\ell(A_1) \cong T_\ell(A_2)$ as $\mathcal{O}_{B,\ell}$-modules and thus by Lemma 6.1.2 there are isomorphisms of

$\mathbb{Z}_\ell$-modules

$$\begin{aligned}\mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell &\cong \mathrm{Hom}_{\mathcal{O}_B}(T_\ell(A_1), T_\ell(A_2)) \cong \mathrm{End}_{\mathcal{O}_B}(T_\ell(A_1))\\ &\cong \mathrm{End}_{\mathcal{O}_B}(A_1) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell.\end{aligned}$$

Therefore we may reduce to the case where the CM false elliptic curves $\mathbf{A}_1$ and $\mathbf{A}_2$ have the same underlying false elliptic curve A. By Lemmas 6.1.1 and 6.1.2 there are isomorphisms of $\mathbb{Z}_\ell$-algebras

$$L_\ell \cong \mathrm{End}_{\mathcal{O}_B}(T_\ell(A)) \cong \mathcal{O}_{B,\ell},$$

and by a proof identical to that in the case of $\ell \nmid d_B$, this isomorphism identifies the quadratic form $\deg^*$ on L_ℓ with the quadratic form Nrd on $\mathcal{O}_{B,\ell}$. If $\mathfrak{n}_\ell \subset \mathcal{O}_{B,\ell}$ is the unique maximal ideal, so $\mathfrak{m}_\ell \mathcal{O}_{B,\ell} = \mathfrak{n}_\ell$, then a calculation shows that the dual lattice of $\mathcal{O}_{B,\ell}$ relative to Nrd is $\mathfrak{n}_\ell^{-1}$. Hence we have $\mathcal{O}_{K,\ell}$-linear isomorphisms

$$\beta_\ell^{-1}\mathfrak{D}^{-1}\mathcal{O}_{K,\ell}/\mathcal{O}_{K,\ell} \cong L_\ell^\vee/L_\ell \cong \mathfrak{n}_\ell^{-1}/\mathcal{O}_{B,\ell}.$$

As a group, $\mathfrak{n}_\ell^{-1}/\mathcal{O}_{B,\ell} \cong \mathcal{O}_{B,\ell}/\mathfrak{n}_\ell \cong \mathbb{F}_{\ell^2}$, so $[\mathcal{O}_{K,\ell} : \beta_\ell \mathfrak{D}\mathcal{O}_{K,\ell}] = \ell^2$.

Recall that $\mathcal{O}_K$ acts on $L_\ell \cong \mathcal{O}_{B,\ell}$ by

$$(t_1 \otimes t_2) \bullet f = \kappa_2(t_2) \circ f \circ \kappa_1(\bar{t}_1).$$

Fixing a uniformizer $\Pi \in \mathcal{O}_{B,\ell}$ satisfying $\kappa_1(\bar{t}_1)\Pi = \Pi\kappa_1(t_1)$ for all $t_1 \in \mathcal{O}_{K_1}$, for any $u \in \kappa_1(\mathcal{O}_{K_1}) \subset \mathcal{O}_{B,\ell}$ we have

$$(t_1 \otimes t_2) \bullet u\Pi^{-1} = \kappa_2(t_2)u\Pi^{-1}\kappa_1(\bar{t}_1) = \kappa_2(t_2)\kappa_1(t_1)u\Pi^{-1}.$$

Since $\mathfrak{n}_\ell^{-1}/\mathcal{O}_{B,\ell}$ is generated by such elements $u\Pi^{-1}$, $\mathcal{O}_K$ acts on $\mathfrak{n}_\ell^{-1}/\mathcal{O}_{B,\ell}$ through left multiplication by the image of the composition $\mathcal{O}_K \to \mathcal{O}_{B,\ell} \to \mathcal{O}_{B,\ell}/\mathfrak{n}_\ell$, where the first map is given by $t_1 \otimes t_2 \mapsto \kappa_2(t_2)\kappa_1(t_1)$. Next, under the isomorphism $L_\ell \cong \mathcal{O}_{B,\ell}$, the action

$$\mathcal{O}_{B,\ell} \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_\ell}(A[\mathfrak{m}_\ell]) \cong \mathcal{O}_B/\mathfrak{m}_\ell$$

determines an isomorphism $\gamma : \mathcal{O}_{B,\ell}/\mathfrak{n}_\ell \to \mathcal{O}_B/\mathfrak{m}_\ell$, which allows us to identify

$$\kappa_j^{\mathfrak{m}_\ell} : \mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_\ell}(A[\mathfrak{m}_\ell])$$

with the composition

$$\mathcal{O}_{K_j} \xrightarrow{\kappa_j} \mathcal{O}_{B,\ell} \to \mathcal{O}_{B,\ell}/\mathfrak{n}_\ell \xrightarrow{\gamma} \mathcal{O}_B/\mathfrak{m}_\ell.$$

However, the map $\mathcal{O}_K \to \mathbb{F}_{\ell^2}$ defined by $t_1 \otimes t_2 \mapsto \kappa_1^{\mathfrak{m}_\ell}(t_1)\kappa_2^{\mathfrak{m}_\ell}(t_2)$ is equal to the map

$$\mathcal{O}_K \xrightarrow{\theta} \mathcal{O}_B/\mathfrak{m}_B \to \mathcal{O}_B/\mathfrak{m}_\ell,$$

by definition of $(\mathbf{A}_1, \mathbf{A}_2)$ being in $\mathscr{X}_\theta(\overline{\mathbb{F}}_\mathfrak{P})$, and the kernel of this map is the prime $\mathfrak{L}$ of K over $\mathfrak{l}$. It then follows from the factorization of $\kappa_j^{\mathfrak{m}_\ell}$ above that any element of $\mathfrak{L}$ acts trivially on $\mathfrak{n}_\ell^{-1}/\mathcal{O}_{B,\ell}$ and therefore there is an $\mathcal{O}_{K,\ell}$-linear map $\mathcal{O}_{K,\ell}/\mathfrak{L}\mathcal{O}_{K,\ell} \hookrightarrow \mathfrak{n}_\ell^{-1}/\mathcal{O}_{B,\ell}$ given by $x \mapsto x \bullet 1$. But $\mathfrak{L}$ has norm ℓ^2, which means

$$\mathcal{O}_{K,\ell}/\mathfrak{L}\mathcal{O}_{K,\ell} \cong \mathfrak{n}_\ell^{-1}/\mathcal{O}_{B,\ell} \cong \beta_\ell^{-1}\mathfrak{D}^{-1}\mathcal{O}_{K,\ell}/\mathcal{O}_{K,\ell}$$

as $\mathcal{O}_{K,\ell}$-modules. It follows that $\beta_\ell\mathfrak{D}\mathcal{O}_{K,\ell} = \mathfrak{L}\mathcal{O}_{K,\ell}$ and thus $\beta_\ell\mathcal{O}_{F,\ell} = \mathfrak{l}\mathfrak{D}_\ell^{-1}$. □

7.2 The case of $\ell = p$

In order to prove a similar result for $\ell = p$ we need a few preliminary results.

Lemma 7.2.1. *If $(A, i) \in \mathscr{Y}_j(\overline{\mathbb{F}}_p)$ with $p \mid d_B$, then $\mathrm{End}_{\mathcal{O}_{B,p}}(\mathrm{Lie}(A)) \cong \overline{\mathbb{F}}_p$ as $\overline{\mathbb{F}}_p$-algebras.*

Proof. Fix an isomorphism $\mathcal{O}_{B,p} \cong \Delta$ and a uniformizer $\Pi \in \Delta$. There are isomorphisms of $\overline{\mathbb{F}}_p$-vector spaces

$$\mathrm{Lie}(A) \cong \mathrm{Lie}(D(A)) \cong D(A)/\mathscr{V}D(A),$$

so $\mathrm{End}_\Delta(\mathrm{Lie}(A)) \cong \mathrm{End}_\Delta(D(A)/\mathscr{V}D(A))$. Let $\{e_n\}$ be a W-basis for $D(A)$ as in Proposition 6.3.2, so the images $\widetilde{e}_1, \widetilde{e}_3$ of e_1, e_3 in $D(A)/\mathscr{V}D(A)$ form a basis for this 2-dimensional vector space over $W/pW \cong \overline{\mathbb{F}}_p$. In the notation of (6.3.2), if $D(i) = f_1$ then the action of Δ on $D(A)/\mathscr{V}D(A)$ is given, in the basis $\{\widetilde{e}_1, \widetilde{e}_3\}$, by the matrix

$$D(i)(a + b\Pi) = \begin{bmatrix} \widetilde{a} & \widetilde{b} \\ 0 & \widetilde{\overline{a}} \end{bmatrix} \in \mathrm{M}_2(\overline{\mathbb{F}}_p),$$

where $\widetilde{a}$ is the image of a in $W/pW \cong \overline{\mathbb{F}}_p$. A computation shows that a matrix in $\mathrm{M}_2(\overline{\mathbb{F}}_p)$ commutes with $D(i)(a + b\Pi)$ for all $a + b\Pi \in \Delta$ if and only if it is a scalar matrix, and therefore

$$\mathrm{End}_\Delta(\mathrm{Lie}(A)) \cong \mathrm{End}_\Delta(D(A)/\mathscr{V}D(A)) \cong \overline{\mathbb{F}}_p.$$

An identical computation gives the same result if $D(i) = f_2$. □

Proposition 7.2.2. *Suppose $(A, i) \in \mathscr{Y}_j(\overline{\mathbb{F}}_p)$ with $p \mid d_B$. Under the isomorphism*

$$\Phi : \mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to R_{11}$$

in Proposition 6.3.1*, the $\mathbb{Z}_p$-quadratic form* $\deg^*$ *on* $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ *is identified with the $\mathbb{Z}_p$-quadratic form Q on R_{11} given by*

$$Q \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix} = x\overline{x} - p^2 y\overline{y}.$$

Proof. Since Φ is an isomorphism of rings and $\deg^*(f) = f \circ f^t$, we have $Q(\varphi) = \varphi\varphi^\dagger$, where $\varphi \mapsto \varphi^\dagger$ is the involution on R_{11} induced by Φ from the involution $f \mapsto f^t$ on $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Recall that $f^t = \lambda^{-1} \circ f^\vee \circ \lambda$, where $\lambda : A \to A^\vee$ is the unique principal polarization satisfying $\lambda^{-1} \circ i(x)^\vee \circ \lambda = i(x^*)$ for all $x \in \mathcal{O}_B$. The polarization λ then induces a map $\Lambda = D(\lambda) : D(A) \to D(A^\vee)$ on Dieudonné modules. There is a canonical isomorphism of $\mathscr{D}$-modules

$$D(A^\vee) \cong D(A)^\vee = \mathrm{Hom}_W(D(A), W),$$

where $D(A)^\vee$ is a $\mathscr{D}$-module via

$$(\mathscr{F} \cdot f)(x) = \sigma(f(\mathscr{V}x)), \quad (\mathscr{V} \cdot f)(x) = \sigma^{-1}(f(\mathscr{F}x)).$$

This map Λ induces a nondegenerate, alternating, bilinear pairing

$$\langle \cdot, \cdot \rangle : D(A) \times D(A) \to W$$

defined by $\langle x, y \rangle = \Lambda(x)(y)$, and this pairing satisfies $\langle \mathscr{F}x, y \rangle = \sigma(\langle x, \mathscr{V}y \rangle)$ for all $x, y \in D(A)$. In fact, if $(\cdot, \cdot)$ is any nondegenerate, alternating, bilinear pairing $D(A) \times D(A) \to W$ satisfying $(\mathscr{F}x, y) = \sigma(x, \mathscr{V}y)$ for all $x, y \in D(A)$, then $(\cdot, \cdot)$ arises from a principal polarization $A[p^\infty] \to A[p^\infty]^\vee$ in this way. (Here, $A[p^\infty]^\vee \cong A^\vee[p^\infty]$ is the Serre dual of $A[p^\infty]$ and a principal polarization $\mu : A[p^\infty] \to A[p^\infty]^\vee$ is by definition an isomorphism such that the composition $A[p^\infty]^{\vee\vee} \xrightarrow{\cong} A[p^\infty] \xrightarrow{\mu} A[p^\infty]^\vee$ is equal to $-\mu^\vee$. Any principal polarization $A \to A^\vee$ induces a principal polarization $A[p^\infty] \to A[p^\infty]^\vee$ ([5, 1.4.3.4]).)

Recall that $x^* = a^{-1}x^\iota a$, where $a \in \mathcal{O}_B$ is an element satisfying $a^2 = -d_B$. In the local case of $a \in \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \Delta$, we can explicitly choose a. Since $\mathbb{Q}_{p^2}/\mathbb{Q}_p$ is unramified, the norm map $\mathrm{N}_{\mathbb{Q}_{p^2}/\mathbb{Q}_p} : \mathbb{Z}_{p^2}^\times \to \mathbb{Z}_p^\times$ is surjective, so there is an $a_0 \in \mathbb{Z}_{p^2}^\times$ such that $a_0\overline{a}_0 = -p^{-1}d_B$ (note that

$\mathrm{ord}_p(d_B) = 1$). Let $a = a_0\Pi \in \Delta$, so $a^2 = pa_0\overline{a}_0 = -d_B$.

Let $\{e_n\}$ be a W-basis for $D(A)$ as in Proposition 6.3.2. First suppose $D(i) = f_1$, in the notation of (6.3.2). Then for $x = u + v\Pi \in \Delta$, one can compute, using $x^\iota = \overline{u} - v\Pi$,

$$D(i(x^*)) = D(i(a))^{-1}D(i(x^\iota))D(i(a)) = \begin{bmatrix} u & 0 & -a_0\overline{a}_0^{-1}\overline{v} & 0 \\ 0 & \overline{u} & 0 & -a_0^{-1}\overline{a}_0 v \\ -pa_0^{-1}\overline{a}_0 v & 0 & \overline{u} & 0 \\ 0 & -pa_0\overline{a}_0^{-1}\overline{v} & 0 & u \end{bmatrix}.$$

Now, viewing Λ as an element of $\mathrm{Hom}_W(D(A), D(A)^\vee) \cong \mathrm{End}_W(D(A)) \cong \mathrm{M}_4(W)$, using that Λ is invertible and alternating, and using that $\Lambda \circ D(i(x^*)) = D(i(x))^\vee \circ \Lambda$ for all $x \in \Delta$, where $D(i(x))^\vee$ is the dual linear map (so its matrix is the transpose of the matrix of $D(i(x))$ with respect to the dual basis), a computation shows Λ must be of the form

$$\Lambda = \begin{bmatrix} 0 & 0 & 0 & ba_0^{-1}\overline{a}_0 \\ 0 & 0 & b & 0 \\ 0 & -b & 0 & 0 \\ -ba_0^{-1}\overline{a}_0 & 0 & 0 & 0 \end{bmatrix}$$

for some $b \in W^\times$. The equality $\langle \mathscr{F}e_1, e_3\rangle = \sigma\langle e_1, \mathscr{V}e_3\rangle$ implies $b = \sigma(b)a_0\overline{a}_0^{-1}$, so $b \in \mathbb{Z}_{p^2}^\times$ and

$$\Lambda = \begin{bmatrix} 0 & 0 & 0 & \sigma(b) \\ 0 & 0 & b & 0 \\ 0 & -b & 0 & 0 \\ -\sigma(b) & 0 & 0 & 0 \end{bmatrix}.$$

The involution $\varphi \mapsto \varphi^\dagger$ on $\mathrm{End}_W(D(A)) \cong \mathrm{M}_4(W)$ corresponding to the Rosati involution $f \mapsto \lambda^{-1} \circ f^\vee \circ \lambda$ on $\mathrm{End}^0(A)$ (which restricts to $f \mapsto f^t$ on $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p$) is then given by $\varphi^\dagger = \Lambda^{-1}\varphi^T\Lambda$, where φ^T is the transpose of the matrix φ. A computation shows that for $\varphi = [\varphi_{ij}] \in \mathrm{M}_4(W)$,

$$\varphi^\dagger = \begin{bmatrix} \varphi_{44} & b\overline{b}^{-1}\varphi_{34} & -b\overline{b}^{-1}\varphi_{24} & -\varphi_{14} \\ b^{-1}\overline{b}\varphi_{43} & \varphi_{33} & -\varphi_{23} & -b^{-1}\overline{b}\varphi_{13} \\ -b^{-1}\overline{b}\varphi_{42} & -\varphi_{32} & \varphi_{22} & b^{-1}\overline{b}\varphi_{12} \\ -\varphi_{41} & -b\overline{b}^{-1}\varphi_{31} & b\overline{b}^{-1}\varphi_{21} & \varphi_{11} \end{bmatrix}.$$

If

$$\varphi = \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix} \in R_{11},$$

then viewing it as an element of $\mathrm{M}_4(W)$ as in (6.3.4), applying the involution †, as described explicitly above, and then viewing it again in R_{11}, gives

$$\varphi^\dagger = \begin{bmatrix} \overline{x} & -y\Pi \\ -py\Pi & \overline{x} \end{bmatrix}.$$

Therefore

$$\varphi\varphi^\dagger = \begin{bmatrix} x\overline{x} - p^2 y\overline{y} & 0 \\ 0 & x\overline{x} - p^2 y\overline{y} \end{bmatrix},$$

so after identifying $\mathbb{Z}_p$ with its diagonal image in $\mathrm{M}_2(\mathbb{Z}_{p^2})$, we obtain $Q(\varphi) = x\overline{x} - p^2 y\overline{y}$. A similar computation gives the same result if $D(i) = f_2$. More specifically, we saw that in this case there is an isomorphism of rings $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to R_{22}$, where

$$R_{22} = \left\{ \begin{bmatrix} x & py\Pi \\ y\Pi & x \end{bmatrix} : x, y \in \mathbb{Z}_{p^2} \right\},$$

and one can check that the involution † on R_{22} is given by

$$\varphi = \begin{bmatrix} x & py\Pi \\ y\Pi & x \end{bmatrix} \mapsto \varphi^\dagger = \begin{bmatrix} \overline{x} & -py\Pi \\ -y\Pi & \overline{x} \end{bmatrix}.$$

However, once we apply the ring isomorphism $R_{22} \to R_{11}$ given by conjugation by

$$\begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix},$$

this involution † on R_{22} corresponds to the involution † on R_{11} described in the first case. □

For $j = 1, 2$ let $\theta_j : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_B$ be a ring homomorphism and let $A_j \in \mathscr{Y}_j^{\theta_j}(\overline{\mathbb{F}}_{\mathfrak{P}})$ for $p \mid d_B$. Then there is a unique ring isomorphism $\mathcal{O}_{K_1,p} \to \mathcal{O}_{K_2,p}$ making the diagram

$$\begin{tikzcd} \mathcal{O}_{K_1,p} \arrow[rr] \arrow[dr, "\theta_1"'] & & \mathcal{O}_{K_2,p} \arrow[dl, "\theta_2"] \\ & \mathcal{O}_B/\mathfrak{m}_B & \end{tikzcd} \tag{7.2.1}$$

commute. We use this to identify the rings $\mathcal{O}_{K_1,p}$ and $\mathcal{O}_{K_2,p}$, and call this ring $\mathcal{O}_L$. Then by Proposition 6.3.2 there are W-bases $\{e_n\}$ and $\{e'_n\}$ for $D(A_1)$ and $D(A_2)$ with $\mathcal{O}_L$ acting via (6.3.3) on both and $\mathcal{O}_{B,p} \cong \Delta$ acting on $D(A_j)$ through one of f_1 or f_2 in (6.3.2).

Definition 7.2.3. With notation as above, if $D(A_1)$ and $D(A_2)$ are isomorphic as $\Delta \otimes_{\mathbb{Z}_p} \mathcal{O}_L$-modules, we say that A_1 and A_2 are of the *same type*.

Note that there are two isomorphism classes of $\Delta \otimes_{\mathbb{Z}_p} \mathcal{O}_L$-modules free of rank 4 over $\mathbb{Z}_p$, and A_1 and A_2 being of the same type just means $D(A_1)$ and $D(A_2)$ lie in the same isomorphism class, and not being of the same type means they lie in the two separate classes. This definition is a bit misleading because we will see below that A_1 and A_2 are of the same type if and only if $\mathfrak{P}$ divides $\ker(\theta)$, where $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ is the map induced by θ_1 and θ_2, so this "type" is really a property between $\mathfrak{P}$ and θ, independent of A_1 and A_2. However, the above definition is the easier one to start with in proving the next few results.

Proposition 7.2.4. *Suppose $(A_j, i_j) \in \mathscr{Y}_j^{\theta_j}(\overline{\mathbb{F}}_{\mathfrak{P}})$ for $j = 1, 2$, where $p \mid d_B$, and A_1 and A_2 are not of the same type. There are isomorphisms of $\mathbb{Z}_p$-modules*

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) \cong \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_2), D(A_1)) \cong R_{12},$$

where

$$R_{12} = \left\{ \begin{bmatrix} px & y\Pi \\ y\Pi & x \end{bmatrix} : x, y \in \mathbb{Z}_{p^2} \right\} \subset \mathrm{M}_2(\Delta)$$

and we have fixed an embedding $\mathbb{Z}_{p^2} \hookrightarrow \Delta$ such that $\Delta = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}\Pi$. Under the isomorphism

$$\mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{D} \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) \cong R_{12},$$

the $\mathbb{Z}_p$-quadratic form $\deg^*$ on $\mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is identified with the $\mathbb{Z}_p$-quadratic form $u \cdot Q'$ on R_{12}, where $u \in \mathbb{Z}_p^\times$ and

$$Q' \begin{bmatrix} px & y\Pi \\ y\Pi & x \end{bmatrix} = p(x\overline{x} - y\overline{y}).$$

Under the isomorphism

$$\mathrm{Hom}_{\mathcal{O}_B}(A_2, A_1) \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{D} \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_2), D(A_1)) \cong R_{12},$$

the quadratic form $\deg^*$ is identified with the quadratic form $u^{-1} \cdot Q'$.

Proof. There is an isomorphism of $\mathscr{D}$-modules $D(A_1) \cong D(A_2)$, so

$$\mathrm{Hom}_{\mathscr{D}}(D(A_1), D(A_2)) \cong \mathrm{End}_{\mathscr{D}}(D(A_1)) \cong \mathrm{End}_{\mathscr{D}}(D(E_1)^2) \cong \mathrm{M}_2(\Delta),$$

where $A_1 \cong M \otimes_{\mathcal{O}_{K_1}} E_1$. Hence

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) = \{\varphi \in \mathrm{M}_2(\Delta) : \varphi i_1(x) = i_2(x)\varphi \text{ for all } x \in \Delta\}$$

and

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_2), D(A_1)) = \{\varphi \in \mathrm{M}_2(\Delta) : \varphi i_2(x) = i_1(x)\varphi \text{ for all } x \in \Delta\}.$$

Suppose we choose bases for $D(A_1)$ and $D(A_2)$ relative to which $D(i_1) = f_1$ and $D(i_2) = f_2$ (as in (6.3.2)). Then an easy computation gives

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) \cong R_{12}$$

and

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_2), D(A_1)) \cong R_{21} = \left\{ \begin{bmatrix} x & y\Pi \\ y\Pi & px \end{bmatrix} : x, y \in \mathbb{Z}_{p^2} \right\}.$$

However, there is an isomorphism of $\mathbb{Z}_p$-modules $R_{21} \to R_{12}$ given by $\varphi \mapsto U\varphi U^{-1}$, where

$$U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

For any $f \in \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ we have $\deg^*(f) = f^t \circ f$, where $f^t = \lambda_1^{-1} \circ f^\vee \circ \lambda_2$ with $\lambda_j : A_j \to A_j^\vee$ the unique principal polarization satisfying $i_j(x^*) = \lambda_j^{-1} \circ i(x)^\vee \circ \lambda_j$ for all $x \in \mathcal{O}_B$. In the proof of Proposition 7.2.2 we showed

$$\Lambda_j = D(\lambda_j) = \begin{bmatrix} 0 & 0 & 0 & \overline{b}_j \\ 0 & 0 & b_j & 0 \\ 0 & -b_j & 0 & 0 \\ -\overline{b}_j & 0 & 0 & 0 \end{bmatrix} \in \mathrm{M}_4(W)$$

for some $b_j \in \mathbb{Z}_{p^2}^\times$ satisfying $b_j = \overline{b}_j a_0 \overline{a}_0^{-1}$, with a_0 as in that proof. In particular, $b_1^{-1} b_2 = \overline{b}_1^{-1} \overline{b}_2$, so $b_1^{-1} b_2 \in \mathbb{Z}_p^\times$. We have

$$D(f^t) = D(\lambda_1^{-1}) \circ D(f^\vee) \circ D(\lambda_2) = \Lambda_1^{-1} D(f)^\vee \Lambda_2,$$

where $D(f)^\vee \in \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_2)^\vee, D(A_1)^\vee)$ is the dual linear map. Therefore, through the map D, the assignment

$$f \mapsto f^t : \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathrm{Hom}_{\mathcal{O}_B}(A_2, A_1) \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

corresponds to the assignment

$$\varphi \mapsto \varphi^\dagger : \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) \to \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_2), D(A_1)),$$

where $\varphi^\dagger = \Lambda_1^{-1} \varphi^T \Lambda_2$. If

$$\varphi = \begin{bmatrix} px & y\Pi \\ y\Pi & x \end{bmatrix} \in R_{12}$$

then a computation shows

$$\varphi^\dagger = \begin{bmatrix} \overline{x}u & -yu\Pi \\ -yu\Pi & p\overline{x}u \end{bmatrix} \in R_{21}$$

where $u = b_1^{-1}b_2$. Under the isomorphism D, the quadratic form $\deg^*$ corresponds to some quadratic form Q_0 on R_{12}, so for $\varphi = D(f)$,

$$Q_0(\varphi) = \deg^*(f) = D(\deg^*(f)) = D(f^t) \circ D(f) = \varphi^\dagger\varphi = \begin{bmatrix} p(x\overline{x} - y\overline{y})u & 0 \\ 0 & p(x\overline{x} - y\overline{y})u \end{bmatrix},$$

so $Q_0 = uQ'$. A similar computation gives the result for the isomorphism

$$\mathrm{Hom}_{\mathcal{O}_B}(A_2, A_1) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_2), D(A_1)) \cong R_{12}. \qquad \square$$

Recall that $(\mathbf{A}_1, \mathbf{A}_2) \in \mathscr{X}_\theta(\overline{\mathbb{F}}_{\mathfrak{P}})$ and for $p \mid d_B$ we are using θ to identify $\mathcal{O}_{K_1,p}$ and $\mathcal{O}_{K_2,p}$ as in (7.2.1).

Proposition 7.2.5. *There is a K_p-linear isomorphism of F_p-quadratic spaces*

$$(V_p(\mathbf{A}_1, \mathbf{A}_2), \deg_{\mathrm{CM}}) \cong (K_p, \beta_p \cdot \mathrm{N}_{K_p/F_p})$$

for some $\beta_p \in F_p^\times$ satisfying

$$\beta_p\mathcal{O}_{F,p} = \begin{cases} \mathfrak{p}\mathfrak{D}_p^{-1} & \text{if } p \nmid d_B \\ \mathfrak{p}^2\mathfrak{D}_p^{-1} & \text{if } p \mid d_B \text{ and } A_1, A_2 \text{ are of the same type} \\ \mathfrak{p}\overline{\mathfrak{p}}\mathfrak{D}_p^{-1} & \text{if } p \mid d_B \text{ and } A_1, A_2 \text{ are not of the same type,} \end{cases}$$

where $\mathfrak{D}_p = \mathfrak{D}\mathcal{O}_{F,p}$, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$, and $\overline{\mathfrak{p}}$ is the other prime ideal of $\mathcal{O}_F$ lying over p. This map takes $L_p(\mathbf{A}_1, \mathbf{A}_2)$ isomorphically to $\mathcal{O}_{K,p}$.

Proof. First suppose $p \nmid d_B$. The proof is very similar to the $\ell \mid d_B$ case of the proof of Proposition 7.1.2. We will write L_p for $L_p(\mathbf{A}_1, \mathbf{A}_2)$. The proof of the existence of the isomorphism taking L_p to $\mathcal{O}_{K,p}$ is the same as for $\ell \neq p$. We may reduce to the case where the CM false elliptic curves $\mathbf{A}_1$ and $\mathbf{A}_2$ have the same underlying false elliptic curve A because the idempotents $\varepsilon, \varepsilon' \in \mathrm{M}_2(W) \cong \mathcal{O}_B \otimes_{\mathbb{Z}} W$ provide a splitting $D(A_j) \cong \varepsilon D(A_j) \oplus \varepsilon' D(A_j)$, which means $D(A_1) \cong D(A_2)$ as $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}$-modules and thus

$$\begin{aligned} \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_p &\cong \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) \cong \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1)) \\ &\cong \mathrm{End}_{\mathcal{O}_B}(A_1) \otimes_{\mathbb{Z}} \mathbb{Z}_p. \end{aligned}$$

By Lemmas 6.2.1 and 6.2.2 there are isomorphisms of $\mathbb{Z}_p$-algebras

$$L_p \cong \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A)) \cong \Delta.$$

Similar to before, this isomorphism identifies the quadratic form $\deg^*$ on L_p with the quadratic form Nrd on Δ. If $\mathfrak{m}_\Delta \subset \Delta$ is the unique maximal ideal then the dual lattice of Δ relative to Nrd is $\mathfrak{m}_\Delta^{-1}$, and there are $\mathcal{O}_{K,p}$-linear isomorphisms

$$\beta_p^{-1}\mathfrak{D}^{-1}\mathcal{O}_{K,p}/\mathcal{O}_{K,p} \cong L_p^\vee/L_p \cong \mathfrak{m}_\Delta^{-1}/\Delta,$$

so $[\mathcal{O}_{K,p} : \beta_p\mathfrak{D}\mathcal{O}_{K,p}] = p^2$.

If p is ramified in K_1 or K_2 then it is ramified in F, and the unique prime of F above p is inert in K. From $p\mathcal{O}_F = \mathfrak{p}^2$ and $[\mathcal{O}_{K,p} : \beta_p\mathfrak{D}\mathcal{O}_{K,p}] = p^2$, we must have $\beta_p\mathfrak{D}\mathcal{O}_{K,p} = \mathfrak{P}\mathcal{O}_{K,p}$, so $\beta_p\mathcal{O}_{F,p} = \mathfrak{p}\mathfrak{D}_p^{-1}$.

Now suppose p is inert in K_1 and K_2. Similar to above, $\mathcal{O}_K$ acts on $\mathfrak{m}_\Delta^{-1}/\Delta$ through left multiplication by the image of the composition $\mathcal{O}_K \to \Delta \to \Delta/\mathfrak{m}_\Delta$, where the first map is given by $t_1 \otimes t_2 \mapsto \kappa_2(t_2)\kappa_1(t_1)$. Under the isomorphism $L_p \cong \Delta$, the action $\Delta \to \mathrm{End}_{\mathcal{O}_B}(\mathrm{Lie}(A)) \cong \overline{\mathbb{F}}_{\mathfrak{P}}$ determines an isomorphism $\gamma : \Delta/\mathfrak{m}_\Delta \to \mathbb{F}_{p^2}$ which allows us to identify $\kappa_j^{\mathrm{Lie}} : \mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B}(\mathrm{Lie}(A))$ with the composition

$$\mathcal{O}_{K_j} \xrightarrow{\kappa_j} \Delta \to \Delta/\mathfrak{m}_\Delta \xrightarrow{\gamma} \mathbb{F}_{p^2}.$$

However, the map $\mathcal{O}_K \to \overline{\mathbb{F}}_{\mathfrak{P}}$ defined by $t_1 \otimes t_2 \mapsto \kappa_1^{\mathrm{Lie}}(t_1)\kappa_2^{\mathrm{Lie}}(t_2)$ is precisely the structure map $\mathcal{O}_K \to \mathbb{F}_{\mathfrak{P}} \hookrightarrow \overline{\mathbb{F}}_{\mathfrak{P}}$ (this is the CM normalization condition), whose kernel is $\mathfrak{P}$. It then follows from the factorization of κ_j^{Lie} above that any element of $\mathfrak{P}$ acts trivially on $\mathfrak{m}_\Delta^{-1}/\Delta$. Therefore there are isomorphisms of $\mathcal{O}_{K,p}$-modules

$$\mathcal{O}_{K,p}/\mathfrak{P}\mathcal{O}_{K,p} \cong \mathfrak{m}_\Delta^{-1}/\Delta \cong \beta_p^{-1}\mathfrak{D}^{-1}\mathcal{O}_{K,p}/\mathcal{O}_{K,p},$$

which shows $\beta_p\mathfrak{D}\mathcal{O}_{K,p} = \mathfrak{P}\mathcal{O}_{K,p}$ and thus $\beta_p\mathcal{O}_{F,p} = \mathfrak{p}\mathfrak{D}_p^{-1}$.

Next suppose $p \mid d_B$, and first assume A_1 and A_2 are of the same type, where $A_j \cong M_j \otimes_{\mathcal{O}_{K_j}} E_j$ for some supersingular CM elliptic curve E_j over $\overline{\mathbb{F}}_{\mathfrak{P}}$. As mentioned above we identify $\mathcal{O}_{K_1,p}$ and $\mathcal{O}_{K_2,p}$, and call this ring $\mathcal{O}_L$. By assumption there is a $\Delta \otimes_{\mathbb{Z}_p} \mathcal{O}_L$-linear isomorphism $f : D(A_1) \to D(A_2)$. Then there is an isomorphism of $\mathbb{Z}_p$-modules

$$G : \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) \to \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1))$$

given by $\varphi \mapsto f^{-1} \circ \varphi$. Also, there are two maps $\mathcal{O}_L \rightrightarrows \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1))$, the first being κ_1 and the second $(f^{-1})_*(\kappa_2)$. However, since f is $\mathcal{O}_L$-linear,

$$(f^{-1})_*(\kappa_2(x)) = f^{-1} \circ \kappa_2(x) \circ f = f^{-1} \circ f \circ \kappa_1(x) = \kappa_1(x),$$

so under the isomorphism G, the two CM actions κ_1 and κ_2 are identified with a single action $\mathcal{O}_L \to \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1))$.

It follows from the above discussion that we may reduce to the case where $\mathbf{A}_1$ and $\mathbf{A}_2$ have the same underlying false elliptic curve $A \cong M \otimes_{\mathcal{O}_{K_j}} E$ and $\kappa_1 = \kappa_2 = \kappa$. If we fix the embedding $\mathcal{O}_L \cong \mathbb{Z}_{p^2} \hookrightarrow \Delta \cong \mathrm{End}_{\mathscr{D}}(D(E))$, the CM action on E, then there is an isomorphism

$$L_p = \mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong R_{11}$$

with $\kappa : \mathcal{O}_L \to R_{11}$ given by $\kappa(x) = \mathrm{diag}(x, x)$, and the quadratic form $\deg^*$ on L_p is identified with the quadratic form Q on R_{11} given by

$$Q \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix} = x\overline{x} - p^2 y\overline{y}.$$

The dual lattice of R_{11} relative to Q is

$$R_{11}^\vee = \left\{ \begin{bmatrix} x & p^{-2}y\Pi \\ p^{-1}y\Pi & x \end{bmatrix} : x, y \in \mathbb{Z}_{p^2} \right\},$$

so $[R_{11}^\vee : R_{11}] = p^4$. Since there are isomorphisms of $\mathcal{O}_{K,p}$-modules

$$\beta_p^{-1}\mathfrak{D}^{-1}\mathcal{O}_{K,p}/\mathcal{O}_{K,p} \cong L_p^\vee/L_p \cong R_{11}^\vee/R_{11},$$

we obtain $[\mathcal{O}_{K,p} : \beta_p\mathfrak{D}\mathcal{O}_{K,p}] = p^4$.

Under the isomorphism $L_p \cong R_{11}$ there is an action $R_{11} \to \mathrm{End}_\Delta(\mathrm{Lie}(A)) \cong \overline{\mathbb{F}}_{\mathfrak{P}}$, and a computation in coordinates shows that any element of

$$\mathfrak{M} = \left\{ \begin{bmatrix} px & y\Pi \\ py\Pi & px \end{bmatrix} : x, y \in \mathbb{Z}_{p^2} \right\} \subset R_{11}, \tag{7.2.2}$$

a maximal ideal of R_{11}, acts trivially on $D(A)/\mathscr{V}D(A) \cong \mathrm{Lie}(A)$, which shows $\mathfrak{M} = \ker(R_{11} \to \overline{\mathbb{F}}_{\mathfrak{P}})$. Hence, the action $R_{11} \to \mathrm{End}_\Delta(\mathrm{Lie}(A))$ determines an isomorphism $\gamma : R_{11}/\mathfrak{M} \to \mathbb{F}_{p^2}$, which allows us to identify $\kappa^{\mathrm{Lie}} : \mathcal{O}_L \to \mathrm{End}_\Delta(\mathrm{Lie}(A))$ with the composition

$$\mathcal{O}_L \xrightarrow{\kappa} R_{11} \to R_{11}/\mathfrak{M} \xrightarrow{\gamma} \mathbb{F}_{p^2}.$$

However, the map $\mathcal{O}_K \to \overline{\mathbb{F}}_{\mathfrak{P}}$ defined by $t_1 \otimes t_2 \mapsto \kappa^{\mathrm{Lie}}(t_1)\kappa^{\mathrm{Lie}}(t_2)$ is the structure map $\mathcal{O}_K \to \mathbb{F}_{\mathfrak{P}} \hookrightarrow \overline{\mathbb{F}}_{\mathfrak{P}}$ by the CM normalization condition, so its kernel is $\mathfrak{P}$. It follows from the factorization of κ^{Lie} above that if $t_1 \otimes t_2 \in \mathfrak{P}^2$ then $\kappa(t_2)\kappa(t_1) \in \mathfrak{M}^2$. But $\kappa(t_j) = \mathrm{diag}(t_j, t_j)$, so $t_2 t_1 \in p^2\mathbb{Z}_{p^2}$ for $t_1 \otimes t_2 \in \mathfrak{P}^2$. Then for

$$\varphi = \begin{bmatrix} x & p^{-2}y\Pi \\ p^{-1}y\Pi & x \end{bmatrix} \in R_{11}^{\vee}$$

and $t_1 \otimes t_2 \in \mathfrak{P}^2$, under the action of $\mathcal{O}_{K,p} \cong \mathcal{O}_L \otimes_{\mathbb{Z}} \mathcal{O}_L$ on L_p defined above,

$$(t_1 \otimes t_2) \bullet \varphi = \kappa(t_2)\varphi\kappa(\bar{t}_1) = \begin{bmatrix} t_2\bar{t}_1 x & p^{-2}t_2 t_1 y\Pi \\ p^{-1}t_2 t_1 y\Pi & t_2\bar{t}_1 x \end{bmatrix} \in R_{11}$$

since $t_2 t_1 \in p^2\mathbb{Z}_{p^2}$. This shows $\mathfrak{P}^2$ acts trivially on $R_{11}^{\vee}/R_{11}$, and conversely, reversing this argument shows that any element of $\mathcal{O}_{K,p}$ acting trivially on $R_{11}^{\vee}/R_{11}$ is in $\mathfrak{P}^2$. Hence there is an $\mathcal{O}_{K,p}$-linear map $\mathcal{O}_{K,p}/\mathfrak{P}^2\mathcal{O}_{K,p} \hookrightarrow R_{11}^{\vee}/R_{11}$ given by $x \mapsto x \bullet 1$. But $\mathfrak{P}^2$ has norm $p^4 = [R_{11}^{\vee} : R_{11}]$, so there are isomorphisms of $\mathcal{O}_{K,p}$-modules

$$\mathcal{O}_{K,p}/\mathfrak{P}^2\mathcal{O}_{K,p} \cong R_{11}^{\vee}/R_{11} \cong \beta_p^{-1}\mathfrak{D}^{-1}\mathcal{O}_{K,p}/\mathcal{O}_{K,p}.$$

It follows that $\beta_p\mathfrak{D}\mathcal{O}_{K,p} = \mathfrak{P}^2\mathcal{O}_{K,p}$ and thus $\beta_p\mathcal{O}_{F,p} = \mathfrak{p}^2\mathfrak{D}_p^{-1}$.

Next assume A_1 and A_2 are not of the same type, with $A_j \cong M_j \otimes_{\mathcal{O}_{K_j}} E_j$. As before we identify $\mathcal{O}_{K_1,p}$ with $\mathcal{O}_{K_2,p}$ and call this ring $\mathcal{O}_L$. Let $\mathfrak{g}$ be the connected p-divisible group of height 2 and dimension 1 over $\overline{\mathbb{F}}_{\mathfrak{P}}$. Isomorphisms $E_j[p^\infty] \cong \mathfrak{g}$ may be chosen in such a way that the CM actions $g_1 : \mathcal{O}_L \to \mathrm{End}(E_1[p^\infty]) \cong \Delta$ and $g_2 : \mathcal{O}_L \to \mathrm{End}(E_2[p^\infty]) \cong \Delta$ have the same image in Δ. (There are two $\Delta^\times$-conjugacy classes of ring embeddings $\mathbb{Z}_{p^2} \hookrightarrow \Delta$ interchanged by precomposing with the nontrivial element of $\mathrm{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$.) Fix an embedding $\mathbb{Z}_{p^2} \hookrightarrow \Delta$ and a uniformizer $\Pi \in \Delta$ satisfying $\Pi g_1(x) = g_1(\overline{x})\Pi$ for all $x \in \mathcal{O}_L$. By Lemma 6.2.2 and Proposition 7.2.4 there are isomorphisms of $\mathbb{Z}_p$-modules

$$L_p \cong \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{D}}(D(A_1), D(A_2)) \cong R_{12},$$

and the quadratic form $\deg^*$ on L_p is identified with the quadratic form uQ' on R_{12}, where $u \in \mathbb{Z}_p^\times$ and

$$Q' \begin{bmatrix} px & y\Pi \\ y\Pi & x \end{bmatrix} = p(x\overline{x} - y\overline{y}).$$

The dual lattice of R_{12} relative to uQ' is

$$R_{12}^{\vee} = u^{-1} \cdot \left\{ \begin{bmatrix} x & p^{-1}y\Pi \\ p^{-1}y\Pi & p^{-1}x \end{bmatrix} : x, y \in \mathbb{Z}_{p^2} \right\},$$

so $[R_{12}^\vee : R_{12}] = p^4$. As before this gives $[\mathcal{O}_{K,p} : \beta_p \mathfrak{D}\mathcal{O}_{K,p}] = p^4$. Fixing ring isomorphisms

$$\mathrm{End}_{\mathcal{O}_B}(A_1) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong R_{11} \cong \mathrm{End}_{\mathcal{O}_B}(A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_p,$$

it makes sense to take the product $\kappa_2(t_2)\kappa_1(t_1)$ in R_{11} for $t_1, t_2 \in \mathcal{O}_L$, and

$$\kappa_2(t_2)\kappa_1(t_1) = \mathrm{diag}(g_2(t_2)g_1(t_1), g_2(t_2)g_1(t_1)),$$

where $g_2(t_2)g_1(t_1)$ is the product in the common image of g_1 and g_2 in Δ. As in the case of A_1 and A_2 having the same type, the action $R_{11} \to \mathrm{End}_\Delta(\mathrm{Lie}(A_j)) \cong \overline{\mathbb{F}}_{\mathfrak{P}}$, for $j = 1, 2$, determines an isomorphism $\gamma_j : R_{11}/\mathfrak{M} \to \mathbb{F}_{p^2}$, which allows us to identify $\kappa_j^{\mathrm{Lie}} : \mathcal{O}_L \to \mathrm{End}_\Delta(\mathrm{Lie}(A_j))$ with the composition

$$\mathcal{O}_L \xrightarrow{\kappa_j} R_{11} \to R_{11}/\mathfrak{M} \xrightarrow{\gamma_j} \mathbb{F}_{p^2}.$$

As above, the map $\mathcal{O}_K \to \overline{\mathbb{F}}_{\mathfrak{P}}$ defined by $t_1 \otimes t_2 \mapsto \kappa_1^{\mathrm{Lie}}(t_1)\kappa_2^{\mathrm{Lie}}(t_2)$ is the structure map $\mathcal{O}_K \to \mathbb{F}_{\mathfrak{P}} \hookrightarrow \overline{\mathbb{F}}_{\mathfrak{P}}$. Therefore $t_1 \otimes t_2 \in \mathfrak{P}$ if and only if $\kappa_1^{\mathrm{Lie}}(t_1)\kappa_2^{\mathrm{Lie}}(t_2) = 0$, if and only if $\kappa_2(t_2)\kappa_1(t_1) \in \mathfrak{M}$.

Let $\overline{\mathfrak{P}}$ be the other prime ideal of $\mathcal{O}_K$ lying over p, so $\overline{\mathfrak{P}} \cap \mathcal{O}_F = \overline{\mathfrak{p}}$. Write $\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \tau_1, \tau_2, \tau_1\tau_2\}$, where $K_j = K^{\langle \tau_j \rangle}$ and $F = K^{\langle \tau_1\tau_2 \rangle}$. If $D(\mathfrak{P}|p)$ is the decomposition group at $\mathfrak{P}$ for $K/\mathbb{Q}$, then since $\mathfrak{p}$ is inert in K and $\mathrm{Gal}(K/F) = \langle \tau_1\tau_2 \rangle$,

$$D(\mathfrak{P}|p) \cap \langle \tau_1\tau_2 \rangle = D(\mathfrak{P}|\mathfrak{p}) = \langle \tau_1\tau_2 \rangle,$$

but $|D(\mathfrak{P}|p)| = 2$, so $D(\mathfrak{P}|p) = \langle \tau_1\tau_2 \rangle$. Hence $\tau_j(\mathfrak{P}) = \overline{\mathfrak{P}}$ for $j = 1, 2$, which means $t_1 \otimes t_2 \in \overline{\mathfrak{P}} = \tau_1(\mathfrak{P})$ if and only if $\bar{t}_1 \otimes t_2 \in \mathfrak{P}$. Now, for

$$\varphi = u^{-1} \cdot \begin{bmatrix} x & p^{-1}y\Pi \\ p^{-1}y\Pi & p^{-1}x \end{bmatrix} \in R_{12}^\vee$$

and $t_1 \otimes t_2 \in \mathcal{O}_{K,p}$,

$$(t_1 \otimes t_2) \bullet \varphi = \kappa_2(t_2)\varphi\kappa_1(\bar{t}_1) = u^{-1} \cdot \begin{bmatrix} g_2(t_2)g_1(\bar{t}_1)x & p^{-1}g_2(t_2)g_1(t_1)y\Pi \\ p^{-1}g_2(t_2)g_1(t_1)y\Pi & p^{-1}g_2(t_2)g_1(\bar{t}_1)x \end{bmatrix}.$$

Therefore

$$\begin{aligned} (t_1 \otimes t_2) \bullet \varphi \in R_{12} \text{ for all } \varphi &\iff g_2(t_2)g_1(t_1) \in p\mathbb{Z}_{p^2} \text{ and } g_2(t_2)g_1(\bar{t}_1) \in p\mathbb{Z}_{p^2} \\ &\iff \kappa_2(t_2)\kappa_1(t_1) \in \mathfrak{M} \text{ and } \kappa_2(t_2)\kappa_1(\bar{t}_1) \in \mathfrak{M} \\ &\iff t_1 \otimes t_2 \in \mathfrak{P} \cap \overline{\mathfrak{P}} = \mathfrak{P}\overline{\mathfrak{P}}. \end{aligned}$$

This shows an element of $\mathcal{O}_{K,p}$ acts trivially on $R_{12}^\vee/R_{12}$ if and only if it is in $\mathfrak{P}\overline{\mathfrak{P}}$. Since $[R_{12}^\vee : R_{12}] = p^4$ is the norm of $\mathfrak{P}\overline{\mathfrak{P}}$, similar to above we obtain $\beta_p\mathcal{O}_{F,p} = \mathfrak{p}\overline{\mathfrak{p}}\mathfrak{D}_p^{-1}$. □

Corollary 7.2.6. *Let $A \in \mathscr{Y}_j(\overline{\mathbb{F}}_p)$. For any prime number ℓ there is an isomorphism of rings*

$$\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \begin{cases} \mathrm{M}_2(\mathbb{Z}_\ell) & \text{if } \ell \neq p \text{ and } \ell \nmid d_B \\ \mathcal{O}_{B,\ell} & \text{if } \ell \neq p \text{ and } \ell \mid d_B \\ \Delta & \text{if } \ell = p \text{ and } p \nmid d_B \\ R_2 & \text{if } \ell = p \text{ and } p \mid d_B, \end{cases}$$

where Δ is the maximal order in the quaternion division algebra over $\mathbb{Q}_p$ and

$$R_2 = \begin{bmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p^2\mathbb{Z}_p & \mathbb{Z}_p \end{bmatrix}.$$

Proposition 7.2.7. *For $p \mid d_B$ let w_p be the corresponding element of the Atkin-Lehner group W_0, so $w_p = \Pi$ is a uniformizer in $\Delta \cong \mathcal{O}_{B,p}$. Let $(A, i, \kappa) \in \mathscr{Y}_j(\overline{\mathbb{F}}_p)$ and set $A' = w_p \cdot A \in \mathscr{Y}_j(\overline{\mathbb{F}}_p)$. Then $D(A)$ and $D(A')$ are not isomorphic as $\Delta \otimes_{\mathbb{Z}_p} \mathcal{O}_{K_j,p}$-modules.*

Proof. This is essentially a claim we made when discussing the action of W_0 on the set $\mathscr{L}_j'$ defined above, that w_p interchanges the two isomorphism classes of $\Delta \otimes_{\mathbb{Z}_p} \mathcal{O}_{K_j,p}$-modules. However, we will include a proof for completeness. Recall that $A' = (A, i', \kappa)$ where $i' : \Delta \to \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is given by $i'(x) = i(\Pi x \Pi^{-1}) = i(\Pi) \circ i(x) \circ i(\Pi)^{-1}$. Suppose there is a Δ-linear isomorphism $D(A) \cong D(A') = D(A)$. Then there is a $u \in \mathrm{End}_{\mathscr{D}}(D(A))^\times$ such that $i'(x) = u \circ i(x) \circ u^{-1}$ for all $x \in \Delta$, viewing $i(x)$ and $i'(x)$ as their induced endomorphisms of $D(A)$. Therefore conjugation by u on $i(\Delta) \subset \mathrm{End}_{\mathscr{D}}(D(A))$ is equal to conjugation by $i(\Pi)$, which means $i(\Pi) = u \circ z$ for some $z \in Z(i(\Delta))$, the center of $i(\Delta)$. However, $i(\Delta) \cong \Delta$ has center $\mathbb{Z}_p$, so $z \in \mathbb{Z}_p \subset \mathrm{M}_2(\Delta)$. Viewing $i(\Pi)$, u, and z as their corresponding endomorphisms of A, we have $\deg(i(\Pi)) = \mathrm{Nrd}(\Pi)^2 = p^2$ and $\deg(u \circ z) = \deg(z) = p^{4k}$ for some integer $k \geqslant 0$ since $\deg([p]) = p^4$. This is a contradiction. □

If $A \in \mathscr{Y}_j(\overline{\mathbb{F}}_p)$ for $p \mid d_B$ and $\mathfrak{m}_p \subset \mathcal{O}_B$ is the unique maximal ideal of residue characteristic p, then the $\mathfrak{m}_p$-torsion $A[\mathfrak{m}_p]$ is defined just as $A[\mathfrak{m}_\ell]$.

Lemma 7.2.8. *Suppose $(A, i) \in \mathscr{Y}_j(\overline{\mathbb{F}}_p)$ with $p \mid d_B$. There is an isomorphism of $\mathcal{O}_B/\mathfrak{m}_p$-algebras $\mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p}(A[\mathfrak{m}_p]) \cong \mathcal{O}_B/\mathfrak{m}_p$.*

Proof. We will use Dieudonné modules. Since $A[p]$ and $A[\mathfrak{m}_p]$ are finite p-group schemes over $\mathrm{Spec}(\overline{\mathbb{F}}_p)$, they have associated covariant Dieudonné modules $D(A[p])$ and $D(A[\mathfrak{m}_p])$, which are $\mathscr{D}$-modules of length 4 and 2 over W, respectively. Viewing $A[p]$ and $A[\mathfrak{m}_p]$ as *fppf* sheaves of abelian groups on $\mathbf{Sch}/\overline{\mathbb{F}}_p$, there is an exact sequence

$$0 \to A[\mathfrak{m}_p] \to A[p] \xrightarrow{i(x_p)} A[p] \to 0,$$

where x_p is any element of $\mathfrak{m}_p$ whose image generates the principal ideal $\mathfrak{m}_p/p\mathcal{O}_B \subset \mathcal{O}_B/p\mathcal{O}_B$. Since D is an exact functor, we obtain an exact sequence of $\mathscr{D}$-modules

$$0 \to D(A[\mathfrak{m}_p]) \to D(A[p]) \xrightarrow{i(x_p)} D(A[p]) \to 0.$$

By definition, $D(A) = \varprojlim_n D(A[p^n])$ where the inverse limit is with respect to the maps $[p] : A[p^{n+1}] \to A[p^n]$. Hence there is an isomorphism of $\mathscr{D}$-modules $D(A[p]) \cong D(A)/pD(A)$, and under this isomorphism the map $i(x_p) : D(A[p]) \to D(A[p])$ is identified with the map $i(\Pi) : D(A)/pD(A) \to D(A)/pD(A)$, where $\Pi \in \mathcal{O}_{B,p}$ is a uniformizer. It follows that $D(A[\mathfrak{m}_p]) \cong D_p$, where

$$D_p = \ker(i(\Pi) : D(A)/pD(A) \to D(A)/pD(A)),$$

and thus, since D is an equivalence of categories,

$$\mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p}(A[\mathfrak{m}_p]) \cong \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p \otimes_{\mathbb{Z}} \mathscr{D}}(D_p).$$

Using a standard W-basis for $D(A)$ as in Proposition 6.3.2, and considering the two possible forms (6.3.2) for i, one sees that $D(A[\mathfrak{m}_p])$ is in particular an $\overline{\mathbb{F}}_p$-vector space of dimension 2. A computation in coordinates, similar to that done in Lemma 7.2.1, then shows

$$\mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p \otimes_{\mathbb{Z}} \mathscr{D}}(D_p) \cong \mathbb{F}_{p^2}.$$

Therefore the action $i : \mathcal{O}_B/\mathfrak{m}_p \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p}(A[\mathfrak{m}_p])$ is an isomorphism of $\mathcal{O}_B/\mathfrak{m}_p$-algebras. □

Corollary 7.2.9. *Suppose $(A, i) \in \mathscr{Y}_j(k)$ for $k = \mathbb{C}$ or $k = \overline{\mathbb{F}}_p$. There is an isomorphism of $\mathcal{O}_B/\mathfrak{m}_B$-algebras $\mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(A[\mathfrak{m}_B]) \cong \mathcal{O}_B/\mathfrak{m}_B$.*

Proof. For each prime $\ell \mid d_B$ let x_ℓ be an element of $\mathfrak{m}_\ell$ whose image generates the principal ideal $\mathfrak{m}_\ell/\ell\mathcal{O}_B \subset \mathcal{O}_B/\ell\mathcal{O}_B$. Under the isomorphism $\mathcal{O}_B/d_B\mathcal{O}_B \to \prod_{\ell \mid d_B} \mathcal{O}_B/\ell\mathcal{O}_B$ the ideal $\mathfrak{m}_B/d_B\mathcal{O}_B$ is sent to the ideal $\prod_{\ell \mid d_B} \mathfrak{m}_\ell/\ell\mathcal{O}_B$, and this principal ideal is generated by the image of $x_B = \prod_{\ell \mid d_B} x_\ell \in \mathfrak{m}_B$. There is then an isomorphism of group schemes over $\mathrm{Spec}(k)$

$$f : A[\mathfrak{m}_B] \to \prod_{\ell \mid d_B} A[\mathfrak{m}_\ell],$$

where the right side is an r-fold fiber product over $\mathrm{Spec}(k)$ (r is the number of primes dividing d_B). The map f is determined by the morphisms $A[\mathfrak{m}_B] \to A[\mathfrak{m}_\ell]$ given on k-points by $a \mapsto i(x_\ell^{-1}x_B)(a)$. The inverse of f is given on points by $(a_1, \ldots, a_r) \mapsto a_1 + \cdots + a_r$, adding in the group $A[\mathfrak{m}_B](k)$. The isomorphism f induces an isomorphism of $\mathcal{O}_B/\mathfrak{m}_B$-algebras

$$\mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_B}(A[\mathfrak{m}_B]) \to \prod_{\ell \mid d_B} \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_\ell}(A[\mathfrak{m}_\ell]) \cong \prod_{\ell \mid d_B} \mathcal{O}_B/\mathfrak{m}_\ell \cong \mathcal{O}_B/\mathfrak{m}_B. \qquad \square$$

Proposition 7.2.10. *Let* $(\mathbf{A}_1, \mathbf{A}_2) \in \mathscr{X}_\theta(\overline{\mathbb{F}}_\mathfrak{P})$ *with* $\mathfrak{P}$ *lying over* $p \mid d_B$. *Then* $\mathfrak{P}$ *divides* $\ker(\theta)$ *if and only if* A_1 *and* A_2 *are of the same type.*

Proof. Suppose A_1 and A_2 are of the same type. The proof essentially follows the part of the proof of Proposition 7.2.5 starting around (7.2.2). Since A_1 and A_2 are of the same type, there is an isomorphism of $\mathbb{Z}_p$-modules $L_p = L_p(\mathbf{A}_1, \mathbf{A}_2) \cong R_{11}$. Fix ring isomorphisms

$$\mathrm{End}_{\mathcal{O}_B}(A_1) \otimes_\mathbb{Z} \mathbb{Z}_p \cong R_{11} \cong \mathrm{End}_{\mathcal{O}_B}(A_2) \otimes_\mathbb{Z} \mathbb{Z}_p.$$

For $j \in \{1, 2\}$, under the action

$$R_{11} \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p}(A_j[\mathfrak{m}_p]) \cong \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p \otimes_\mathbb{Z} \mathscr{D}}(D(A_j[\mathfrak{m}_p])) \cong \mathbb{F}_{p^2},$$

any element of

$$\mathfrak{M} = \left\{ \begin{bmatrix} px & y\Pi \\ py\Pi & px \end{bmatrix} : x, y \in \mathbb{Z}_{p^2} \right\} \subset R_{11}$$

acts trivially on

$$D(A_j[\mathfrak{m}_p]) = \ker(i_j(\Pi) : D(A_j)/pD(A_j) \to D(A_j)/pD(A_j)),$$

so $\mathfrak{M} = \ker(R_{11} \to \mathbb{F}_{p^2})$. It follows that the map $R_{11} \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p}(A_j[\mathfrak{m}_p])$ determines an isomorphism $\gamma_j : R_{11}/\mathfrak{M} \to \mathbb{F}_{p^2}$ which allows us to identify $\kappa_j^{\mathfrak{m}_p} : \mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p}(A_j[\mathfrak{m}_p])$ with the composition

$$\mathcal{O}_{K_j} \xrightarrow{\kappa_j} R_{11} \to R_{11}/\mathfrak{M} \xrightarrow{\gamma_j} \mathbb{F}_{p^2}.$$

Let $\mathfrak{Q} \subset \mathcal{O}_K$ be the prime over p dividing $\ker(\theta)$, so $\mathfrak{Q}$ is the kernel of the map $\mathcal{O}_K \to \mathbb{F}_{p^2}$ defined by $t_1 \otimes t_2 \mapsto \kappa_1^{\mathfrak{m}_p}(t_1)\kappa_2^{\mathfrak{m}_p}(t_2)$. Now, using the factorization of $\kappa_j^{\mathfrak{m}_p}$ given above and following the rest of this part of the proof of Proposition 7.2.5 (adjusting slightly for the fact that κ_1 and κ_2 are not equal here, similar to what is done in the mixed type case later in that proof), we find that an element of $\mathcal{O}_{K,p}$ acts trivially on $L_p^\vee/L_p$ if and only if it is in $\mathfrak{Q}^2$. However, the same is true for $\mathfrak{P}$

in place of $\mathfrak{Q}$, so $\mathfrak{Q}^2 = \mathfrak{P}^2$ and therefore $\mathfrak{P} = \mathfrak{Q}$.

Now suppose A_1 and A_2 are not of the same type. Define a ring homomorphism $\eta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ according to

$$\eta_j^{\mathfrak{m}_\ell} : \mathcal{O}_{K_j} \to \mathcal{O}_B/\mathfrak{m}_\ell$$

being defined by $\eta_j^{\mathfrak{m}_\ell} = \theta_j^{\mathfrak{m}_\ell}$ for all $\ell \neq p$ and $j = 1, 2$, $\eta_1^{\mathfrak{m}_p} = \theta_1^{\mathfrak{m}_p}$, and $\eta_2^{\mathfrak{m}_p}(x) = \theta_2^{\mathfrak{m}_p}(\overline{x})$. Consider the CM pair $(\mathbf{A}_1, \mathbf{A}_2')$, where $\mathbf{A}_2' = w_p \cdot \mathbf{A}_2$ and w_p is the Atkin-Lehner operator at p. The map

$$(\kappa_2')^{\mathfrak{m}_p} : \mathcal{O}_{K_2} \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p}(A_2'[\mathfrak{m}_p]) \cong \mathcal{O}_B/\mathfrak{m}_p$$

is given by $(\kappa_2')^{\mathfrak{m}_p}(x) = \kappa_2^{\mathfrak{m}_p}(\overline{x})$, where

$$\kappa_2^{\mathfrak{m}_p} : \mathcal{O}_{K_2} \to \mathrm{End}_{\mathcal{O}_B/\mathfrak{m}_p}(A_2[\mathfrak{m}_p]) \cong \mathcal{O}_B/\mathfrak{m}_p.$$

The resulting map $\mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_p$ for the pair $(\mathbf{A}_1, \mathbf{A}_2')$ is given by

$$t_1 \otimes t_2 \mapsto \kappa_1^{\mathfrak{m}_p}(t_1)\kappa_2^{\mathfrak{m}_p}(\bar{t}_2),$$

so $(\mathbf{A}_1, \mathbf{A}_2') \in \mathscr{X}_\eta(\overline{\mathbb{F}}_{\mathfrak{P}})$ and the kernel of this map is $\overline{\mathfrak{Q}}$, where $\mathfrak{Q}$ is the prime over p dividing $\ker(\theta)$. As A_1 and $w_p \cdot A_2$ are of the same type (Proposition 7.2.7), $\overline{\mathfrak{Q}} = \mathfrak{P}$ by the first part of the proof applied to $(\mathbf{A}_1, \mathbf{A}_2')$, so $\mathfrak{P}$ does not divide $\ker(\theta)$. □

7.3 Cases combined

Let $(\mathbf{A}_1, \mathbf{A}_2) \in \mathscr{X}_\theta(\overline{\mathbb{F}}_{\mathfrak{P}})$ with $\mathfrak{P}$ lying over some prime p, and let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$. Set $\mathfrak{a}_\theta = \ker(\theta) \cap \mathcal{O}_F$.

Theorem 7.3.1. *For any finite idele $\beta \in \widehat{F}^\times$ satisfying $\beta\widehat{\mathcal{O}}_F = \mathfrak{a}_\theta\mathfrak{p}\mathfrak{D}^{-1}\widehat{\mathcal{O}}_F$, there is a $\widehat{K}$-linear isomorphism of $\widehat{F}$-quadratic spaces*

$$(\widehat{V}(\mathbf{A}_1, \mathbf{A}_2), \deg_{\mathrm{CM}}) \cong (\widehat{K}, \beta \cdot \mathrm{N}_{K/F})$$

taking $\widehat{L}(\mathbf{A}_1, \mathbf{A}_2)$ isomorphically to $\widehat{\mathcal{O}}_K$.

Proof. Combining Propositions 7.1.2 and 7.2.5, and Proposition 7.2.10 proves the claim for some $\beta \in \widehat{F}^\times$ satisfying $\beta\widehat{\mathcal{O}}_F = \mathfrak{a}_\theta\mathfrak{p}\mathfrak{D}^{-1}\widehat{\mathcal{O}}_F$, and the surjectivity of the norm map $\widehat{\mathcal{O}}_K^\times \to \widehat{\mathcal{O}}_F^\times$ gives the result for all such β. □

Recall the definitions of the functions ρ and ρ_ℓ from the introduction.

Proposition 7.3.2. *Let ℓ be a prime number. For any $\alpha \in F_\ell^\times$,*

$$O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2) = \begin{cases} \rho_\ell(\alpha \mathfrak{D}_\ell) & \text{if } \ell \neq p,\ \ell \nmid d_B \\ \rho_\ell(\alpha \mathfrak{l}(\ell)^{-1}\mathfrak{D}_\ell) & \text{if } \ell \neq p,\ \ell \mid d_B \\ \rho_p(\alpha \mathfrak{p}^{-1}\mathfrak{l}(p)^{-1}\mathfrak{D}_p) & \text{if } \ell = p, \end{cases}$$

where $\mathfrak{l}(\ell)$ is the prime over ℓ dividing $\mathfrak{a}_\theta$, with the convention that $\mathfrak{l}(p) = \mathcal{O}_F$ if $p \nmid d_B$.

Proof. Using Propositions 7.1.2 and 7.2.5 in place of Lemmas 2.10 and 2.11 of [14], the proof is identical to that of [14, Lemmas 2.19, 2.20]. Let us prove one case to give a sample of these types of calculations. Suppose $\ell \neq p$ and $\ell \nmid d_B$. By Proposition 7.1.2 there is an isomorphism

$$(V_\ell(\mathbf{A}_1, \mathbf{A}_2, \deg_{\mathrm{CM}}) \cong (K_\ell, \beta_\ell \cdot \mathrm{N}_{K_\ell/F_\ell}),$$

where $\beta_\ell \in F_\ell^\times$ satisfies $\beta_\ell \mathcal{O}_{F,\ell} = \mathfrak{D}_\ell^{-1}$. It follows from Lemma 4.0.8 that there is an isomorphism

$$\mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell \cong T^1(\mathbb{Q}_\ell)/V_\ell,$$

so the orbital integral can be written as

$$O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2) = \sum_{t \in T^1(\mathbb{Q}_\ell)/V_\ell} \mathbf{1}_{\mathcal{O}_{K,\ell}}(t^{-1}f)$$

if there is an $f \in K_\ell$ satisfying $\mathrm{N}_{K_\ell/F_\ell}(f) = \alpha\beta_\ell^{-1}$, and $O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2) = 0$ otherwise. Suppose ℓ is inert in K_1 and K_2, so $\mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell = \{1\}$. Then $O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2) = 1$ if there is an $f \in K_\ell$ satisfying $\mathrm{N}_{K_\ell/F_\ell}(f) = \alpha\beta_\ell^{-1}$ and $O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2) = 0$ otherwise. Hence $O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2) = \rho_\ell(\alpha\mathfrak{D}_\ell)$ since both sides are equal to 1 if $\mathrm{ord}_v(\alpha\beta_\ell^{-1})$ is even and non-negative for both places v of F above ℓ, and otherwise both sides are zero (K_v/F_v is unramified and $\beta_\ell^{-1}\mathcal{O}_{F,\ell} = \mathfrak{D}_\ell$). See [14, Lemmas 2.19, 2.20] for the other cases. □

Theorem 7.3.3. *For any $\alpha \in F^\times$ we have*

$$\prod_\ell O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2) = \rho(\alpha\mathfrak{a}_\theta^{-1}\mathfrak{p}^{-1}\mathfrak{D}).$$

Proof. This follows from the previous proposition and the product expansion for ρ. □

Chapter 8

Deformation theory II

This chapter is devoted to the calculation of the length of the local ring $\mathscr{O}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}$, which relies on the deformation theory of objects $(\mathbf{A}_1, \mathbf{A}_2, f)$ of $\mathscr{X}_{\theta,\alpha}(\overline{\mathbb{F}}_{\mathfrak{P}})$. We continue with the notation of Chapter 5.

8.1 General theory

Definition 8.1.1. Let $(\mathbf{A}_1, \mathbf{A}_2)$ be a CM pair over $\overline{\mathbb{F}}_{\mathfrak{P}}$ and $R \in \mathbf{CLN}$. A *deformation* of $(\mathbf{A}_1, \mathbf{A}_2)$ to R is a CM pair $(\widetilde{\mathbf{A}}_1, \widetilde{\mathbf{A}}_2)$ over R together with an isomorphism of CM pairs $(\widetilde{\mathbf{A}}_1, \widetilde{\mathbf{A}}_2)_{/\overline{\mathbb{F}}_{\mathfrak{P}}} \cong (\mathbf{A}_1, \mathbf{A}_2)$.

Given a CM pair $(\mathbf{A}_1, \mathbf{A}_2)$ over $\overline{\mathbb{F}}_{\mathfrak{P}}$, define $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2)$ to be the functor $\mathbf{CLN} \to \mathbf{Sets}$ that assigns to each $R \in \mathbf{CLN}$ the set of isomorphism classes of deformations of $(\mathbf{A}_1, \mathbf{A}_2)$ to R. By Corollary 5.1.3,

$$\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2) \cong \mathrm{Def}_{\mathcal{O}_B}(A_1, \mathcal{O}_{K_1}) \times \mathrm{Def}_{\mathcal{O}_B}(A_2, \mathcal{O}_{K_2})$$

is represented by $\mathscr{W} \widehat{\otimes}_{\mathscr{W}} \mathscr{W} \cong \mathscr{W}$. Given a nonzero $f \in L(\mathbf{A}_1, \mathbf{A}_2)$ define $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ to be the functor $\mathbf{CLN} \to \mathbf{Sets}$ that assigns to each $R \in \mathbf{CLN}$ the set of isomorphism classes of deformations of $(\mathbf{A}_1, \mathbf{A}_2, f)$ to R, where a deformation is a triple $(\widetilde{\mathbf{A}}_1, \widetilde{\mathbf{A}}_2, \widetilde{f})$ with $(\widetilde{\mathbf{A}}_1, \widetilde{\mathbf{A}}_2)$ a deformation of $(\mathbf{A}_1, \mathbf{A}_2)$ to R and $\widetilde{f} \in L(\widetilde{\mathbf{A}}_1, \widetilde{\mathbf{A}}_2)$ such that the following diagram commutes

$$\begin{tikzcd}
\widetilde{A}_1 \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \arrow[r, "\widetilde{f} \otimes \mathrm{id}"] \arrow[d, "\cong"'] & \widetilde{A}_2 \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \arrow[d, "\cong"] \\
A_1 \arrow[r, "f"] & A_2.
\end{tikzcd}$$

It follows easily that $\deg_{\mathrm{CM}}(\widetilde{f}) = \deg_{\mathrm{CM}}(f)$.

The following is the Serre-Tate theorem for false elliptic curves.

Theorem 8.1.2. *Let $R \in \mathbf{CLN}$ and suppose (A_0, i_0) is a false elliptic curve over $\overline{\mathbb{F}}_{\mathfrak{P}}$.*
(a) *The rule $(A, i) \mapsto (A[p^\infty], i[p^\infty])$ defines a bijection between the following two sets:*

(1) Isomorphism classes of false elliptic curves (A, i) over R together with an isomorphism $A \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \to A_0$ of false elliptic curves over $\overline{\mathbb{F}}_{\mathfrak{P}}$;

(2) Isomorphism classes of p-divisible groups $\mathfrak{G}$ over R with an action of $\mathcal{O}_B$, together with an $\mathcal{O}_B$-linear isomorphism $\mathfrak{G} \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \to A_0[p^\infty]$.

(b) *With the same notation, if $f_0 \in \mathrm{End}_{\mathcal{O}_B}(A_0)$ then the rule $(A, f) \mapsto (A[p^\infty], f[p^\infty])$ defines a bijection between the following two sets:*

(3) Isomorphism classes of pairs (A, f), where (A, i) is a false elliptic curve over R and $f \in \mathrm{End}_{\mathcal{O}_B}(A)$, together with an isomorphism

$$\varphi : A \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \to A_0$$

of false elliptic curves over $\overline{\mathbb{F}}_{\mathfrak{P}}$ satisfying $\varphi \circ (f \otimes \mathrm{id}) = f_0 \circ \varphi$;

(4) Isomorphism classes of pairs $(\mathfrak{G}, g)$, where $\mathfrak{G}$ is a p-divisible group over R with an action of $\mathcal{O}_B$ and $g \in \mathrm{End}_{\mathcal{O}_B}(\mathfrak{G})$, together with an $\mathcal{O}_B$-linear isomorphism

$$\psi : \mathfrak{G} \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \to A_0[p^\infty]$$

satisfying $\psi \circ (g \otimes \mathrm{id}) = f_0[p^\infty] \circ \psi$.

Proof. (a) We will define an inverse to the map $A \mapsto A[p^\infty]$. Given a p-divisible group $\mathfrak{G}$ as in (2), by the usual Serre-Tate theorem for abelian schemes, there is an abelian surface A over R and an isomorphism of abelian schemes

$$\varphi : A \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \to A_0.$$

Now let $x \in \mathcal{O}_B$. Since the isomorphism $\mathfrak{G} \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \to A_0[p^\infty]$ is compatible with the actions of $\mathcal{O}_B$ on $\mathfrak{G}$ and $A_0[p^\infty]$, by the Serre-Tate theorem there is an endomorphism $i(x)$ of A inducing $i_0(x)$ on A_0 via the isomorphism φ, and $i(x)[p^\infty]$ defines the action of x on $\mathfrak{G}$. This makes A into a false elliptic curve, and the inverse map in the bijection is given by $\mathfrak{G} \mapsto A$.

(b) Given a pair $(\mathfrak{G}, g)$ as in (4), by part (a) and the Serre-Tate theorem, there is a false elliptic curve (A, i) over R, an $f \in \mathrm{End}_R(A)$ satisfying $f[p^\infty] = g$, and an isomorphism of false elliptic curves

$$\varphi : A \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \to A_0$$

satisfying $\varphi \circ (f \otimes \mathrm{id}) = f_0 \circ \varphi$. All we need to show is that f is $\mathcal{O}_B$-linear. Let $x \in \mathcal{O}_B$. Using the $\mathcal{O}_B$-linearity of φ and f_0, we have

$$\begin{aligned}(f \otimes \mathrm{id}) \circ (i(x) \otimes \mathrm{id}) &= \varphi^{-1} \circ f_0 \circ \varphi \circ (i(x) \otimes \mathrm{id}) \\ &= \varphi^{-1} \circ f_0 \circ i_0(x) \circ \varphi \\ &= \varphi^{-1} \circ i_0(x) \circ f_0 \circ \varphi \\ &= (i(x) \otimes \mathrm{id}) \circ \varphi^{-1} \circ f_0 \circ \varphi \\ &= (i(x) \otimes \mathrm{id}) \circ (f \otimes \mathrm{id}),\end{aligned}$$

and thus $f \circ i(x) = i(x) \circ f$. The map $(\mathfrak{G}, g) \mapsto (A, f)$ is the inverse in the bijection. □

The most useful case of part (b) for us will be the following. Let R be an object of **CLN**. A *CM p-divisible group with an action of $\mathcal{O}_B$* over R is a triple $(\mathfrak{G}, g_0, g)$, where $\mathfrak{G}$ is a p-divisible group over R, $g_0 : \mathcal{O}_B \to \mathrm{End}_R(\mathfrak{G})$ is an action of $\mathcal{O}_B$, and $g : \mathcal{O}_{K_j} \to \mathrm{End}_{\mathcal{O}_B}(\mathfrak{G})$ is an action of $\mathcal{O}_{K_j}$ such that the diagram

$$\begin{tikzcd} \mathcal{O}_{K_j} \arrow[rr, "g^{\mathrm{Lie}}"] \arrow[dr] & & \mathrm{End}_R(\mathrm{Lie}(\mathfrak{G})) \\ & R \arrow[ur] & \end{tikzcd}$$

commutes, where $\mathcal{O}_{K_j} \hookrightarrow \mathcal{O}_K \to R$ is the structure map (the CM normalization condition).

Now let $(A_0, i_0, \kappa_0) \in \mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})$. Then by the theorem, the map

$$(A, i, \kappa) \mapsto (A[p^\infty], i[p^\infty], \kappa[p^\infty])$$

defines a bijection between the set of isomorphism classes of deformations of (A_0, i_0, κ_0) to R and the set of isomorphism classes of deformations of $(A_0[p^\infty], i_0[p^\infty], \kappa_0[p^\infty])$ to R (as CM p-divisible groups with an action of $\mathcal{O}_B$). The only thing to note is that (A, i, κ) satisfies the CM normalization condition for false elliptic curves if and only if $(A[p^\infty], i[p^\infty], \kappa[p^\infty])$ satisfies the CM normalization condition for p-divisible groups, since there is an isomorphism of R-modules $\mathrm{Lie}(A) \cong \mathrm{Lie}(A[p^\infty])$. Therefore if we define a functor $\mathrm{Def}_{\mathcal{O}_B}(A_0[p^\infty], \mathcal{O}_{K_j}) : \mathbf{CLN} \to \mathbf{Sets}$ by sending R to the set of isomorphism classes of deformations of $(A_0[p^\infty], i_0[p^\infty], \kappa_0[p^\infty])$ to R, then there is a natural isomorphism of functors

$$\mathrm{Def}_{\mathcal{O}_B}(A_0, \mathcal{O}_{K_j}) \cong \mathrm{Def}_{\mathcal{O}_B}(A_0[p^\infty], \mathcal{O}_{K_j}).$$

Continuing with $(A_0, i_0, \kappa_0) \in \mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})$, assume $\mathfrak{P}$ lies over a prime p nonsplit in K_j. We have $A_0 \cong M_0 \otimes_{\mathcal{O}_{K_j}} E_0$ for some $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_{K_j}$-module M_0 and some supersingular elliptic curve E_0 over

$\overline{\mathbb{F}}_{\mathfrak{P}}$ with an action $g_0 : \mathcal{O}_{K_j} \to \mathrm{End}(E_0)$ satisfying

$$\kappa_0(a)(m \otimes x) = m \otimes g_0(a)(x)$$

on points. Define a functor $\mathrm{Def}(E_0, \mathcal{O}_{K_j}) : \mathbf{CLN} \to \mathbf{Sets}$ by sending R to the set of isomorphism classes of deformations of E_0 with its $\mathcal{O}_{K_j}$-action to R.

Proposition 8.1.3. *There is a natural isomorphism of functors*

$$\mathscr{G} : \mathrm{Def}(E_0, \mathcal{O}_{K_j}) \to \mathrm{Def}_{\mathcal{O}_B}(A_0, \mathcal{O}_{K_j})$$

given by $\mathscr{G}(R) : E \mapsto M_0 \otimes_{\mathcal{O}_{K_j}} E$ *for any* $R \in \mathbf{CLN}$.

Proof. Let R be an object of $\mathbf{CLN}$ and let $(E, g) \in \mathrm{Def}(E_0, \mathcal{O}_{K_j})(R)$, so there is an isomorphism of elliptic curves $E \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \to E_0$ compatible with the CM actions g and g_0. Setting $A = M_0 \otimes_{\mathcal{O}_{K_j}} E$, there is an isomorphism of abelian varieties $A \otimes_R \overline{\mathbb{F}}_{\mathfrak{P}} \to A_0$, such that if we define an $\mathcal{O}_{K_j}$-action κ on A through the action g on E, then this action lifts κ_0 and the above isomorphism is compatible with κ and κ_0. It follows from the proof of Theorem 5.1.1 that the usual principal polarization on A_0 automatically lifts to an $\mathcal{O}_{K_j}$-linear principal polarization on A, so $A \in \mathscr{M}_j^2(R)$ is a deformation of $A_0 \in \mathscr{M}_j^2(\overline{\mathbb{F}}_{\mathfrak{P}})$. Therefore the reduction map $\mathrm{End}_{\mathcal{O}_{K_j}}(A) \to \mathrm{End}_{\mathcal{O}_{K_j}}(A_0)$ is an isomorphism and we can lift the $\mathcal{O}_{K_j}$-linear action of $\mathcal{O}_B$ on A_0 to a unique such action on A, which shows A is a deformation of A_0 to R (A satisfies the CM normalization condition since E does). Define

$$\mathscr{G}(R) : \mathrm{Def}(E_0, \mathcal{O}_{K_j})(R) \to \mathrm{Def}_{\mathcal{O}_B}(A_0, \mathcal{O}_{K_j})(R)$$

by $E \mapsto M_0 \otimes_{\mathcal{O}_{K_j}} E$. If $R \to R'$ is a morphism in $\mathbf{CLN}$ then the diagram

$$\begin{tikzcd}
\mathrm{Def}(E_0, \mathcal{O}_{K_j})(R) \arrow[r, "\mathscr{G}(R)"] \arrow[d] & \mathrm{Def}_{\mathcal{O}_B}(A_0, \mathcal{O}_{K_j})(R) \arrow[d] \\
\mathrm{Def}(E_0, \mathcal{O}_{K_j})(R') \arrow[r, "\mathscr{G}(R')"] & \mathrm{Def}_{\mathcal{O}_B}(A_0, \mathcal{O}_{K_j})(R')
\end{tikzcd}$$

commutes since

$$(M_0 \otimes_{\mathcal{O}_{K_j}} E) \otimes_R R' \cong M_0 \otimes_{\mathcal{O}_{K_j}} (E \otimes_R R').$$

Now, the main point is that $\mathscr{G}(R)$ is a bijection because $\mathrm{Def}(E_0, \mathcal{O}_{K_j})(R)$ and $\mathrm{Def}_{\mathcal{O}_B}(A_0, \mathcal{O}_{K_j})(R)$ are both one point sets by Theorem 5.1.1. □

With the same notation as above, if we define a functor $\mathrm{Def}(E_0[p^\infty], \mathcal{O}_{K_j}) : \mathbf{CLN} \to \mathbf{Sets}$ in the obvious way, then there is a natural isomorphism of functors

$$\mathscr{G}' : \mathrm{Def}(E_0[p^\infty], \mathcal{O}_{K_j}) \to \mathrm{Def}_{\mathcal{O}_B}(A_0[p^\infty], \mathcal{O}_{K_j}).$$

This is a consequence of the above proposition and the Serre-Tate theorem (both in the usual form and Theorem 8.1.2). Explicitly, $\mathscr{G}'$ is the composition of isomorphisms

$$\mathrm{Def}(E_0[p^\infty], \mathcal{O}_{K_j}) \to \mathrm{Def}(E_0, \mathcal{O}_{K_j}) \xrightarrow{\mathscr{G}} \mathrm{Def}_{\mathcal{O}_B}(A_0, \mathcal{O}_{K_j}) \to \mathrm{Def}_{\mathcal{O}_B}(A_0[p^\infty], \mathcal{O}_{K_j}),$$

so $\mathscr{G}'(R) : \mathfrak{h} \mapsto M_0 \otimes_{\mathcal{O}_{K_j}} \mathfrak{h}$, where $M_0 \otimes_{\mathcal{O}_{K_j}} \mathfrak{h}$ is the p-divisible group $(G_n)_n$ with $G_n = M_0 \otimes_{\mathcal{O}_{K_j}} H_n$ (where $\mathfrak{h} = (H_n)_n$). The ring $\mathcal{O}_B$ acts on $M_0 \otimes_{\mathcal{O}_{K_j}} \mathfrak{h}$ through its action on M_0. As a p-divisible group with an action of $\mathcal{O}_{K_j}$, we have $M_0 \otimes_{\mathcal{O}_{K_j}} \mathfrak{h} \cong \mathfrak{h} \times \mathfrak{h}$, with $\mathcal{O}_{K_j}$ acting diagonally on $\mathfrak{h} \times \mathfrak{h}$.

Let $\mathfrak{g}$ be the unique (up to isomorphism) connected p-divisible group of height 2 and dimension 1 over $\overline{\mathbb{F}}_{\mathfrak{p}}$, and set $\Delta = \mathrm{End}(\mathfrak{g})$ as above. Since the functor $\mathrm{Def}_{\mathcal{O}_B}(A_0, \mathcal{O}_{K_j})$ is represented by $\mathscr{W}$, there is a bijection

$$\mathrm{Def}_{\mathcal{O}_B}(A_0, \mathcal{O}_{K_j})(R) \cong \mathrm{Hom}_{\mathbf{CLN}}(\mathscr{W}, R)$$

for any $R \in \mathbf{CLN}$. The unique element of $\mathrm{Def}_{\mathcal{O}_B}(A_0, \mathcal{O}_{K_j})(\mathscr{W})$, which corresponds to the identity map $\mathscr{W} \to \mathscr{W}$, is called the *universal deformation* of A_0 to $\mathscr{W}$. A similar definition can be made for the other deformation functors we have defined. Let A be the universal deformation of A_0 to $\mathscr{W}$. From the above discussion, $A[p^\infty]$ is the universal deformation of $A_0[p^\infty]$ to $\mathscr{W}$, and there is an isomorphism $A \cong M_0 \otimes_{\mathcal{O}_{K_j}} E$ for some CM elliptic curve E over $\mathscr{W}$ lifting E_0, where $A_0 \cong M_0 \otimes_{\mathcal{O}_{K_j}} E_0$. Let $\mathfrak{G}$ be the universal deformation of $E_0[p^\infty] \cong \mathfrak{g}$ to $\mathscr{W}$ (the universal deformation with respect to the functor $\mathrm{Def}(\mathfrak{g}, \mathcal{O}_{K_j})$). Since $\mathscr{G}$ is an isomorphism, E is the universal deformation of E_0 to $\mathscr{W}$ (with respect to $\mathrm{Def}(E_0, \mathcal{O}_{K_j})$), so $E[p^\infty] \cong \mathfrak{G}$ and therefore there is an isomorphism $A[p^\infty] \cong M_0 \otimes_{\mathcal{O}_{K_j}} \mathfrak{G}$. Again, as a p-divisible group with an action of $\mathcal{O}_{K_j}$, we have $M_0 \otimes_{\mathcal{O}_{K_j}} \mathfrak{G} \cong \mathfrak{G} \times \mathfrak{G}$.

In the context of the previous paragraph, suppose we are in the case of $p \nmid d_B$. The standard idempotents ε and ε' in

$$\mathrm{M}_2(\mathscr{W}) \cong \mathrm{M}_2(\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathscr{W} \cong \mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{W}$$

induce a splitting $A[p^\infty] \cong \varepsilon A[p^\infty] \times \varepsilon' A[p^\infty]$, and conjugation by

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in \mathrm{M}_2(\mathscr{W})$$

defines an isomorphism $\varepsilon A[p^\infty] \to \varepsilon' A[p^\infty]$, so there are isomorphisms of p-divisible groups over $\mathscr{W}$

$$\mathfrak{G} \times \mathfrak{G} \cong A[p^\infty] \cong \varepsilon A[p^\infty] \times \varepsilon A[p^\infty].$$

Hence $\mathfrak{G} \times \mathfrak{G}$ and $\varepsilon A[p^\infty] \times \varepsilon A[p^\infty]$ are both in $\mathrm{Def}_{\mathcal{O}_B}(A_0[p^\infty], \mathcal{O}_{K_j})(\mathscr{W})$, which is a one point set, so by the injectivity of the map $\mathscr{G}'(\mathscr{W})$ defined above, $\varepsilon A[p^\infty] \cong \mathfrak{G}$. By a proof similar to that of Lemma 6.1.1, we then have

$$\mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{W}}(A[p^\infty]) \cong \mathrm{End}_{\mathscr{W}}(\mathfrak{G}).$$

Back to no assumption on p, let L be a quadratic field extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_L$ and let $\pi_L \in \mathcal{O}_L$ be a uniformizer. Let $\mathscr{W}_L$ be the ring of integers in the completion of the maximal unramified extension of L, and choose a ring homomorphism $W \to \mathscr{W}_L$. Viewing $\mathcal{O}_L$ as a $\mathbb{Z}_p$-subalgebra of Δ, there is an action of $\mathcal{O}_L$ on $\mathfrak{g}$. By [10, Proposition 2.1] there is a unique (up to isomorphism) deformation $\mathfrak{g}_L$ of $\mathfrak{g}$ with its $\mathcal{O}_L$-action to $\mathscr{W}_L$, where $\mathfrak{g}_L$ satisfies the CM normalization condition: the induced map $\mathcal{O}_L \to \mathrm{End}_{\mathscr{W}_L}(\mathrm{Lie}(\mathfrak{g}_L)) \cong \mathscr{W}_L$ is the structure map $\mathcal{O}_L \hookrightarrow \mathscr{W}_L$. For any integer $m \geqslant 1$ set $\mathscr{W}_{L,m} = \mathscr{W}_L/(\pi_L^m)$, and for any p-divisible group $\mathfrak{h}$ over $\mathscr{W}_L$ set $\mathfrak{h}_m = \mathfrak{h} \otimes_{\mathscr{W}_L} \mathscr{W}_{L,m}$. By [10, Proposition 3.3] the reduction map $\mathrm{End}_{\mathscr{W}_{L,m}}(\mathfrak{g}_{L,m}) \hookrightarrow \mathrm{End}(\mathfrak{g})$ induces an isomorphism

$$\mathrm{End}_{\mathscr{W}_{L,m}}(\mathfrak{g}_{L,m}) \cong \mathcal{O}_L + \pi_L^{m-1}\Delta. \tag{8.1.1}$$

Continuing with the notation of the previous paragraph, given any $f \in \Delta \smallsetminus \mathcal{O}_L$, the functor $\mathrm{Def}(\mathfrak{g}, \mathcal{O}_L[f]) : \mathbf{CLN} \to \mathbf{Sets}$, defined in the obvious way, is represented by $\mathscr{W}_{L,m}$, where m is the largest integer such that f lifts (necessarily uniquely, by the injectivity of the reduction map) to an element of $\mathrm{End}_{\mathscr{W}_{L,m}}(\mathfrak{g}_{L,m})$. To prove this, we need to show that given a deformation $(\widetilde{\mathfrak{g}}, \widetilde{f})$ of $(\mathfrak{g}, f)$ to an object R of $\mathbf{CLN}$, including a lift of the $\mathcal{O}_L$-action, there is a unique morphism $\mathscr{W}_{L,m} \to R$ in $\mathbf{CLN}$ such that $(\widetilde{\mathfrak{g}}, \widetilde{f})$ is the reduction of $(\mathfrak{g}_{L,m}, f_m)$ via this morphism, where f_m is the assumed lift of f. It suffices to assume R is Artinian as usual. By construction there is a unique morphism $\mathscr{W}_L \to R$ such that $\widetilde{\mathfrak{g}}$, with its $\mathcal{O}_L$-action, is the reduction of $\mathfrak{g}_L$. Then for some $n > m+1$ sufficiently large, the morphism $\mathscr{W}_L \to R$ factors through $\varphi : \mathscr{W}_{L,n} \to R$ since R is Artinian. Set $S = \mathrm{Spec}(\mathscr{W}_{L,n})$, so $\varphi \in S(R)$. Now by (8.1.1),

$$f \in \mathrm{End}_{\mathscr{W}_{L,n}}(\mathfrak{g}_{L,n}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \Delta_{\mathbb{Q}},$$

which means f is a quasi-isogeny $f_n : \mathfrak{g}_{L,n} \to \mathfrak{g}_{L,n}$. Then by [22, Proposition 2.9], the functor

$$T \mapsto \{\psi \in \mathrm{Hom}_S(T, S) : \psi^* f_n \text{ is an isogeny}\}$$

on S-schemes is represented by a closed subscheme $S_0 \subset S$. As $\widetilde{f}$ is an isogeny, we have $\varphi \in S_0(R)$. Since m is the largest integer such that $S_0(\mathscr{W}_{L,m})$ is nonempty, the closed subscheme S_0 must be $\mathrm{Spec}(\mathscr{W}_{L,m})$, so from $\varphi \in S_0(R)$ the claim follows.

8.2 Deformations of CM pairs

Fix a ring homomorphism $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$, a CM pair $(\mathbf{A}_1, \mathbf{A}_2) \in \mathscr{X}_\theta(\overline{\mathbb{F}}_{\mathfrak{P}})$, and a nonzero $f \in L(\mathbf{A}_1, \mathbf{A}_2)$. Let p be the residue characteristic of $\mathfrak{P}$, let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$, and assume p is nonsplit in K_1 and K_2.

Proposition 8.2.1. *If $p \nmid d_B$ and p is inert in K_1 and K_2, then the functor* $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ *is represented by a local Artinian $\mathscr{W}$-algebra of length*

$$\frac{\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(f)) + 1}{2}.$$

Proof. Since $p \nmid d_B$, the standard idempotent $\varepsilon \in \mathrm{M}_2(\mathbb{Z}_p) \cong \mathcal{O}_B \otimes_{\mathbb{Z}} \mathbb{Z}_p$ induces an isomorphism $L_p(\mathbf{A}_1, \mathbf{A}_2) \cong \Delta$ of $\mathbb{Z}_p$-modules (Lemmas 6.2.1 and 6.2.2), and this isomorphism identifies the quadratic form $\deg^*$ on $L_p(\mathbf{A}_1, \mathbf{A}_2)$ with the quadratic form $u \cdot \mathrm{Nrd}$ on Δ for some $u \in \mathbb{Z}_p^\times$. Isomorphisms $\varepsilon A_j[p^\infty] \cong \mathfrak{g}$ may be chosen so that $\kappa_1 : \mathcal{O}_{K_1,p} \to \mathrm{End}_{\mathcal{O}_B}(A_1) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \Delta$ and $\kappa_2 : \mathcal{O}_{K_2,p} \to \mathrm{End}_{\mathcal{O}_B}(A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \Delta$ have the same image $\mathcal{O}_L \cong \mathbb{Z}_{p^2}$. Let $L \cong K_{1,p} \cong K_{2,p}$ be the fraction field of $\mathcal{O}_L$. Fix a uniformizer $\Pi \in \Delta$ satisfying $v\Pi = \Pi v^\iota$ for all $v \in \mathcal{O}_L \subset \Delta$, so there is a decomposition of left $\mathcal{O}_L$-modules $\Delta = \Delta_+ \oplus \Delta_-$, where $\Delta_+ = \mathcal{O}_L$ and $\Delta_- = \mathcal{O}_L\Pi$. This decomposition is orthogonal with respect to the quadratic form $\deg^*$ on Δ because if $a, b \in \mathcal{O}_L$ then

$$\begin{aligned}\deg^*(a + b\Pi) - \deg^*(a) - \deg^*(b\Pi) &= u\,\mathrm{Nrd}(a + b\Pi) - u\,\mathrm{Nrd}(a) - u\,\mathrm{Nrd}(b\Pi)\\ &= u(\overline{a} - b\Pi) - u\overline{a} + ub\Pi = 0.\end{aligned}$$

Define $\varphi_\pm : \mathcal{O}_{K,p} \to \mathcal{O}_L$ by

$$\begin{aligned}\varphi_+(x_1 \otimes x_2) &= \kappa_2(x_2)\kappa_1(\overline{x}_1)\\ \varphi_-(x_1 \otimes x_2) &= \kappa_2(x_2)\kappa_1(x_1),\end{aligned}$$

and let Φ be the isomorphism

$$\Phi = \varphi_+ \times \varphi_- : \mathcal{O}_{K,p} \to \mathcal{O}_L \times \mathcal{O}_L.$$

Then the usual action of $\mathcal{O}_K$ on Δ is given by

$$x \bullet f = \varphi_+(x) f_+ + \varphi_-(x) f_-$$

for $f = f_+ + f_- \in \Delta$, because for $f_+ \in \mathcal{O}_L$ and $f_- \in \mathcal{O}_L \Pi$,

$$\begin{aligned}(x_1 \otimes x_2) \bullet f_+ &= \kappa_2(x_2) f_+ \kappa_1(\overline{x}_1) = \kappa_2(x_2)\kappa_1(\overline{x}_1) f_+ \\ (x_1 \otimes x_2) \bullet f_- &= \kappa_2(x_2) f_- \kappa_1(\overline{x}_1) = \kappa_2(x_2)\kappa_1(x_1) f_-\end{aligned}$$

by the choice of Π. Also, the $\mathcal{O}_{F,p}$-quadratic form $\deg_{\mathrm{CM}}$ on Δ takes the form

$$\Phi(\deg_{\mathrm{CM}}(f)) = (\deg^*(f_+), \deg^*(f_-))$$

since

$$\mathrm{Tr}_{F_p/\mathbb{Q}_p}(\deg^*(f_+), \deg^*(f_-)) = \deg^*(f_+) + \deg^*(f_-) = \deg^*(f_+ + f_-) = \deg^*(f),$$

the second equality coming from orthogonality. Therefore if $\mathfrak{p}_- = \mathfrak{p}$ and $\mathfrak{p}_+ = \overline{\mathfrak{p}}$ is the other prime of F over p, then

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}_+}(\deg_{\mathrm{CM}}(f)) &= \mathrm{ord}_p(\deg^*(f_+)) \\ \mathrm{ord}_{\mathfrak{p}_-}(\deg_{\mathrm{CM}}(f)) &= \mathrm{ord}_p(\deg^*(f_-)).\end{aligned}$$

This follows from $\Phi(\mathfrak{P}\mathcal{O}_{K,p}) = \mathcal{O}_L \times p\mathcal{O}_L$ and $\Phi(\overline{\mathfrak{P}}\mathcal{O}_{K,p}) = p\mathcal{O}_L \times \mathcal{O}_L$, where $\overline{\mathfrak{P}}$ is the prime of K over $\mathfrak{p}_+$, and this is a result of the equivalences

$$\begin{aligned}x_1 \otimes x_2 \in \mathfrak{P}\mathcal{O}_{K,p} &\iff \kappa_2(x_2)\kappa_1(x_1) \in \mathfrak{m}_\Delta \cap \mathcal{O}_L = p\mathcal{O}_L \\ x_1 \otimes x_2 \in \overline{\mathfrak{P}}\mathcal{O}_{K,p} &\iff \kappa_2(x_2)\kappa_1(\overline{x}_1) \in \mathfrak{m}_\Delta \cap \mathcal{O}_L = p\mathcal{O}_L\end{aligned}$$

we saw in the proof of Proposition 7.2.5, where $\mathfrak{m}_\Delta \subset \Delta$ is the unique maximal ideal. Hence, for any integer $m \geqslant 1$ and any $f \in \Delta$,

$$\begin{aligned}f \in \mathcal{O}_L + p^{m-1}\Delta &\iff f_- \in p^{m-1}\mathcal{O}_L\Pi \\ &\iff \mathrm{ord}_p(\deg^*(f_-)) \geqslant 2m-1 \\ &\iff \frac{\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(f)) + 1}{2} \geqslant m,\end{aligned}$$

where the second equivalence comes from $\deg^*(\Pi) = p$ and $\deg^*(p) = p^2$. Note that $\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(f)) = \mathrm{ord}_p(\deg^*(f_-))$ is odd because any $f_- \in \mathcal{O}_L\Pi$ can be written as $f_- = vp^k\Pi$ for some $v \in \mathbb{Z}_{p^2}^\times$ and $k \geqslant 0$, and thus $\deg^*(f_-) = p^{2k+1}$.

The functor

$$\begin{aligned}\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2) &\cong \mathrm{Def}_{\mathcal{O}_B}(A_1[p^\infty], \mathcal{O}_L) \times \mathrm{Def}_{\mathcal{O}_B}(A_2[p^\infty], \mathcal{O}_L) \\ &\cong \mathrm{Def}(\mathfrak{g}, \mathcal{O}_L) \times \mathrm{Def}(\mathfrak{g}, \mathcal{O}_L)\end{aligned}$$

is represented by $\mathscr{W}\widehat{\otimes}_{\mathscr{W}}\mathscr{W} \cong \mathscr{W}$. As above let $\mathfrak{G}$ be the universal deformation of $\mathfrak{g}$ to $\mathscr{W}$ (with respect to $\mathrm{Def}(\mathfrak{g}, \mathcal{O}_L)$), let $\pi_K \in K_{\mathfrak{P}}$ be a uniformizer, and set $\mathscr{W}_m = \mathscr{W}/(\pi_K^m)$. Then the p-divisible group of the universal deformation of $(\mathbf{A}_1, \mathbf{A}_2)$ to $\mathscr{W}$ is $(\mathfrak{H}_1, \mathfrak{H}_2)$, where $\mathfrak{H}_j \cong \mathfrak{G} \times \mathfrak{G}$ for $j = 1, 2$, with $\mathcal{O}_B$ acting on $\mathfrak{G} \times \mathfrak{G} \cong \varepsilon\mathfrak{H}_j \times \varepsilon\mathfrak{H}_j$ via the natural action of $\mathrm{M}_2(\mathscr{W})$. By what we showed above, the functor $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ is represented by $\mathscr{W}_m$, where m is the largest integer such that $f \in \mathrm{Hom}_{\mathcal{O}_B}(A_1[p^\infty], A_2[p^\infty]) \cong \mathrm{End}(\mathfrak{g})$ lifts to an element of

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{W}_m}(\mathfrak{H}_1 \otimes_{\mathscr{W}} \mathscr{W}_m, \mathfrak{H}_2 \otimes_{\mathscr{W}} \mathscr{W}_m) \cong \mathrm{End}_{\mathscr{W}_m}(\mathfrak{G} \otimes_{\mathscr{W}} \mathscr{W}_m).$$

Since p is inert in K_1 and K_2, we have $K_{\mathfrak{P}} \cong L$, so $\mathscr{W} = \mathscr{W}_L = W$. If $\mathfrak{g}_L$ is the unique deformation of $\mathfrak{g}$ with its $\mathcal{O}_L$-action to W, then $\mathfrak{g}_L = \mathfrak{G}$, so by (8.1.1),

$$\mathrm{End}_{\mathscr{W}_m}(\mathfrak{G}_m) = \mathrm{End}_{W_m}(\mathfrak{g}_{L,m}) \cong \mathcal{O}_L + p^{m-1}\Delta.$$

Hence $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ is represented by $\mathscr{W}_m$, which is an Artinian $\mathscr{W}$-algebra of length m, where m is the largest integer such that $f \in \mathcal{O}_L + p^{m-1}\Delta$, and the formula for m follows from the calculation above. □

We will need an analogue of (8.1.1) for the p-divisible group of a false elliptic curve defined over $\overline{\mathbb{F}}_p$ for $p \mid d_B$. This is what we prove next.

Lemma 8.2.2. *Let $(A, i, \kappa) \in \mathscr{Y}_j(\overline{\mathbb{F}}_{\mathfrak{P}})$ for $p \mid d_B$. Set*

$$R = \mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{End}_{\mathcal{O}_B}(A[p^\infty]),$$

let $\mathscr{A}$ be the universal deformation of A to $\mathscr{W} = W$, and for each integer $m \geqslant 1$ set

$$R_m = \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W_m}(\mathscr{A} \otimes_W W_m) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W_m}(\mathscr{A}[p^\infty] \otimes_W W_m),$$

where $W_m = W/(p^m)$. Then the reduction map $R_m \hookrightarrow R$ induces an isomorphism

$$R_m \cong \mathcal{O}_L + p^{m-1}R,$$

where $\mathcal{O}_L = \kappa(\mathcal{O}_{K_j,p})$.

Proof. We will use Grothendieck-Messing deformation theory. Let $D = D(A)$ be the covariant Dieudonné module of A as above and set $\mathcal{O}_j = \mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_{K_j}$. There is an isomorphism of $\mathscr{D} \otimes_{\mathbb{Z}} \mathcal{O}_j$-modules $H_1^{\mathrm{dR}}(\mathscr{A}) \to D$, where $H_1^{\mathrm{dR}}(\mathscr{A}) = \mathrm{Hom}_W(H^1_{\mathrm{dR}}(\mathscr{A}), W)$ is the first de Rham homology group of $\mathscr{A}$ (which is a free W-module of rank 4). It follows that for any $m \geqslant 1$ there are $\mathcal{O}_j$-linear isomorphisms of W_m-modules

$$H_1^{\mathrm{dR}}(\mathscr{A} \otimes_W W_m) \cong D \otimes_W W_m \cong D/p^m D.$$

For any $m \geqslant 1$ the surjection $W_m \to \overline{\mathbb{F}}_{\mathfrak{P}}$ has kernel $\mathfrak{a} = pW/p^mW$. Since $\mathfrak{a}$ has the canonical divided power structure, the deformations of A, as an abelian scheme, to W_m are in one-to-one correspondence with direct summands $M \subset \widetilde{H}_1^{\mathrm{dR}}(A)$, where $\widetilde{H}_1^{\mathrm{dR}}(A) = H_1^{\mathrm{dR}}(\widetilde{A})$ for any deformation $\widetilde{A}$ of A to W_m, such that the image of M under the reduction $\widetilde{H}_1^{\mathrm{dR}}(A) \to H_1^{\mathrm{dR}}(A)$ is $\mathrm{Fil}(A)$, the Hodge filtration of $H_1^{\mathrm{dR}}(A)$. By Corollary 5.1.3, (A, i, κ) has a unique deformation to W_m, namely $\mathscr{A}_m = \mathscr{A} \otimes_W W_m$. Therefore there is a unique direct summand $M_m \subset \widetilde{H}_1^{\mathrm{dR}}(A)$, stable under the action of $\mathcal{O}_j$ on $\widetilde{H}_1^{\mathrm{dR}}(A)$, that reduces to $\mathrm{Fil}(A)$, and such that the diagram

$$\begin{tikzcd}
\mathcal{O}_{K_j} \arrow[rr] \arrow[dr] & & \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W_m}(\widetilde{H}_1^{\mathrm{dR}}(A)/M_m) \\
& W_m \arrow[ur] &
\end{tikzcd} \tag{8.2.1}$$

commutes, namely $M_m = \mathrm{Fil}(\mathscr{A}_m)$. The Hodge sequence for A takes the form

$$0 \to \mathrm{Fil}(A) \to D/pD \to \mathrm{Lie}(A) \to 0.$$

Using a W-basis $\{e_1, e_2, e_3, e_4\}$ for D as in Proposition 6.3.2, it also defines an $\overline{\mathbb{F}}_{\mathfrak{P}}$-basis for D/pD, and

$$\mathrm{Fil}(A) = \ker(D/pD \to D/\mathscr{V}D)$$

has $\{e_2, e_4\}$ as an $\overline{\mathbb{F}}_{\mathfrak{P}}$-basis.

Any $f \in R$ induces a map $H_1^{\mathrm{dR}}(A) \to H_1^{\mathrm{dR}}(A)$ which lifts to a map $\widetilde{f} : \widetilde{H}_1^{\mathrm{dR}}(A) \to \widetilde{H}_1^{\mathrm{dR}}(A)$, and

f lifts to an element of R_m if and only if $\widetilde{f}(M_m) \subset M_m$. The map

$$\widetilde{f} : \widetilde{H}_1^{\mathrm{dR}}(A) \cong D/p^m D \to D/p^m D \cong \widetilde{H}_1^{\mathrm{dR}}(A)$$

corresponds to the reduction modulo p^m of $f : D \to D$. Consider the W_m-submodule $N = \mathrm{Span}_{W_m}(e_2, e_4) \subset D/p^m D$. In the basis $\{e_n\}$, the $\mathcal{O}_{K_j}$-action on D is given by (6.3.3) and the $\mathcal{O}_B$-action is given by one of the matrices in (6.3.2). Each of these maps stabilizes N, so N is an $\mathcal{O}_j$-stable direct summand of $D/p^m D$ that reduces to $\mathrm{Fil}(A) = \mathrm{Span}_{\mathbb{F}_{\mathfrak{P}}}(e_2, e_4)$ modulo p. Also, a computation in coordinates shows that the diagram

$$\begin{tikzcd}
\mathcal{O}_{K_j} \arrow[rr] \arrow[dr] & & \mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W_m}((D/p^m D)/N) \\
& W_m \arrow[ur] &
\end{tikzcd}$$

commutes. Hence $N \cong M_m$ under the isomorphism $D/p^m D \cong \widetilde{H}_1^{\mathrm{dR}}(A)$. Now,

$$R \cong \left\{ \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix} : x, y \in \mathcal{O}_{K_j,p} \right\},$$

where we have fixed a decomposition $\Delta = \mathcal{O}_{K_j,p} \oplus \mathcal{O}_{K_j,p}\Pi$. Expressing

$$f = \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix} \in R$$

as an element of $\mathrm{M}_4(W)$ as in (6.3.4), we have

$$\begin{aligned}
f \text{ lifts to an element of } R_m &\iff \widetilde{f}(N) \subset N \\
&\iff f : D/p^m D \to D/p^m D \text{ stabilizes } N \\
&\iff f(e_2), f(e_4) \in We_2 + We_4 + p^m D \\
&\iff p^2 y \in p^m W \text{ and } py \in p^m W \\
&\iff y \in p^{m-1}\mathcal{O}_{K_j,p} \\
&\iff f \in \mathcal{O}_L + p^{m-1}R. \qquad \square
\end{aligned}$$

Proposition 8.2.3. *If $p \mid d_B$ and $\mathfrak{P}$ divides $\ker(\theta)$, then $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ is represented by a local Artinian $\mathscr{W}$-algebra of length $\frac{1}{2}\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(f))$.*

Proof. The proof is very similar to that of Proposition 8.2.1. As usual $A_j \cong M_j \otimes_{\mathcal{O}_{K_j}} E_j$ for some supersingular elliptic curve E_j. Isomorphisms $E_j[p^\infty] \cong \mathfrak{g}$ may be chosen so that the CM actions

$\mathcal{O}_{K_1,p} \to \Delta$ and $\mathcal{O}_{K_2,p} \to \Delta$ on E_1 and E_2, respectively, have the same image $\mathcal{O}_L \cong \mathbb{Z}_{p^2}$. Fix a uniformizer $\Pi \in \Delta$ satisfying $v\Pi = \Pi v^\iota$ for all $x \in \mathcal{O}_L \subset \Delta$. There is an isomorphism of $\mathbb{Z}_p$-modules $L_p(\mathbf{A}_1, \mathbf{A}_2) \cong R$, where

$$R = \left\{ \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix} : x, y \in \mathcal{O}_L \right\},$$

and the CM actions κ_1 and κ_2 are identified with a single action $\mathcal{O}_L \to R$ given by $x \mapsto \mathrm{diag}(x, x)$ (see the proof of Proposition 7.2.5). Under the isomorphism $L_p(\mathbf{A}_1, \mathbf{A}_2) \cong R$ the quadratic form $\deg^*$ on $L_p(\mathbf{A}_1, \mathbf{A}_2)$ is identified with the quadratic form Q on R defined in Proposition 7.2.2. There is a decomposition of left $\mathcal{O}_L$-modules $R = R_+ \oplus R_-$, with $R_+ = \mathcal{O}_L$, embedded diagonally in R, and $R_- = \mathcal{O}_L P$, where

$$P = \begin{bmatrix} 0 & \Pi \\ p\Pi & 0 \end{bmatrix},$$

and this decomposition is orthogonal with respect to the quadratic form $\deg^*$. Similar to before, define $\varphi_\pm : \mathcal{O}_{K,p} \to \mathcal{O}_L \subset R$ by

$$\varphi_+(x_1 \otimes x_2) = \kappa_2(x_2)\kappa_1(\overline{x}_1)$$
$$\varphi_-(x_1 \otimes x_2) = \kappa_2(x_2)\kappa_1(x_1),$$

and let Φ be the isomorphism

$$\Phi = \varphi_+ \times \varphi_- : \mathcal{O}_{K,p} \to \mathcal{O}_L \times \mathcal{O}_L.$$

Then the usual action of $\mathcal{O}_K$ on R is given by

$$x \bullet f = \varphi_+(x) f_+ + \varphi_-(x) f_-$$

for $f = f_+ + f_- \in R$ since $P\kappa_1(\overline{x}_1) = \kappa_1(x_1)P$ by the choice of Π. As above it follows that

$$\Phi(\deg_{\mathrm{CM}}(f)) = (\deg^*(f_+), \deg^*(f_-)).$$

Now let

$$\mathfrak{M} = \left\{ \begin{bmatrix} px & y\Pi \\ py\Pi & px \end{bmatrix} : x, y \in \mathcal{O}_L \right\} \subset R.$$

We saw in the proof of Proposition 7.2.5 that

$$x_1 \otimes x_2 \in \mathfrak{P}\mathcal{O}_{K,p} \iff \kappa_2(x_2)\kappa_1(x_1) \in \mathfrak{M} \cap \mathcal{O}_L = p\mathcal{O}_L$$
$$x_1 \otimes x_2 \in \overline{\mathfrak{P}}\mathcal{O}_{K,p} \iff \kappa_2(x_2)\kappa_1(\overline{x}_1) \in \mathfrak{M} \cap \mathcal{O}_L = p\mathcal{O}_L,$$

and thus, as in the proof of Proposition 8.2.1,

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}_+}(\deg_{\mathrm{CM}}(f)) &= \mathrm{ord}_p(\deg^*(f_+))\\ \mathrm{ord}_{\mathfrak{p}_-}(\deg_{\mathrm{CM}}(f)) &= \mathrm{ord}_p(\deg^*(f_-)),\end{aligned}$$

where $\mathfrak{p}_- = \mathfrak{p}$ and $\mathfrak{p}_+ = \overline{\mathfrak{p}}$. Since $\deg^*(P) = Q(P) = -p^2$, for any integer $m \geqslant 1$ and any $f \in R$ we have

$$\begin{aligned} f \in \mathcal{O}_L + p^{m-1}R &\iff f_- \in p^{m-1}\mathcal{O}_L P\\ &\iff \mathrm{ord}_p(\deg^*(f_-)) \geqslant 2m\\ &\iff \tfrac{1}{2}\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(f)) \geqslant m.\end{aligned}$$

The functor

$$\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2) \cong \mathrm{Def}_{\mathcal{O}_B}(A_1[p^\infty], \mathcal{O}_L) \times \mathrm{Def}_{\mathcal{O}_B}(A_2[p^\infty], \mathcal{O}_L)$$

is represented by $\mathscr{W}\widehat{\otimes}_{\mathscr{W}}\mathscr{W} \cong \mathscr{W}$. Let $(\widetilde{\mathbf{A}}_1, \widetilde{\mathbf{A}}_2)$ be the universal deformation of $(\mathbf{A}_1, \mathbf{A}_2)$ to $\mathscr{W} = W$. A similar argument to above shows that the functor $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ is represented by $W_m = W/(p^m)$, where m is the largest integer such that $f \in \mathrm{Hom}_{\mathcal{O}_B}(A_1[p^\infty], A_2[p^\infty]) \cong R$ lifts to an element of

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W_m}(\widetilde{A}_1[p^\infty] \otimes_W W_m, \widetilde{A}_2[p^\infty] \otimes_W W_m).$$

Since there are $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_L$-linear isomorphisms $A_1[p^\infty] \cong A_2[p^\infty]$ and $\widetilde{A}_j \otimes_W \overline{\mathbb{F}}_{\mathfrak{P}} \cong A_j$, there is an $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_L$-linear isomorphism $\widetilde{A}_1[p^\infty] \cong \widetilde{A}_2[p^\infty]$ by the uniqueness of the universal deformation. Hence

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W_m}(\widetilde{A}_1[p^\infty] \otimes_W W_m, \widetilde{A}_2[p^\infty] \otimes_W W_m) \cong R_m \cong \mathcal{O}_L + p^{m-1}R$$

in the notation of Lemma 8.2.2, and therefore $m = \frac{1}{2}\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(f))$ by the above calculation. □

With $(\mathbf{A}_1, \mathbf{A}_2)$ as above, suppose $p \mid d_B$ and $\mathfrak{P}$ does not divide $\ker(\theta)$. As usual $A_j \cong M_j \otimes_{\mathcal{O}_{K_j}} E_j$ for some elliptic curve E_j. Choose isomorphisms $E_j[p^\infty] \cong \mathfrak{g}$ so that the CM actions $g_1 : \mathcal{O}_{K_1,p} \to \Delta$ and $g_2 : \mathcal{O}_{K_2,p} \to \Delta$ on E_1 and E_2 have the same image $\mathcal{O}_L \cong \mathbb{Z}_{p^2}$. Fix a uniformizer $\Pi \in \Delta$ satisfying $\Pi g_1(x) = g_1(\overline{x})\Pi$ for all $x \in \mathcal{O}_{K_1,p}$. There is an isomorphism of $\mathbb{Z}_p$-modules $L_p(\mathbf{A}_1, \mathbf{A}_2) \cong R'$, where

$$R' = \left\{ \begin{bmatrix} px & y\Pi \\ y\Pi & x \end{bmatrix} : x, y \in \mathcal{O}_L \right\},$$

and the quadratic form $\deg^*$ on $L_p(\mathbf{A}_1, \mathbf{A}_2)$ is identified with the quadratic form uQ' on R' defined in Proposition 7.2.4. There is a decomposition of left $\mathcal{O}_L$-modules $R' = R'_+ \oplus R'_-$, where $R'_+ = \mathcal{O}_L P_1$

and $R'_- = \mathcal{O}_L P_2$, with

$$P_1 = \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 0 & \Pi \\ \Pi & 0 \end{bmatrix}.$$

Lemma 8.2.4. *With notation as above, let $\mathscr{A}_j$ be the universal deformation of A_j to $\mathscr{W} = W$, and for each integer $m \geqslant 1$ set*

$$R'_m = \mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W_m}(\mathscr{A}_1 \otimes_W W_m, \mathscr{A}_2 \otimes_W W_m) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Then the reduction map $R'_m \hookrightarrow R'$ induces an isomorphism

$$R'_m \cong \mathcal{O}_L P_1 + p^{m-1} \mathcal{O}_L P_2.$$

Proof. The proof is very similar to that of Lemma 8.2.2, using the following two facts. For each $j \in \{1, 2\}$ there is a unique $\mathcal{O}_j$-stable direct summand $M_j \subset \widetilde{H}_1^{\mathrm{dR}}(A_j)$ whose image under the reduction map $\widetilde{H}_1^{\mathrm{dR}}(A_j) \to H_1^{\mathrm{dR}}(A_j)$ is $\mathrm{Fil}(A_j)$, and such that a diagram such as (8.2.1) commutes, corresponding to the unique deformation $\mathscr{A}_j \otimes_W W_m$ of A_j to W_m. Any $f \in R'$ lifts to an element of R'_m if and only if $\widetilde{f}(M_1) \subset M_2$, where $\widetilde{f} : \widetilde{H}_1^{\mathrm{dR}}(A_1) \to \widetilde{H}_1^{\mathrm{dR}}(A_2)$ is the unique lift of $f : H_1^{\mathrm{dR}}(A_1) \to H_1^{\mathrm{dR}}(A_2)$. □

Proposition 8.2.5. *If $p \mid d_B$ and $\mathfrak{P}$ does not divide* $\ker(\theta)$*, then* $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ *is represented by a local Artinian $\mathscr{W}$-algebra of length*

$$\frac{\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(f)) + 1}{2}.$$

Proof. The decomposition $R' = R'_+ \oplus R'_-$ is orthogonal with respect to the quadratic from $\deg^*$. Fix ring isomorphisms

$$\mathrm{End}_{\mathcal{O}_B}(A_1) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong R \cong \mathrm{End}_{\mathcal{O}_B}(A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_p,$$

with R as in the proof of Proposition 8.2.3. Define $\varphi_\pm : \mathcal{O}_{K,p} \to \mathcal{O}_L \subset R$ by

$$\varphi_+(x_1 \otimes x_2) = \kappa_2(x_2)\kappa_1(\overline{x}_1) = \mathrm{diag}(g_2(x_2)g_1(\overline{x}_1), g_2(x_2)g_1(\overline{x}_1))$$
$$\varphi_-(x_1 \otimes x_2) = \kappa_2(x_2)\kappa_1(x_1) = \mathrm{diag}(g_2(x_2)g_1(x_1), g_2(x_2)g_1(x_1))$$

and let

$$\Phi = \varphi_+ \times \varphi_- : \mathcal{O}_{K,p} \to \mathcal{O}_L \times \mathcal{O}_L.$$

The action of $\mathcal{O}_K$ on R' is then given by

$$x \bullet f = \varphi_+(x) f_+ + \varphi_-(x) f_-$$

for $f = f_+ + f_-$, where we are viewing R' as a left R-module. As before,

$$\Phi(\deg_{\mathrm{CM}}(f)) = (\deg^*(f_+), \deg^*(f_-))$$

and thus

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}_+}(\deg_{\mathrm{CM}}(f)) &= \mathrm{ord}_p(\deg^*(f_+)) \\ \mathrm{ord}_{\mathfrak{p}_-}(\deg_{\mathrm{CM}}(f)) &= \mathrm{ord}_p(\deg^*(f_-)), \end{aligned}$$

where $\mathfrak{p}_- = \mathfrak{p}$ and $\mathfrak{p}_+ = \overline{\mathfrak{p}}$. The key difference now is that $\deg^*(P_2) = uQ'(P_2) = -up$, so for any integer $m \geqslant 1$ and any $f \in R'$ we have

$$\begin{aligned} f \in \mathcal{O}_L P_1 + p^{m-1}\mathcal{O}_L P_2 &\iff f_- \in p^{m-1}\mathcal{O}_L P_2 \\ &\iff \mathrm{ord}_p(\deg^*(f_-)) \geqslant 2m - 1 \\ &\iff \frac{\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(f)) + 1}{2} \geqslant m. \end{aligned}$$

If $(\widetilde{\mathbf{A}}_1, \widetilde{\mathbf{A}}_2)$ is the universal deformation of $(\mathbf{A}_1, \mathbf{A}_2)$, then $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ is represented by $W_m = W/(p^m)$, where m is the largest integer such that

$$f \in \mathrm{Hom}_{\mathcal{O}_B}(A_1[p^\infty], A_2[p^\infty]) \cong R'$$

lifts to an element of

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W_m}(\widetilde{A}_1[p^\infty] \otimes_W W_m, \widetilde{A}_2[p^\infty] \otimes_W W_m) \cong R'_m \cong \mathcal{O}_L P_1 + p^{m-1}\mathcal{O}_L P_2.$$

The formula for m then follows from the above calculation. □

Proposition 8.2.6. *If $p \nmid d_B$ and p is ramified in K_1 or K_2, then* $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ *is represented by a local Artinian $\mathscr{W}$-algebra of length*

$$\frac{\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(f)) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}) + 1}{2}.$$

Proof. Suppose p is ramified in K_2 and inert in K_1, and let $\mathcal{O}_{L_j}$ be the image of $\kappa_j : \mathcal{O}_{K_j,p} \to \Delta$. If

$\varpi \in \mathcal{O}_{K_2,p}$ is a uniformizer then $\pi = 1 \otimes \varpi$ is a uniformizer of $\mathcal{O}_{K,p}$ and $\Pi = \kappa_2(\varpi)$ is a uniformizer of $\mathcal{O}_{L_2}$ and of Δ. The action of $\pi \in \mathcal{O}_{K,p}$ on $L_p(\mathbf{A}_1, \mathbf{A}_2) \cong \Delta$ is then given by $\pi \bullet x = \Pi x$. By Proposition 7.2.5 there is an $\mathcal{O}_{K,p}$-linear isomorphism

$$(\mathcal{O}_{K,p}, \beta \cdot \mathrm{N}_{K_p/F_p}) \cong (\Delta, \deg_{\mathrm{CM}}),$$

with $\beta\mathcal{O}_{F,p} = \mathfrak{p}\mathfrak{D}^{-1}\mathcal{O}_{F,p}$, so by $\mathcal{O}_{K,p}$-linearity this isomorphism sends $\pi^m\mathcal{O}_{K,p}$ isomorphically to $\Pi^m\Delta$. Viewing f both as an element of Δ and as an element of $\mathcal{O}_{K,p}$, we have

$$\begin{aligned} v_\Delta(f) &= \mathrm{ord}_\pi(f) \\ &= \mathrm{ord}_{\mathfrak{P}}(f) \\ &= \tfrac{1}{2}\mathrm{ord}_{\mathfrak{p}}(\mathrm{N}_{K_p/F_p}(f)) \\ &= \frac{\mathrm{ord}_{\mathfrak{p}}(\beta\mathrm{N}_{K_p/F_p}(f)) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}) - 1}{2} \\ &= \frac{\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(f)) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}) - 1}{2}. \end{aligned}$$

The functor

$$\begin{aligned} \mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2) &\cong \mathrm{Def}_{\mathcal{O}_B}(A_1[p^\infty], \mathcal{O}_{L_1}) \times \mathrm{Def}_{\mathcal{O}_B}(A_2[p^\infty], \mathcal{O}_{L_2}) \\ &\cong \mathrm{Def}(\mathfrak{g}, \mathcal{O}_{L_1}) \times \mathrm{Def}(\mathfrak{g}, \mathcal{O}_{L_2}) \end{aligned}$$

is represented by $\mathscr{W}\widehat{\otimes}_{\mathscr{W}}\mathscr{W} \cong \mathscr{W}$. Since p is ramified in K_2, the extension $K_{\mathfrak{P}} = K_p$ of $K_{2,p}$ is unramified, which means $\mathscr{W} = \mathscr{W}_{L_2}$, where $L_2 \cong K_{2,p}$ is the fraction field of $\mathcal{O}_{L_2}$. For $j \in \{1, 2\}$ let $\mathfrak{G}^{(j)}$ be the universal deformation of $\mathfrak{g}$, with its $\mathcal{O}_{L_j}$-action, to $\mathscr{W}$, and for any integer $m \geqslant 1$ set $\mathfrak{G}^{(j)}_m = \mathfrak{G}^{(j)} \otimes_{\mathscr{W}} \mathscr{W}/(\pi^m)$. Let $(\mathfrak{H}_1, \mathfrak{H}_2)$ be the p-divisible group of the universal deformation of $(\mathbf{A}_1, \mathbf{A}_2)$. Since $p \nmid d_B$, we have seen that there is an $\mathcal{O}_B$-linear isomorphism $\mathfrak{H}_j \cong \mathfrak{G}^{(j)} \times \mathfrak{G}^{(j)}$. The functor $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ is represented by $\mathscr{W}_m = \mathscr{W}/(\pi^m)$, where m is the largest integer such that $f \in \mathrm{Hom}_{\mathcal{O}_B}(A_1[p^\infty], A_2[p^\infty]) \cong \mathrm{End}(\mathfrak{g})$ lifts to an element of

$$\mathrm{Hom}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathscr{W}_m}(\mathfrak{H}_1 \otimes_{\mathscr{W}} \mathscr{W}_m, \mathfrak{H}_2 \otimes_{\mathscr{W}} \mathscr{W}_m) \cong \mathrm{Hom}_{\mathscr{W}_m}(\mathfrak{G}^{(1)}_m, \mathfrak{G}^{(2)}_m).$$

Viewing f as an element of $\mathrm{End}(\mathfrak{g}) = \Delta$, factor $f = \Pi^m u$ with $u \in \Delta^\times$ and $m = v_\Delta(f)$. Suppose u lifts to a homomorphism $\mathfrak{G}^{(1)}_m \to \mathfrak{G}^{(2)}_m$. Since $u \in \Delta^\times$, this lift is an isomorphism, and since $\Pi \in \mathcal{O}_{L_2}$ lifts to an endomorphism of $\mathfrak{G}^{(2)}$, $u^{-1} \circ \Pi \circ u$ lifts to an endomorphism of $\mathfrak{G}^{(1)}_m$. As $\mathcal{O}_{L_1} \cong \mathbb{Z}_{p^2}$ and $u^{-1}\Pi u$ generate Δ as a $\mathbb{Z}_p$-algebra, every element of Δ lifts to an endomorphism of

$\mathfrak{G}_m^{(1)}$ and thus by (8.1.1),

$$\Delta \cong \mathrm{End}_{\mathscr{W}_m}(\mathfrak{G}_m^{(1)}) \cong \mathrm{End}_{\mathscr{W}_m}(\mathfrak{G}_m^{(2)}) \cong \mathcal{O}_{L_2} + \Pi^{m-1}\Delta.$$

Here we are using that $\mathscr{W} = \mathscr{W}_{L_2}$. This shows $m = 1$ and therefore u lifts to a homomorphism $\mathfrak{G}_1^{(1)} \to \mathfrak{G}_1^{(2)}$, but not to $\mathfrak{G}_2^{(1)} \to \mathfrak{G}_2^{(2)}$. It follows from [28, Proposition 5.2] that $f = \Pi^m u$ lifts to $\mathfrak{G}_{m+1}^{(1)} \to \mathfrak{G}_{m+1}^{(2)}$ but not to $\mathfrak{G}_{m+2}^{(1)} \to \mathfrak{G}_{m+2}^{(2)}$, so $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ is represented by $\mathscr{W}/(\pi^{m+1})$, where

$$m + 1 = v_\Delta(f) + 1 = \frac{\mathrm{ord}_\mathfrak{p}(\deg_{\mathrm{CM}}(f)) + \mathrm{ord}_\mathfrak{p}(\mathfrak{D}) + 1}{2}. \qquad \square$$

8.3 The étale local ring

Let $\mathscr{X}$ be a stack over $\mathrm{Spec}(\mathcal{O}_K)$ and let $z \in \mathscr{X}(\overline{\mathbb{F}}_\mathfrak{P})$ be a geometric point. For any object R of **CLN** there is an equivalence of categories between the category of morphisms of stacks $\mathrm{Spec}(R) \to \mathscr{X}$ over $\mathrm{Spec}(\mathcal{O}_K)$ and the category $\mathscr{X}(R)$, the fiber of $\mathscr{X}$ over R, by a form of Yoneda's lemma, so we can view a geometric point in either way. An *étale neighborhood* of z is a commutative diagram in the category of stacks over $\mathrm{Spec}(\mathcal{O}_K)$

$$\begin{tikzcd}
 & U \arrow[d] \\
\mathrm{Spec}(\overline{\mathbb{F}}_\mathfrak{P}) \arrow[ru, "\widetilde{z}"] \arrow[r, "z"'] & \mathscr{X}
\end{tikzcd}$$

where U is an $\mathcal{O}_K$-scheme and $U \to \mathscr{X}$ is an étale morphism. The *strictly Henselian local ring* of $\mathscr{X}$ at z is the direct limit

$$\mathscr{O}^{\mathrm{sh}}_{\mathscr{X},z} = \varinjlim_{(U,\widetilde{z})} \mathscr{O}_{U,\widetilde{z}}$$

over all étale neighborhoods of z, where $\mathscr{O}_{U,\widetilde{z}}$ is the local ring of the scheme U at the image of $\widetilde{z}$. The ring $\mathscr{O}^{\mathrm{sh}}_{\mathscr{X},z}$ is a strictly Henselian local ring with residue field $\overline{\mathbb{F}}_\mathfrak{P}$. Suppose $C \subset \mathscr{W}$ is a subring that is étale as an $\mathcal{O}_K$-algebra, and let $(U, \widetilde{z})$ be an étale neighborhood of z. Then the diagram

$$\begin{tikzcd}
 & U \times_{\mathrm{Spec}(\mathcal{O}_K)} \mathrm{Spec}(C) \arrow[d] \\
 & U \arrow[d] \\
\mathrm{Spec}(\overline{\mathbb{F}}_\mathfrak{P}) \arrow[ruu, "{(\widetilde{z},f)}"] \arrow[r, "z"] & \mathscr{X}
\end{tikzcd}$$

is an étale neighborhood of z, where $f : \mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{P}}) \to \mathrm{Spec}(C)$ is determined by the ring homomorphism $C \hookrightarrow \mathscr{W} \to \overline{\mathbb{F}}_{\mathfrak{P}}$. This shows $\mathscr{O}^{\mathrm{sh}}_{\mathscr{X},z}$ is a C-algebra. The union of all such C is dense in $\mathscr{W}$, so the completed strictly Henselian local ring $\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X},z}$ is a $\mathscr{W}$-algebra.

Theorem 8.3.1. *Let $\alpha \in F^\times$, let $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ be a ring homomorphism, and suppose $\mathfrak{P} \subset \mathcal{O}_K$ is a prime ideal lying over a prime p. Set*

$$\nu_{\mathfrak{p}}(\alpha) = \frac{1}{2}\mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{p}\mathfrak{D}), \quad \nu'_{\mathfrak{p}}(\alpha) = \frac{1}{2}\mathrm{ord}_{\mathfrak{p}}(\alpha),$$

where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$. For any $x = (\mathbf{A}_1, \mathbf{A}_2, f) \in \mathscr{X}_{\theta,\alpha}(\overline{\mathbb{F}}_{\mathfrak{P}})$, the strictly Henselian local ring $\mathscr{O}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}$ is Artinian of length $\nu_{\mathfrak{p}}(\alpha)$ if $p \nmid d_B$ or $p \mid d_B$ and $\mathfrak{P} \nmid \ker(\theta)$, and is Artinian of length $\nu'_{\mathfrak{p}}(\alpha)$ if $p \mid d_B$ and $\mathfrak{P} \mid \ker(\theta)$.

By length we mean the length of the ring as a module over itself.

Proof. Let R be an Artinian object of **CLN** and suppose $z \in \mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)(R)$. Then z is an element of $[\mathscr{X}_{\theta,\alpha}(R)]$ whose image under the reduction map $[\mathscr{X}_{\theta,\alpha}(R)] \to [\mathscr{X}_{\theta,\alpha}(\overline{\mathbb{F}}_{\mathfrak{P}})]$ is the isomorphism class of x (see Corollary 5.2.9), and thus there is a commutative diagram

$$\begin{tikzcd}
\mathrm{Spec}(R) \arrow[dr, "z"] & \\
\mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{P}}) \arrow[u] \arrow[r, "x"'] & \mathscr{X}_{\theta,\alpha},
\end{tikzcd}$$

where we are fixing a representative $z \in \mathscr{X}_{\theta,\alpha}(R)$ of the isomorphism class $z \in [\mathscr{X}_{\theta,\alpha}(R)]$. Given an étale neighborhood of x,

$$\begin{tikzcd}
& U \arrow[d] \\
\mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{P}}) \arrow[ur, "\widetilde{x}"] \arrow[r, "x"'] & \mathscr{X}_{\theta,\alpha},
\end{tikzcd}$$

there is a unique morphism $\widetilde{z} : \mathrm{Spec}(R) \to U$ making the diagram

$$\begin{tikzcd}
\mathrm{Spec}(R) \arrow[r, "\widetilde{z}"] \arrow[dr] & U \arrow[d] \\
\mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{P}}) \arrow[u] \arrow[ur] \arrow[r, "x"'] & \mathscr{X}_{\theta,\alpha}
\end{tikzcd}$$

commute. This follows from the closed immersion $\mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{P}}) \to \mathrm{Spec}(R)$ being defined by a nilpotent ideal (R is Artinian) and the étale morphism $U \to \mathscr{X}_{\theta,\alpha}$ necessarily being formally étale (see [17,

p. 30] for a proof in the case of schemes). Then $\widetilde{z}$ induces a ring homomorphism $\widetilde{z} : \mathscr{O}_{U,\widetilde{x}} \to R$, and by varying the étale neighborhood we obtain a map $\widetilde{z} : \mathscr{O}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x} \to R$ that induces the identity $\overline{\mathbb{F}}_{\mathfrak{P}} \to \overline{\mathbb{F}}_{\mathfrak{P}}$ on residue fields (by the commutativity of the above diagram for each étale neighborhood). In particular, $\widetilde{z}$ maps the maximal ideal of $\mathscr{O}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}$ onto the maximal ideal of R and hence extends uniquely to $\widetilde{z} \in \mathrm{Hom}_{\mathbf{CLN}}(\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}, R)$, as R is complete. Define a map

$$\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)(R) \to \mathrm{Hom}_{\mathbf{CLN}}(\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}, R)$$

by $z \mapsto \widetilde{z}$.

Now let $z \in \mathrm{Hom}_{\mathbf{CLN}}(\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}, R)$. Viewing z as a morphism

$$z : \mathrm{Spec}(R) \to \mathrm{Spec}(\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}),$$

consider the morphism of stacks over $\mathrm{Spec}(\mathcal{O}_K)$

$$z' : \mathrm{Spec}(R) \xrightarrow{z} \mathrm{Spec}(\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}) \to \mathrm{Spec}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}) \to \mathscr{X}_{\theta,\alpha}.$$

This corresponds to an object z' of $\mathscr{X}_{\theta,\alpha}(R)$. Since $z : \widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x} \to R$ induces the identity $\overline{\mathbb{F}}_{\mathfrak{P}} \to \overline{\mathbb{F}}_{\mathfrak{P}}$ on residue fields, the diagram

$$\begin{tikzcd}
\mathrm{Spec}(R) \arrow[dr, "z'"] & \\
\mathrm{Spec}(\overline{\mathbb{F}}_{\mathfrak{P}}) \arrow[u] \arrow[r, "x"'] & \mathscr{X}_{\theta,\alpha}
\end{tikzcd}$$

commutes, so $z' \in \mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)(R)$. The map

$$\mathrm{Hom}_{\mathbf{CLN}}(\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}, R) \to \mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)(R)$$

defined by $z \mapsto z'$ is the inverse of the map $z \mapsto \widetilde{z}$ defined above, so there is a bijection

$$\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)(R) \cong \mathrm{Hom}_{\mathbf{CLN}}(\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}, R)$$

for any Artinian R in **CLN**. As in Corollary 5.1.3 it follows that there is such a bijection for any R in **CLN**, so the functor $\mathrm{Def}(\mathbf{A}_1, \mathbf{A}_2, f)$ is represented by the ring $\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}$. The result now follows from Propositions 8.2.1, 8.2.3, 8.2.5, 8.2.6, and the fact that $\mathrm{length}(\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x}) = \mathrm{length}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x})$. □

Chapter 9

Final formula

9.1 Degree of $\mathscr{X}_{\theta,\alpha}$

As in the introduction, let χ be the quadratic Hecke character associated with the extension K/F, so if v is a place of F then $\chi_v : F_v^\times \to \{\pm 1\}$ is given by

$$\chi_v(x) = \begin{cases} 1 & \text{if } x \in \mathrm{N}_{K_v/F_v}(K_v^\times) \\ -1 & \text{if } x \notin \mathrm{N}_{K_v/F_v}(K_v^\times). \end{cases}$$

We may interpret χ as a character on ideals as follows. Since K_v/F_v is unramified for any finite place v of F, the norm map $\mathrm{N}_{K_v/F_v} : \mathcal{O}_{K,v}^\times \to \mathcal{O}_{F,v}^\times$ is surjective, so if $\mathfrak{a}$ is a fractional $\mathcal{O}_F$-ideal, then the definition $\chi_v(\mathfrak{a}) = \chi_v(\alpha_v)$ is independent of the choice of $\alpha_v \in F_v^\times$ satisfying $\alpha_v \mathcal{O}_{F,v} = \mathfrak{a}\mathcal{O}_{F,v}$.

For any $\alpha \in F^\times$ totally positive and any ring homomorphism $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$, define a finite set of prime ideals

$$\mathrm{Diff}_\theta(\alpha) = \{\mathfrak{p} \subset \mathcal{O}_F : \chi_{\mathfrak{p}}(\alpha\mathfrak{a}_\theta\mathfrak{D}) = -1\},$$

where $\mathfrak{a}_\theta = \ker(\theta) \cap \mathcal{O}_F$. It follows from the product formula $\prod_v \chi_v(x) = 1$ that $\mathrm{Diff}_\theta(\alpha)$ has odd cardinality, and in particular is nonempty. (If v_1, v_2 are the two archimedean places of F, then $\chi_{v_1}(\alpha\sqrt{D})\chi_{v_2}(\alpha\sqrt{D}) = -1$, where $D = \mathrm{disc}(F)$ and thus $\mathfrak{D} = \sqrt{D}\mathcal{O}_F$.) Note that if $\mathfrak{p} \in \mathrm{Diff}_\theta(\alpha)$ then $\mathfrak{p}$ is inert in K. The only other possibility is $\mathfrak{p}$ is split in K, in which case

$$K_{\mathfrak{p}} = F_{\mathfrak{p}} \otimes_F K \cong F_{\mathfrak{p}} \times F_{\mathfrak{p}}$$

and the norm map $\mathrm{N} : K_{\mathfrak{p}} \to F_{\mathfrak{p}}$ is just multiplication. If $\alpha\mathfrak{a}_\theta\mathfrak{D}\mathcal{O}_{F,\mathfrak{p}} = \xi\mathcal{O}_{F,\mathfrak{p}}$ for some $\xi \in F_{\mathfrak{p}}^\times$, then clearly $\xi = \mathrm{N}(\xi, 1)$, so $\chi_{\mathfrak{p}}(\alpha\mathfrak{a}_\theta\mathfrak{D}) = 1$. Recall that $\Gamma = \mathrm{Cl}(\mathcal{O}_{K_1}) \times \mathrm{Cl}(\mathcal{O}_{K_2})$.

Lemma 9.1.1. *For any prime $\mathfrak{P} \subset \mathcal{O}_K$ and any ring homomorphism $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$, we have $\#[\mathscr{X}_\theta(\overline{\mathbb{F}}_\mathfrak{P})] = |\Gamma|$.*

Proof. Let $\theta_j = \theta|_{\mathcal{O}_{K_j}}$. By definition, an object of $\mathscr{X}_\theta(\overline{\mathbb{F}}_\mathfrak{P})$ is a pair $(\mathbf{A}_1, \mathbf{A}_2)$ with $\mathbf{A}_j$ an object of $\mathscr{Y}_j^{\theta_j}(\overline{\mathbb{F}}_\mathfrak{P})$, so by what we proved in Section 5.2,

$$\#[\mathscr{X}_\theta(\overline{\mathbb{F}}_\mathfrak{P})] = \#[\mathscr{Y}_1^{\theta_1}(\overline{\mathbb{F}}_\mathfrak{P})] \cdot \#[\mathscr{Y}_2^{\theta_2}(\overline{\mathbb{F}}_\mathfrak{P})] = |\operatorname{Cl}(\mathcal{O}_{K_1})| \cdot |\operatorname{Cl}(\mathcal{O}_{K_2})| = |\Gamma|. \qquad \square$$

Proposition 9.1.2. *Suppose $\alpha \in F^\times$ and $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ is a ring homomorphism. If $\#\operatorname{Diff}_\theta(\alpha) > 1$ then $\mathscr{X}_{\theta,\alpha} = \varnothing$. Suppose $\operatorname{Diff}_\theta(\alpha) = \{\mathfrak{p}\}$, let $\mathfrak{P} \subset \mathcal{O}_K$ be the prime over $\mathfrak{p}$, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Then the stack $\mathscr{X}_{\theta,\alpha}$ is supported in characteristic p. More specifically, it only has geometric points over the field $\overline{\mathbb{F}}_\mathfrak{P}$ (if it has any at all).*

Proof. By Proposition 3.2.7 the stack $\mathscr{X}_{\theta,\alpha}$ has no geometric points in characteristic 0. Suppose $\mathscr{X}_{\theta,\alpha}(\overline{\mathbb{F}}_\mathfrak{P}) \neq \varnothing$ for some prime ideal $\mathfrak{P} \subset \mathcal{O}_K$. Fix $(\mathbf{A}_1, \mathbf{A}_2, f) \in \mathscr{X}_{\theta,\alpha}(\overline{\mathbb{F}}_\mathfrak{P})$, and let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$ and $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Any prime ideal $\mathfrak{q}$ of $\mathcal{O}_F$ lying over p or lying over any divisor of d_B is inert in K (by Proposition 3.2.7(d) and our assumption about the primes dividing d_B), so for such a $\mathfrak{q}$,

$$\chi_\mathfrak{l}(\mathfrak{q}) = \begin{cases} -1 & \text{if } \mathfrak{l} = \mathfrak{q} \\ 1 & \text{if } \mathfrak{l} \neq \mathfrak{q} \end{cases}$$

for any prime $\mathfrak{l} \subset \mathcal{O}_F$. By Theorem 7.3.1, the quadratic space $(\widehat{K}, \beta \cdot \mathrm{N}_{K/F})$ represents α for any $\beta \in \widehat{F}^\times$ satisfying $\beta\widehat{\mathcal{O}}_F = \mathfrak{a}_\theta \mathfrak{p} \mathfrak{D}^{-1} \widehat{\mathcal{O}}_F$. It follows that $\chi_\mathfrak{l}(\alpha) = \chi_\mathfrak{l}(\mathfrak{a}_\theta \mathfrak{p} \mathfrak{D}^{-1})$ for every prime $\mathfrak{l} \subset \mathcal{O}_F$, so $\operatorname{Diff}_\theta(\alpha) = \{\mathfrak{p}\}$. This shows that if $\mathscr{X}_{\theta,\alpha}(\overline{\mathbb{F}}_\mathfrak{P}) \neq \varnothing$ then $\operatorname{Diff}_\theta(\alpha) = \{\mathfrak{p}\}$, where $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_F$. $\square$

Recall the definition of the arithmetic degree of $\mathscr{X}_{\theta,\alpha}$ from the introduction:

$$\deg(\mathscr{X}_{\theta,\alpha}) = \sum_{\mathfrak{P} \subset \mathcal{O}_K} \log(|\mathbb{F}_\mathfrak{P}|) \sum_{x \in [\mathscr{X}_{\theta,\alpha}(\overline{\mathbb{F}}_\mathfrak{P})]} \frac{\operatorname{length}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x})}{|\operatorname{Aut}(x)|}.$$

Theorem 9.1.3. *Let $\alpha \in F^\times$ be totally positive and suppose $\alpha \in \mathfrak{D}^{-1}$. Let $\theta : \mathcal{O}_K \to \mathcal{O}_B/\mathfrak{m}_B$ be a ring homomorphism with $\mathfrak{a}_\theta = \ker(\theta) \cap \mathcal{O}_F$, suppose $\operatorname{Diff}_\theta(\alpha) = \{\mathfrak{p}\}$, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathcal{O}_F$.*
(a) *If $p \nmid d_B$ then*

$$\deg(\mathscr{X}_{\theta,\alpha}) = \frac{1}{2}\log(p) \cdot \operatorname{ord}_\mathfrak{p}(\alpha\mathfrak{p}\mathfrak{D}) \cdot \rho(\alpha\mathfrak{a}_\theta^{-1}\mathfrak{p}^{-1}\mathfrak{D}).$$

(b) *Suppose $p \mid d_B$ and let $\mathfrak{P} \subset \mathcal{O}_K$ be the prime over $\mathfrak{p}$. If $\mathfrak{P}$ divides $\ker(\theta)$ then*

$$\deg(\mathscr{X}_{\theta,\alpha}) = \frac{1}{2}\log(p) \cdot \operatorname{ord}_\mathfrak{p}(\alpha) \cdot \rho(\alpha\mathfrak{a}_\theta^{-1}\mathfrak{p}^{-1}\mathfrak{D}).$$

If $\mathfrak{P}$ *does not divide* $\ker(\theta)$ *then*

$$\deg(\mathscr{X}_{\theta,\alpha}) = \frac{1}{2}\log(p) \cdot \mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{p}) \cdot \rho(\alpha\mathfrak{a}_\theta^{-1}\mathfrak{p}^{-1}\mathfrak{D}).$$

If $\alpha \notin \mathfrak{D}^{-1}$ *or if* $\#\,\mathrm{Diff}_\theta(\alpha) > 1$*, then* $\deg(\mathscr{X}_{\theta,\alpha}) = 0$.

Proof. The group $\mathrm{Aut}(\mathbf{A}_1, \mathbf{A}_2)$ acts on the set $L(\mathbf{A}_1, \mathbf{A}_2)$ according to the rule

$$(g_1, g_2) \cdot f = g_2^{-1} \circ f \circ g_1$$

for $(g_1, g_2) \in \mathrm{Aut}(\mathbf{A}_1, \mathbf{A}_2)$ and $f \in L(\mathbf{A}_1, \mathbf{A}_2)$. Under this action the stabilizer of f is

$$\begin{aligned}\mathrm{Stab}(f) &= \{(g_1, g_2) \in \mathrm{Aut}(\mathbf{A}_1, \mathbf{A}_2) : g_2^{-1} \circ f \circ g_1 = f\} \\ &= \mathrm{Aut}(\mathbf{A}_1, \mathbf{A}_2, f).\end{aligned}$$

(a) Using Theorem 8.3.1, Proposition 9.1.2, Lemma 4.1.3, and the fact that $|\mathbb{F}_{\mathfrak{P}}| = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P}) = p^2$,

$$\begin{aligned}\deg(\mathscr{X}_{\theta,\alpha}) &= \log(|\mathbb{F}_{\mathfrak{P}}|) \sum_{x \in [\mathscr{X}_{\theta,\alpha}(\overline{\mathbb{F}}_{\mathfrak{P}})]} \frac{\mathrm{length}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{X}_{\theta,\alpha},x})}{|\mathrm{Aut}(x)|} \\ &= 2\log(p)\nu_{\mathfrak{p}}(\alpha) \sum_{(\mathbf{A}_1,\mathbf{A}_2,f) \in [\mathscr{X}_{\theta,\alpha}(\overline{\mathbb{F}}_{\mathfrak{P}})]} \frac{1}{|\mathrm{Aut}(\mathbf{A}_1, \mathbf{A}_2, f)|} \\ &= 2\log(p)\nu_{\mathfrak{p}}(\alpha) \sum_{(\mathbf{A}_1,\mathbf{A}_2) \in [\mathscr{X}_{\theta}(\overline{\mathbb{F}}_{\mathfrak{P}})]} \sum_{\substack{f \in L(\mathbf{A}_1,\mathbf{A}_2) \\ \deg_{\mathrm{CM}}(f) = \alpha}} \frac{1}{|\mathrm{Aut}(\mathbf{A}_1, \mathbf{A}_2, f)|} \cdot \frac{|\mathrm{Stab}(f)|}{|\mathrm{Aut}(\mathbf{A}_1, \mathbf{A}_2)|} \\ &= 2\log(p)\nu_{\mathfrak{p}}(\alpha) \sum_{(\mathbf{A}_1,\mathbf{A}_2) \in [\mathscr{X}_{\theta}(\overline{\mathbb{F}}_{\mathfrak{P}})]} \sum_{\substack{f \in L(\mathbf{A}_1,\mathbf{A}_2) \\ \deg_{\mathrm{CM}}(f) = \alpha}} \frac{1}{w_1 w_2}.\end{aligned}$$

Now using Proposition 4.1.4, Theorem 7.3.3, and Lemma 9.1.1, we have

$$\begin{aligned}\deg(\mathscr{X}_{\theta,\alpha}) &= 2\log(p)\nu_{\mathfrak{p}}(\alpha) \sum_{(\mathbf{A}_1,\mathbf{A}_2) \in [\mathscr{X}_{\theta}(\overline{\mathbb{F}}_{\mathfrak{P}})]} \frac{1}{|\Gamma|} \sum_{(\mathfrak{s}_1,\mathfrak{s}_2) \in \Gamma} \sum_{\substack{f \in L(\mathfrak{s}_1 \otimes \mathbf{A}_1, \mathfrak{s}_2 \otimes \mathbf{A}_2) \\ \deg_{\mathrm{CM}}(f) = \alpha}} \frac{1}{w_1 w_2} \\ &= \log(p)\frac{\nu_{\mathfrak{p}}(\alpha)}{|\Gamma|} \sum_{(\mathbf{A}_1,\mathbf{A}_2) \in [\mathscr{X}_{\theta}(\overline{\mathbb{F}}_{\mathfrak{P}})]} \prod_{\ell} O_\ell(\alpha, \mathbf{A}_1, \mathbf{A}_2) \\ &= \log(p)\frac{\nu_{\mathfrak{p}}(\alpha)}{|\Gamma|} \sum_{(\mathbf{A}_1,\mathbf{A}_2) \in [\mathscr{X}_{\theta}(\overline{\mathbb{F}}_{\mathfrak{P}})]} \rho(\alpha\mathfrak{a}_\theta^{-1}\mathfrak{p}^{-1}\mathfrak{D}) \\ &= \frac{1}{2}\log(p) \cdot \mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{p}\mathfrak{D}) \cdot \rho(\alpha\mathfrak{a}_\theta^{-1}\mathfrak{p}^{-1}\mathfrak{D}).\end{aligned}$$

(b) Suppose $p \mid d_B$. If $\mathfrak{P}$ divides $\ker(\theta)$ then a similar calculation to that in (a), replacing $\nu_{\mathfrak{p}}(\alpha)$ with $\nu'_{\mathfrak{p}}(\alpha)$, gives the desired result. If $\mathfrak{P}$ does not divide $\ker(\theta)$ then the exact same calculation as in (a) gives the desired formula, noting that $\nu_{\mathfrak{p}}(\alpha) = \frac{1}{2}\mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{p})$ for $p \mid d_B$ (since p is unramified in F).

The final claim follows from Proposition 9.1.2 and the fact that $\deg_{\mathrm{CM}}$ takes values in $\mathfrak{D}^{-1}$. □

Chapter 10

Special endomorphisms of CM false elliptic curves

In this chapter we prove Theorem 4 of the introduction. The method of proof follows what was done in proving Theorem 9.1.3 and many of the proofs are very similar, but simpler. We continue with the same notation as in the previous chapters except now let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$ and discriminant d_K. We write $x \mapsto \overline{x}$ for the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$. For $\mathfrak{p} \subset \mathcal{O}_K$ a prime ideal, let $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ be the residue field. We assume that each prime dividing d_B is inert in K, so in particular K embeds into B (equivalently, K splits B). Let e_p and f_p be the ramification index and residue field degree of $K/\mathbb{Q}$ at a prime p, let s be the number of distinct prime factors of d_K, and set $\varepsilon_p = 1 - \mathrm{ord}_p(d_B)$.

10.1 Moduli spaces

Definition 10.1.1. Define $\mathscr{Y}$ to be the category whose objects are triples (A, i, κ) where (A, i) is a false elliptic curve over some $\mathcal{O}_K$-scheme with complex multiplication $\kappa : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_B}(A)$ (so in particular, A satisfies the CM normalization condition). A morphism $(A', i', \kappa') \to (A, i, \kappa)$ between two such triples defined over $\mathcal{O}_K$-schemes T and S, respectively, is a morphism of $\mathcal{O}_K$-schemes $T \to S$ together with an $\mathcal{O}_K$-linear isomorphism $A' \to A \times_S T$ of false elliptic curves.

Definition 10.1.2. Let $(A, i, \kappa) \in \mathscr{Y}(S)$ for some $\mathcal{O}_K$-scheme S. A *special endomorphism* of (A, κ) is an endomorphism $f \in \mathrm{End}_{\mathcal{O}_B}(A)$ satisfying

$$\kappa(x) \circ f = f \circ \kappa(\overline{x})$$

for all $x \in \mathcal{O}_K$. We write $L(A, \kappa)$ for the $\mathbb{Z}$-module of all special endomorphisms and set $V(A, \kappa) = L(A, \kappa) \otimes_{\mathbb{Z}} \mathbb{Q}$.

We make $L(A, \kappa)$ into a left $\mathcal{O}_K$-module through the action $x \cdot f = \kappa(x) \circ f$. There is the quadratic form $\deg^*$ on $L(A, \kappa)$ and this satisfies

$$\deg^*(x \cdot f) = \mathrm{N}_{K/\mathbb{Q}}(x) \cdot \deg^*(f)$$

for all $x \in \mathcal{O}_K$.

Definition 10.1.3. For any positive integer m, define $\mathscr{Y}^m$ to be the category whose objects are triples (A, κ, f) where $(A, i, \kappa) \in \mathscr{Y}(S)$ for some $\mathcal{O}_K$-scheme S and $f \in L(A, \kappa)$ satisfies $\deg^*(f) = m$ on every connected component of S. A morphism

$$(A', \kappa', f') \to (A, \kappa, f)$$

between two such triples, with (A', i', κ') and (A, i, κ) CM false elliptic curves over $\mathcal{O}_K$-schemes T and S, respectively, is a morphism of $\mathcal{O}_K$-schemes $T \to S$ together with an $\mathcal{O}_K$-linear isomorphism $g : A' \to A \times_S T$ of false elliptic curves such that the diagram

$$\begin{tikzcd}
A' \arrow[r, "g"] \arrow[d, "f'"'] & A \times_S T \arrow[d, "f \times \mathrm{id}_T"] \\
A' \arrow[r, "g"] & A \times_S T
\end{tikzcd}$$

commutes.

The same proofs as in Chapter 5 show that for any prime $\mathfrak{p} \subset \mathcal{O}_K$, the group $W_0 \times \mathrm{Cl}(\mathcal{O}_K)$ acts simply transitively on $[\mathscr{Y}(\overline{\mathbb{F}}_\mathfrak{p})]$ and that for any $A \in \mathscr{Y}(\overline{\mathbb{F}}_\mathfrak{p})$, there is an isomorphism of CM false elliptic curves $A \cong M \otimes_{\mathcal{O}_K} E$ for some $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_K$-module M, free of rank 4 over $\mathbb{Z}$, and some elliptic curve E over $\overline{\mathbb{F}}_\mathfrak{p}$ with CM by $\mathcal{O}_K$ (supersingular in the case of the prime below $\mathfrak{p}$ nonsplit in K).

Proposition 10.1.4. *If $(A, \kappa) \in \mathscr{Y}(\mathbb{C})$ then $V(A, \kappa) = 0$ and if $(A, \kappa) \in \mathscr{Y}(\overline{\mathbb{F}}_\mathfrak{p})$ then*

$$\dim_K(V(A, \kappa)) = \begin{cases} 1 & \textit{if } A \textit{ is supersingular} \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. First fix a homomorphism $\mathcal{O}_K \to \mathbb{C}$ and suppose $(A, \kappa) \in \mathscr{Y}(\mathbb{C})$. Since $\mathrm{End}_{\mathcal{O}_B}(A)$ is isomorphic to $\mathbb{Z}$ or an order in an imaginary quadratic field, $\kappa : \mathcal{O}_K \to \mathrm{End}_{\mathcal{O}_B}(A)$ is an isomorphism. It follows that $L(A, \kappa) = 0$. Now suppose $(A, \kappa) \in \mathscr{Y}(\overline{\mathbb{F}}_\mathfrak{p})$ for some prime $\mathfrak{p} \subset \mathcal{O}_K$. If $A \cong M \otimes_{\mathcal{O}_K} E$ with E ordinary, then $\mathrm{End}^0_{\mathcal{O}_B}(A) \cong K$ and $L(A, \kappa) = 0$ as above. If A is supersingular then

$\mathrm{End}^0_{\mathcal{O}_B}(A) \cong B^{(p)}$, where $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. As K is a simple $\mathbb{Q}$-algebra and $B^{(p)}$ is a central simple $\mathbb{Q}$-algebra, by the Noether-Skolem theorem applied to the two maps $K \to B^{(p)}$ given by $x \mapsto \kappa(x)$ and $x \mapsto \kappa(\overline{x})$, there is an $f \in (B^{(p)})^\times$ such that $\kappa(x) = f \circ \kappa(\overline{x}) \circ f^{-1}$ for all $x \in K$. This means $f \in V(A, \kappa)$, so $\dim_K(V(A, \kappa)) \geqslant 1$. However, the K-subspaces $\kappa(K)$ and $V(A, \kappa)$ in $B^{(p)}$ intersect trivially, so $B^{(p)} = \kappa(K) \oplus V(A, \kappa)$ and $\dim_K(V(A, \kappa)) = 1$. □

For each place $\ell \leqslant \infty$ of $\mathbb{Q}$ let $(\cdot\,,\cdot)_\ell : \mathbb{Q}_\ell^\times \times \mathbb{Q}_\ell^\times \to \{\pm 1\}$ be the Hilbert symbol. For each positive integer m define a finite set of prime numbers

$$\mathrm{Diff}_B(m) = \{\ell < \infty : (d_K, -m)_\ell \cdot \mathrm{inv}_\ell(B) = -1\}.$$

From the product formula

$$\prod_{\ell \leqslant \infty} (d_K, -m)_\ell \cdot \mathrm{inv}_\ell(B) = 1$$

and $(d_K, -m)_\infty \cdot \mathrm{inv}_\infty(B) = (-1, -1)_\infty \cdot \mathrm{inv}_\infty(B) = -1$, it follows that $\mathrm{Diff}_B(m)$ has odd cardinality. If ℓ is a prime number split in K then $\ell \nmid d_B$ by assumption and

$$\mathbb{Q}_\ell(\sqrt{d_K}) \cong K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell \times \mathbb{Q}_\ell.$$

The norm map $\mathbb{Q}_\ell(\sqrt{d_K}) \to \mathbb{Q}_\ell$ is then just multiplication, so clearly $-m$ is a norm from $\mathbb{Q}_\ell(\sqrt{d_K})$, which means $(d_K, -m)_\ell = 1$. Hence $(d_K, -m)_\ell \cdot \mathrm{inv}_\ell(B) = 1$, which shows $\ell \notin \mathrm{Diff}_B(m)$ if ℓ is split in K.

Proposition 10.1.5. *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal lying over a prime p. If $\mathscr{Y}^m(\overline{\mathbb{F}}_{\mathfrak{p}}) \neq \varnothing$ then* $\mathrm{Diff}_B(m) = \{p\}$.

Proof. Fix $(A, \kappa, f) \in \mathscr{Y}^m(\overline{\mathbb{F}}_{\mathfrak{p}})$. View K as a $\mathbb{Q}$-subalgebra of $B^{(p)}$ via $\kappa : K \to B^{(p)}$ and consider the element $f + f^t \in B^{(p)}$. By definition, $f^t = \lambda^{-1} \circ f^\vee \circ \lambda$, where $\lambda : A \to A^\vee$ is the usual principal polarization, so $f^t = f^\dagger$ where $g \mapsto g^\dagger$ is the Rosati involution on $\mathrm{End}^0_{\mathcal{O}_B}(A)$ corresponding to λ. Since $f + f^t$ is fixed by the Rosati involution, we have $f + f^t \in \mathbb{Z} \subset \mathrm{End}_{\mathcal{O}_B}(A)$. However, as f is a special endomorphism, for any $x \in K$,

$$\begin{aligned} x(f + f^t) &= xf + xf^t = xf + (\overline{x})^t f^t = xf + (f\overline{x})^t \\ &= f\overline{x} + (xf)^t = f\overline{x} + f^t\overline{x} = (f + f^t)\overline{x}, \end{aligned}$$

so from $f + f^t \in \mathbb{Z}$ it follows that $f + f^t = 0$. Hence

$$m = \deg^*(f) = f \circ f^t = -f^2.$$

Setting $\delta = \sqrt{d_K} \in K \subset B^{(p)}$, the $\mathbb{Q}$-algebra $B^{(p)}$ is generated by elements δ, f satisfying

$$\delta^2 = d_K, \quad f^2 = -m, \quad \delta f = -f\delta,$$

the last relation coming from $\overline{\delta} = -\delta$, so

$$B^{(p)} \cong \left(\frac{d_K, -m}{\mathbb{Q}}\right).$$

Therefore

$$(d_K, -m)_\ell \cdot \mathrm{inv}_\ell(B) = \mathrm{inv}_\ell(B^{(p)}) \cdot \mathrm{inv}_\ell(B) = \begin{cases} 1 & \text{if } \ell \neq p, \infty \\ -1 & \text{if } \ell = p, \infty, \end{cases}$$

which means $\mathrm{Diff}_B(m) = \{p\}$. □

Corollary 10.1.6. *If $\mathrm{Diff}_B(m) = \{p\}$ then there is a unique prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ over p and $\mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{q}) = \varnothing$ for every prime $\mathfrak{q} \neq \mathfrak{p}$. If $\# \mathrm{Diff}_B(m) > 1$ then $\mathscr{Y}^m = \varnothing$.*

Proof. If $\mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{q}) \neq \varnothing$ then $\mathrm{Diff}_B(m) = \{q\}$ where $q\mathbb{Z} = \mathfrak{q} \cap \mathbb{Z}$. Hence $p = q$ and then $\mathfrak{p} = \mathfrak{q}$ since p and q are nonsplit in K. □

10.2 Local quadratic spaces

Let m be a positive integer, p a prime nonsplit in K, $\mathfrak{p} \subset \mathcal{O}_K$ the prime over p, and $(A, \kappa) \in \mathscr{Y}(\overline{\mathbb{F}}_\mathfrak{p})$. For each prime ℓ set

$$L_\ell(A, \kappa) = L(A, \kappa) \otimes_\mathbb{Z} \mathbb{Z}_\ell, \quad V_\ell(A, \kappa) = V(A, \kappa) \otimes_\mathbb{Q} \mathbb{Q}_\ell.$$

Proposition 10.2.1. *If $\ell \neq p$ is a prime then there is an $\mathcal{O}_{K,\ell}$-linear isomorphism of quadratic spaces*

$$(\mathcal{O}_{K,\ell}, \beta_\ell \cdot \mathrm{N}_{K_\ell/\mathbb{Q}_\ell}) \cong (L_\ell(A, \kappa), \deg^*)$$

for some $\beta_\ell \in \mathbb{Z}_\ell$ with $\beta_\ell = -1$ if $\ell \nmid d_B$ and $\mathrm{ord}_\ell(\beta_\ell) = 1$ if $\ell \mid d_B$.

Proof. First suppose $\ell \nmid d_B$ and let $T_\ell = T_\ell(A)$ be the ℓ-adic Tate module of A. The standard idempotents $\varepsilon, \varepsilon' \in \mathrm{M}_2(\mathbb{Z}_\ell) \cong \mathcal{O}_B \otimes_\mathbb{Z} \mathbb{Z}_\ell$ induce a decomposition $T_\ell = \varepsilon T_\ell \oplus \varepsilon' T_\ell$. As the $\mathcal{O}_{K,\ell}$ and $\mathcal{O}_{B,\ell}$ actions on T_ℓ commute, the $\mathbb{Z}_\ell$-module εT_ℓ is an $\mathcal{O}_{K,\ell}$-module. In fact, εT_ℓ is a free $\mathcal{O}_{K,\ell}$-module of rank 1. Indeed, $\varepsilon T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a K_ℓ-vector space of dimension 1, so there is an isomorphism of K_ℓ-vector spaces $\varepsilon T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong K_\ell$, which identifies εT_ℓ with a finitely generated $\mathcal{O}_{K,\ell}$-submodule of K_ℓ, that is, a fractional $\mathcal{O}_{K,\ell}$-ideal. But every ideal of $\mathcal{O}_{K,\ell}$ is principal, so $\varepsilon T_\ell \cong \mathcal{O}_{K,\ell}$ as an $\mathcal{O}_{K,\ell}$-module.

There are $\mathbb{Z}_\ell$-algebra isomorphisms

$$\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{End}_{\mathcal{O}_B}(T_\ell) \cong \mathrm{End}_{\mathbb{Z}_\ell}(\varepsilon T_\ell) \cong \mathrm{End}_{\mathbb{Z}_\ell}(\mathcal{O}_{K,\ell}).$$

Let $f_0 \in \mathrm{End}_{\mathbb{Z}_\ell}(\mathcal{O}_{K,\ell})$ be defined by $f_0(x) = \overline{x}$. Then

$$\mathrm{End}_{\mathbb{Z}_\ell}(\mathcal{O}_{K,\ell}) = \mathcal{O}_{K,\ell} \oplus \mathcal{O}_{K,\ell} \cdot f_0$$

and $L_\ell(A,\kappa) = \mathcal{O}_{K,\ell} \cdot f_0$, so for any $xf_0 \in L_\ell(A,\kappa)$,

$$\deg^*(xf_0) = -(xf_0)^2 = -xf_0xf_0 = -x\overline{x}f_0^2 = -\mathrm{N}_{K_\ell/\mathbb{Q}_\ell}(x)$$

since $f_0^2 = 1$. Therefore the map $\mathcal{O}_{K,\ell} \to L_\ell(A,\kappa)$ given by $x \mapsto xf_0$ defines an $\mathcal{O}_{K,\ell}$-linear isomorphism of quadratic spaces

$$(\mathcal{O}_{K,\ell}, -\mathrm{N}_{K_\ell/\mathbb{Q}_\ell}) \to (L_\ell(A,\kappa), \deg^*).$$

Now suppose $\ell \mid d_B$. Viewing K as a $\mathbb{Q}$-subalgebra of $B^{(p)}$ via κ, there is a decomposition

$$B_\ell^{(p)} = K_\ell \oplus K_\ell \cdot f_0$$

for any $f_0 \in V_\ell(A,\kappa)$. Choosing f_0 to be an $\mathcal{O}_{K,\ell}$-generator of $L_\ell(A,\kappa)$, the map $x \mapsto xf_0$ defines an isomorphism of quadratic spaces

$$(\mathcal{O}_{K,\ell}, \beta_\ell \cdot \mathrm{N}_{K_\ell/\mathbb{Q}_\ell}) \to (L_\ell(A,\kappa), \deg^*)$$

with $\beta_\ell = -f_0^2 = \deg^*(f_0)$. Then from

$$B_\ell^{(p)} \cong \left(\frac{d_K, -\beta_\ell}{\mathbb{Q}_\ell}\right)$$

we have $(d_K, -\beta_\ell)_\ell = -1$ as $\ell \mid \mathrm{disc}(B^{(p)})$.

In the proof of Proposition 7.1.2 we saw that $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathcal{O}_{B,\ell}$ is the unique maximal order in $B_\ell^{(p)}$ and the quadratic form $\deg^*$ on $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ corresponds to the quadratic form Nrd on $\mathcal{O}_{B,\ell}$, so $f \in B_\ell^{(p)}$ is in $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ if and only if $\deg^*(f) \in \mathbb{Z}_\ell$. As $(d_K, -\beta_\ell)_\ell = -1$, the element $-\beta_\ell \in \mathbb{Z}_\ell$ is not a norm from $\mathbb{Q}_\ell(\sqrt{d_K}) \cong K_\ell$, which means $\mathrm{ord}_\ell(-\beta_\ell) = \mathrm{ord}_\ell(\beta_\ell)$ is odd (since $K_\ell/\mathbb{Q}_\ell$ is unramified). If $\mathrm{ord}_\ell(\beta_\ell) \geqslant 3$ then $\deg^*(\ell^{-1}f_0) \in \mathbb{Z}_\ell$ since $\deg^*(\ell) = \ell^2$, so $\ell^{-1}f_0 \in L_\ell(A,\kappa)$. But f_0 is an $\mathcal{O}_{K,\ell}$-module generator of $L_\ell(A,\kappa)$, so this is a contradiction and hence $\mathrm{ord}_\ell(\beta_\ell) = 1$. □

Proposition 10.2.2. *There is an $\mathcal{O}_{K,p}$-linear isomorphism of quadratic spaces*

$$(\mathcal{O}_{K,p}, \beta_p \cdot \mathrm{N}_{K_p/\mathbb{Q}_p}) \cong (L_p(A,\kappa), \deg^*)$$

for some $\beta_p \in \mathbb{Z}_p$ satisfying $\mathrm{ord}_p(\beta_p) = 2 - e_p\varepsilon_p$.

Proof. There is an $\mathcal{O}_{K,p}$-linear isomorphism of quadratic spaces

$$(\mathcal{O}_{K,p}, \beta_p \cdot \mathrm{N}_{K_p/\mathbb{Q}_p}) \to (L_p(A,\kappa), \deg^*)$$

given by $x \mapsto xf_0$, where f_0 is an $\mathcal{O}_{K,p}$-module generator of $L_p(A,\kappa)$ and $\beta_p = \deg^*(f_0)$. First suppose $p \nmid d_B$. Then

$$B_p^{(p)} \cong \left(\frac{d_K, -\beta_p}{\mathbb{Q}_p}\right)$$

implies $(d_K, -\beta_p)_p = -1$, and $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \Delta$ is the unique maximal order in $B_p^{(p)}$. Suppose p is unramified in K, so $\mathrm{ord}_p(\beta_p)$ is odd. If $\mathrm{ord}_p(\beta_p) \geqslant 3$ then $\deg^*(p^{-1}f_0) \in \mathbb{Z}_p$, which means $p^{-1}f_0 \in L_p(A,\kappa)$. This is a contradiction, so $\mathrm{ord}_p(\beta_p) = 1$. Next suppose p is ramified in K and let $\pi \in \mathcal{O}_{K,p}$ be a uniformizer. If $\mathrm{ord}_p(\beta_p) > 0$ then $\deg^*(\pi^{-1}f_0) \in \mathbb{Z}_p$ as $\mathrm{N}_{K_p/\mathbb{Q}_p}(\pi)$ is a uniformizer of $\mathbb{Z}_p$. Again this implies $\pi^{-1}f_0 \in L_p(A,\kappa)$, which is a contradiction, so $\mathrm{ord}_p(\beta_p) = 0$.

Now suppose $p \mid d_B$, so $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong R_{11}$, with

$$R_{11} = \left\{ \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix} : x, y \in \mathcal{O}_{K,p} \right\},$$

where $\Pi \in \Delta$ is a uniformizer satisfying $\Pi x = \overline{x}\Pi$ for all $x \in \mathcal{O}_{K,p}$, and $\kappa : \mathcal{O}_{K,p} \to R_{11}$ is given by $\kappa(x) = \mathrm{diag}(x,x)$. It follows that $L_p(A,\kappa) = \mathcal{O}_{K,p} \cdot f_0$, where

$$f_0 = \begin{bmatrix} 0 & \Pi \\ p\Pi & 0 \end{bmatrix}.$$

Since $\beta_p = \deg^*(f_0) = -p^2$ (Proposition 7.2.2), we have $\mathrm{ord}_p(\beta_p) = 2$. □

10.3 Counting geometric points

Define two algebraic groups T and T^1 over $\mathbb{Q}$ whose functors of points are given by

$$\begin{aligned} T(R) &= (K \otimes_{\mathbb{Q}} R)^{\times} \\ T^1(R) &= \{x \in T(R) : \mathrm{N}_{K/\mathbb{Q}}(x) = 1\} \end{aligned}$$

for any $\mathbb{Q}$-algebra R. Define a homomorphism $\eta : T \to T^1$ given on points by $\eta(x) = \overline{x}^{-1}x$. Let $U = \widehat{\mathcal{O}}_K^{\times} \subset T(\mathbb{A}_f) = \widehat{K}^{\times}$, so $U = \prod_{\ell} U_{\ell}$ for some groups $U_{\ell} \subset T(\mathbb{Q}_{\ell})$, and let $V = \eta(U)$. If R is a field of characteristic 0 or $\mathbb{A}_f$, then the sequence

$$1 \to R^{\times} \to T(R) \xrightarrow{\eta} T^1(R) \to 1 \tag{10.3.1}$$

is exact, so in particular there is an isomorphism of groups

$$T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U \cong T^1(\mathbb{Q})\backslash T^1(\mathbb{A}_f)/V. \tag{10.3.2}$$

Also, there is an isomorphism of groups

$$T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U \to \mathrm{Cl}(\mathcal{O}_K) \tag{10.3.3}$$

given by

$$t \mapsto \prod_{\mathfrak{p} \subset \mathcal{O}_K} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(t_{\mathfrak{p}})}.$$

Let p be a prime that is nonsplit in K, let $\mathfrak{p} \subset \mathcal{O}_K$ be the prime over p, and let $(A, \kappa) \in \mathscr{Y}(\overline{\mathbb{F}}_{\mathfrak{p}})$. Recall that K acts on $V(A, \kappa)$ by $x \cdot f = \kappa(x) \circ f$. By restriction, the group $T^1(\mathbb{Q}) \subset K^{\times}$ acts on $V(A, \kappa)$, and for any $m \in \mathbb{Q}^{\times}$, the set

$$\{f \in V(A, \kappa) : \deg^*(f) = m\}$$

is either empty or a simply transitive $T^1(\mathbb{Q})$-set. By composing with the homomorphism $\eta : T \to T^1$, the group $T(\mathbb{Q})$ acts on $V(A, \kappa)$, and this action is given by

$$t \bullet f = \kappa(t) \circ f \circ \kappa(t)^{-1}.$$

Now fix $t \in \mathbb{A}_f$ and let $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_K)$ be its image under (10.3.3). We will write $\mathfrak{a} \otimes A$ for the false elliptic curve $\mathfrak{a} \otimes_{\mathcal{O}_K} A$. There is an $\mathcal{O}_K$-linear quasi-isogeny

$$f \in \operatorname{Hom}_{\mathcal{O}_B}(A, \mathfrak{a} \otimes A) \otimes_{\mathbb{Z}} \mathbb{Q},$$

given on points by $f(x) = 1 \otimes x$. Then the map

$$\operatorname{End}^0_{\mathcal{O}_B}(\mathfrak{a} \otimes A) \to \operatorname{End}^0_{\mathcal{O}_B}(A)$$

given by $\varphi \mapsto f^{-1} \circ \varphi \circ f$ is an isomorphism of K-vector spaces, and restricting gives an isomorphism $V(\mathfrak{a} \otimes A, \kappa) \to V(A, \kappa)$. This map identifies $\operatorname{End}_{\mathcal{O}_B}(\mathfrak{a} \otimes A)$ with the $\mathcal{O}_K$-submodule

$$\kappa(\mathfrak{a}) \circ \operatorname{End}_{\mathcal{O}_B}(A) \circ \kappa(\mathfrak{a}^{-1}) \subset \operatorname{End}^0_{\mathcal{O}_B}(A)$$

and identifies $L(\mathfrak{a} \otimes A, \kappa)$ with $\kappa(\mathfrak{a}) \circ L(A, \kappa) \circ \kappa(\mathfrak{a}^{-1})$. Therefore there is a $\widehat{K}$-linear isomorphism

$$\widehat{V}(A, \kappa) \cong \widehat{V}(\mathfrak{a} \otimes A, \kappa)$$

with $\widehat{L}(\mathfrak{a} \otimes A, \kappa)$ isomorphic to the $\widehat{\mathcal{O}}_K$-submodule

$$t \bullet \widehat{L}(A, \kappa) = \{\kappa(t) \circ f \circ \kappa(t)^{-1} : f \in \widehat{L}(A, \kappa)\}$$

of $\widehat{V}(A, \kappa)$.

Definition 10.3.1. Let $(A, \kappa) \in \mathscr{Y}(\overline{\mathbb{F}}_{\mathfrak{p}})$. For each prime number ℓ and $m \in \mathbb{Q}^\times$, define the *orbital integral* at ℓ by

$$O_\ell(m, A, \kappa) = \sum_{t \in \mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell} \mathbf{1}_{L_\ell(A,\kappa)}(t^{-1} \bullet f)$$

if there is an $f \in V_\ell(A, \kappa)$ satisfying $\deg^*(f) = m$. If no such f exists, set $O_\ell(m, A, \kappa) = 0$.

This definition does not depend on the choice of $f \in V_\ell(A, \kappa)$ such that $\deg^*(f) = m$ since $T(\mathbb{Q}_\ell)$ acts simply transitively on the set of all such f.

Proposition 10.3.2. *Let p be a prime nonsplit in K, let $\mathfrak{p} \subset \mathcal{O}_K$ be the prime over p, and suppose $(A, \kappa) \in \mathscr{Y}(\overline{\mathbb{F}}_{\mathfrak{p}})$. For any $m \in \mathbb{Q}^\times$ positive,*

$$\sum_{\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_K)} \#\{f \in L(\mathfrak{a} \otimes A, \kappa) : \deg^*(f) = m\} = \frac{|\mathcal{O}_K^\times|}{2} \prod_\ell O_\ell(m, A, \kappa).$$

Proof. Using the isomorphisms (10.3.3) and (10.3.2), we have

$$\begin{aligned}
\sum_{\mathfrak{a}\in \mathrm{Cl}(\mathcal{O}_K)} \#\{f \in L(\mathfrak{a}\otimes A, \kappa) : \deg^*(f) = m\} \\
&= \sum_{\mathfrak{a}\in \mathrm{Cl}(\mathcal{O}_K)} \sum_{\substack{f\in V(\mathfrak{a}\otimes A,\kappa)\\ \deg^*(f)=m}} \mathbf{1}_{\widehat{L}(\mathfrak{a}\otimes A,\kappa)}(f)\\
&= \sum_{t\in T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U} \sum_{\substack{f\in V(A,\kappa)\\ \deg^*(f)=m}} \mathbf{1}_{t\bullet\widehat{L}(A,\kappa)}(f)\\
&= \sum_{t\in T^1(\mathbb{Q})\backslash T^1(\mathbb{A}_f)/V} \sum_{\substack{f\in V(A,\kappa)\\ \deg^*(f)=m}} \mathbf{1}_{t\bullet\widehat{L}(A,\kappa)}(f).
\end{aligned}$$

Suppose there is an $f_0 \in V(A,\kappa)$ such that $\deg^*(f) = m$. Since the action of $T^1(\mathbb{Q})$ on the set of all such f_0 is simply transitive,

$$\begin{aligned}
\sum_{t\in T^1(\mathbb{Q})\backslash T^1(\mathbb{A}_f)/V} \sum_{\substack{f\in V(A,\kappa)\\ \deg^*(f)=m}} \mathbf{1}_{t\bullet\widehat{L}(A,\kappa)}(f) &= \sum_{t\in T^1(\mathbb{Q})\backslash T^1(\mathbb{A}_f)/V} \sum_{\gamma\in T^1(\mathbb{Q})} \mathbf{1}_{t\bullet\widehat{L}(A,\kappa)}(\gamma^{-1}\bullet f_0)\\
&= \sum_{t\in T^1(\mathbb{Q})\backslash T^1(\mathbb{A}_f)/V} \sum_{\gamma\in T^1(\mathbb{Q})} \mathbf{1}_{\gamma t\bullet\widehat{L}(A,\kappa)}(f_0)\\
&= |T^1(\mathbb{Q})\cap V| \sum_{t\in T^1(\mathbb{A}_f)/V} \mathbf{1}_{t\bullet\widehat{L}(A,\kappa)}(f_0)\\
&= \frac{|\mathcal{O}_K^\times|}{2}\prod_\ell O_\ell(m,A,\kappa),
\end{aligned}$$

where we are using

$$T^1(\mathbb{Q})\cap V \cong (T(\mathbb{Q})\cap U)/\{\pm 1\} = \mathcal{O}_K^\times/\{\pm 1\}$$

and the isomorphism

$$\mathbb{Q}_\ell^\times\backslash T(\mathbb{Q}_\ell)/U_\ell \cong T^1(\mathbb{Q}_\ell)/V_\ell$$

coming from the exact sequence (10.3.1). If there is no such f_0 then by the Hasse-Minkowski theorem there is some prime $\ell < \infty$ such that $(V_\ell(A,\kappa), \deg^*)$ does not represent m ($V_\infty(A,\kappa)$ does represent m). Thus $O_\ell(m,A,\kappa) = 0$ and both sides of the stated equality are 0. □

Proposition 10.3.3. *If (A,κ) is any object of $\mathscr{Y}(\overline{\mathbb{F}}_\mathfrak{p})$ and m is a positive integer, then*

$$\#[\mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{p})] = 2^r\prod_\ell O_\ell(m,A,\kappa),$$

where r is the number of primes dividing d_B.

Proof. The group $\mathrm{Aut}(A,\kappa)$ acts on the set $L(A,\kappa)$ by

$$g \cdot f = g^{-1} \circ f \circ g$$

for $g \in \mathrm{Aut}(A,\kappa)$ and $f \in L(A,\kappa)$. Under this action the stabilizer of f is

$$\mathrm{Stab}(f) = \{g \in \mathrm{Aut}(A,\kappa) : g^{-1} \circ f \circ g = f\} = \mathrm{Aut}(A,\kappa,f).$$

Since $\mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_K}(A) \cong \mathcal{O}_K$, we have $\mathrm{Aut}(A,\kappa) \cong \mathcal{O}_K^\times$, so an element of $\mathrm{Aut}(A,\kappa,f)$ is $\kappa(x)$ for some $x \in \mathcal{O}_K^\times$ satisfying $\kappa(x) \circ f = f \circ \kappa(x)$. But f is a special endomorphism, which means $\kappa(x) = \kappa(\overline{x})$ and thus $x \in \{\pm 1\}$. This shows $\mathrm{Aut}(A,\kappa,f) = \{\pm 1\}$ for $f \in L(A,\kappa)$.

As the group $W_0 \times \mathrm{Cl}(\mathcal{O}_K)$ acts simply transitively on the set $[\mathscr{Y}(\mathbb{F}_\mathfrak{p})]$,

$$\begin{aligned}\#[\mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{p})] &= \sum_{(A,\kappa) \in [\mathscr{Y}(\overline{\mathbb{F}}_\mathfrak{p})]} \sum_{\substack{f \in V(A,\kappa) \\ \deg^*(f) = m}} \frac{|\mathrm{Stab}(f)|}{|\mathrm{Aut}(A,\kappa)|} \cdot \mathbf{1}_{\widehat{L}(A,\kappa)}(f) \\ &= \frac{2}{|\mathcal{O}_K^\times|} \sum_{g \in W_0 \times \mathrm{Cl}(\mathcal{O}_K)} \sum_{\substack{f \in V(g \cdot A,\kappa) \\ \deg^*(f) = m}} \mathbf{1}_{\widehat{L}(g \cdot A,\kappa)}(f).\end{aligned}$$

But the action of W_0 on $[\mathscr{Y}(\overline{\mathbb{F}}_\mathfrak{p})]$ does not change the underlying false elliptic curve or the CM action, so $V(w \cdot A,\kappa) \cong V(A,\kappa)$ for any $w \in W_0$, and therefore

$$\begin{aligned}\#[\mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{p})] &= \frac{2|W_0|}{|\mathcal{O}_K^\times|} \sum_{\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_K)} \sum_{\substack{f \in V(\mathfrak{a} \otimes A,\kappa) \\ \deg^*(f) = m}} \mathbf{1}_{\widehat{L}(\mathfrak{a} \otimes A,\kappa)}(f) \\ &= 2^r \prod_\ell O_\ell(m,A,\kappa)\end{aligned}$$

by Proposition 10.3.2. □

Recall the definitions of the functions R and R_ℓ from the introduction.

Proposition 10.3.4. *Let ℓ be a prime, m a positive integer, and $(A,\kappa) \in \mathscr{Y}(\overline{\mathbb{F}}_\mathfrak{p})$. If the quadratic space $(V_\ell(A,\kappa), \deg^*)$ represents m, then*

$$O_\ell(m,A,\kappa) = e_\ell R_\ell(m d_B^{-1} p^{(e_p - 1)\varepsilon_p - 1}).$$

Proof. Fix an $f \in V_\ell(A,\kappa)$ satisfying $\deg^*(f) = m$ and fix an isomorphism

$$(\mathcal{O}_{K,\ell}, \beta_\ell \cdot \mathrm{N}_{K_\ell/\mathbb{Q}_\ell}) \cong (L_\ell(A,\kappa), \deg^*)$$

with β_ℓ as in Propositions 10.2.1 and 10.2.2. Using the isomorphism

$$\mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell \cong T^1(\mathbb{Q}_\ell)/V_\ell$$

we have

$$O_\ell(m,A,\kappa) = \sum_{t \in T^1(\mathbb{Q}_\ell)/V_\ell} \mathbf{1}_{\mathcal{O}_{K,\ell}}(t^{-1}f).$$

First suppose ℓ is inert in K. Then $\mathbb{Q}_\ell^\times \backslash K_\ell^\times / U_\ell = \{1\}$, so $T^1(\mathbb{Q}_\ell)/V_\ell = \{1\}$. Hence

$$O_\ell(m,A,\kappa) = \mathbf{1}_{\mathcal{O}_{K,\ell}}(f) = R_\ell(m\beta_\ell^{-1})$$

since $\mathrm{N}_{K_\ell/\mathbb{Q}_\ell}(f) = m\beta_\ell^{-1}$. Next suppose ℓ is ramified in K and let $\pi \in \mathcal{O}_{K,\ell}$ be a uniformizer. Then $\mathbb{Q}_\ell^\times \backslash K_\ell^\times / U_\ell = \{1, \pi\}$ and $T^1(\mathbb{Q}_\ell)/V_\ell = \{1, u\}$ where $u = \overline{\pi}^{-1}\pi \in \mathcal{O}_{K,\ell}^\times$, so

$$O_\ell(m,A,\kappa) = \mathbf{1}_{\mathcal{O}_{K,\ell}}(f) + \mathbf{1}_{\mathcal{O}_{K,\ell}}(u^{-1}f) = 2R_\ell(m\beta_\ell^{-1}).$$

Finally suppose ℓ is split in K, so $K_\ell \cong \mathbb{Q}_\ell \times \mathbb{Q}_\ell$. Then

$$\mathbb{Q}_\ell^\times \backslash K_\ell^\times / U_\ell = \{(\ell^k, 0) : k \in \mathbb{Z}\}$$

and $T^1(\mathbb{Q}_\ell)/V_\ell = \{(\ell^k, \ell^{-k}) : k \in \mathbb{Z}\}$. Writing $f = (f_1, f_2) \in \mathbb{Q}_\ell \times \mathbb{Q}_\ell$, we have

$$\begin{aligned} O_\ell(m,A,\kappa) &= \sum_{k \in \mathbb{Z}} \mathbf{1}_{\mathbb{Z}_\ell \times \mathbb{Z}_\ell}(\ell^k f_1, \ell^{-k} f_2) \\ &= 1 + \mathrm{ord}_\ell(f_1) + \mathrm{ord}_\ell(f_2) \\ &= 1 + \mathrm{ord}_\ell(f_1 f_2) \\ &= 1 + \mathrm{ord}_\ell(m\beta_\ell^{-1}) \\ &= R_\ell(m\beta_\ell^{-1}). \end{aligned}$$

□

Theorem 10.3.5. *Let m be a positive integer. If $\mathrm{Diff}_B(m) = \{p\}$ then*

$$\#[\mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{p})] = 2^{r+s} R(m d_B^{-1} p^{(e_p - 1)\varepsilon_p - 1}),$$

where $\mathfrak{p} \subset \mathcal{O}_K$ is the unique prime over p. Furthermore, the number $\#[\mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{p})]$ is nonzero.

Proof. Let $(A, \kappa) \in \mathscr{Y}(\overline{\mathbb{F}}_\mathfrak{p})$, so $\mathrm{End}^0_{\mathcal{O}_B}(A) \cong B^{(p)}$. From $\mathrm{Diff}_B(m) = \{p\}$ we have

$$(d_K, -m)_\ell = \begin{cases} -1 & \text{if } \ell \mid \mathrm{disc}(B^{(p)}) \\ 1 & \text{if } \ell \nmid \mathrm{disc}(B^{(p)}), \end{cases}$$

so there is an isomorphism

$$B^{(p)} \cong \left(\frac{d_K, -m}{\mathbb{Q}} \right).$$

Hence $B^{(p)}$ has a $\mathbb{Q}$-basis $\{1, \delta, f, \delta f\}$ satisfying

$$\delta^2 = d_K, \quad f^2 = -m, \quad \delta f = -f\delta.$$

Embed K into $B^{(p)}$ via $\sqrt{d_K} \mapsto \delta$. Then $\{f, \delta f\}$ is a $\mathbb{Q}$-basis for $V(A, \kappa) \subset \mathrm{End}^0_{\mathcal{O}_B}(A)$ and $\mathrm{Nrd}(f) = m$. Thus, there is an $f \in V(A, \kappa)$ satisfying $\deg^*(f) = m$. Then by Propositions 10.3.3 and 10.3.4,

$$\begin{aligned} \#[\mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{p})] &= 2^r \prod_\ell O_\ell(m, A, \kappa) \\ &= 2^r \prod_\ell e_\ell R_\ell(m d_B^{-1} p^{(e_p - 1)\varepsilon_p - 1}) \\ &= 2^{r+s} R(m d_B^{-1} p^{(e_p - 1)\varepsilon_p - 1}). \end{aligned}$$

Now we will show that this number is nonzero by showing $R_\ell = R_\ell(m d_B^{-1} p^{(e_p-1)\varepsilon_p - 1})$ is nonzero for each prime ℓ. First suppose $\ell \neq p$. If $\ell \nmid d_B$ then $(d_K, -m)_\ell = 1$, which means $-m \in \mathrm{N}_{K_\ell/\mathbb{Q}_\ell}(K_\ell)$ and thus $R_\ell = R_\ell(m) > 0$. If $\ell \mid d_B$ then $(d_K, -m)_\ell = -1$, so $-m \notin \mathrm{N}_{K_\ell/\mathbb{Q}_\ell}(K_\ell)$. As $K_\ell/\mathbb{Q}_\ell$ is unramified, this is equivalent to $\mathrm{ord}_\ell(m)$ being odd and hence $m\ell^{-1} \in \mathrm{N}_{K_\ell/\mathbb{Q}_\ell}(K_\ell)$, so $R_\ell = R_\ell(m\ell^{-1}) > 0$. Finally we consider $\ell = p$. If $p \nmid d_B$ then $(d_K, -m)_p = -1$, so $-m \notin \mathrm{N}_{K_p/\mathbb{Q}_p}(K_p)$. If $K_p/\mathbb{Q}_p$ is unramified then $mp^{-1} \in \mathrm{N}_{K_p/\mathbb{Q}_p}(K_p)$ and thus $R_p = R_p(mp^{-1}) > 0$. If $K_p/\mathbb{Q}_p$ is ramified and $\pi \in \mathcal{O}_{K,p}$ is a uniformizer, then $\mathrm{N}(\pi^k \mathcal{O}_{K,p}) = m\mathbb{Z}_p$ where $k = \mathrm{ord}_p(m)$, so $R_p = R_p(m) > 0$. If $p \mid d_B$ then $(d_K, -m)_p = 1$, which implies $\mathrm{ord}_p(m)$ is even and therefore $R_p = R_p(mp^{-2}) > 0$. □

10.4 Deformation theory

Let p be a prime nonsplit in K and let $\mathfrak{p} \subset \mathcal{O}_K$ be the prime over p. Let $\mathscr{W}$ be the ring of integers in the completion of the maximal unramified extension of $K_\mathfrak{p}$, so $\mathscr{W}$ is an $\mathcal{O}_K$-algebra. Let **CLN** be the category of complete local Noetherian $\mathscr{W}$-algebras with residue field $\overline{\mathbb{F}}_\mathfrak{p}$, where a morphism $R \to R'$ is a local ring homomorphism inducing the identity $\overline{\mathbb{F}}_\mathfrak{p} \to \overline{\mathbb{F}}_\mathfrak{p}$ on residue fields.

For $x = (A, i, \kappa) \in \mathscr{Y}(\overline{\mathbb{F}}_{\mathfrak{p}})$ define a functor $\mathrm{Def}_{\mathcal{O}_B}(A, \mathcal{O}_K) : \mathbf{CLN} \to \mathbf{Sets}$ by assigning to each $R \in \mathbf{CLN}$ the set of isomorphism classes of deformations of x to R. Just as in Corollary 5.1.3, $\mathrm{Def}_{\mathcal{O}_B}(A, \mathcal{O}_K)$ is represented by $\mathscr{W}$. Also, there is an isomorphism $A \cong M \otimes_{\mathcal{O}_K} E$ for some $\mathcal{O}_B \otimes_{\mathbb{Z}} \mathcal{O}_K$-module M and some supersingular CM elliptic curve E over $\overline{\mathbb{F}}_{\mathfrak{p}}$, and if we define a functor $\mathrm{Def}(E, \mathcal{O}_K) : \mathbf{CLN} \to \mathbf{Sets}$ in the obvious way, there is an isomorphism of functors $\mathrm{Def}_{\mathcal{O}_B}(A, \mathcal{O}_K) \cong \mathrm{Def}(E, \mathcal{O}_K)$. For $(A, i, \kappa) \in \mathscr{Y}(\overline{\mathbb{F}}_{\mathfrak{p}})$ and $f \in \mathrm{End}_{\mathcal{O}_B}(A)$, define a functor $\mathrm{Def}(A, \kappa, f) : \mathbf{CLN} \to \mathbf{Sets}$ by assigning to each R the set of isomorphism classes of deformations of (A, i, κ, f) to R. If $R \in \mathbf{CLN}$, $(A, \kappa, f) \in \mathscr{Y}^m(\overline{\mathbb{F}}_{\mathfrak{p}})$, and $(\widetilde{A}, \widetilde{\kappa}, \widetilde{f})$ is a deformation of (A, κ, f) to R, then me must have $(\widetilde{A}, \widetilde{\kappa}, \widetilde{f}) \in \mathscr{Y}^m(R)$. To see this, consider the following two commutative diagrams

$$\begin{tikzcd}
\widetilde{A} \otimes_R \overline{\mathbb{F}}_{\mathfrak{p}} \arrow[r, "\widetilde{f} \otimes \mathrm{id}"] \arrow[d, "\cong"'] & \widetilde{A} \otimes_R \overline{\mathbb{F}}_{\mathfrak{p}} \arrow[d, "\cong"] \\
A \arrow[r, "f"] & A
\end{tikzcd}
\qquad
\begin{tikzcd}
\widetilde{A} \otimes_R \overline{\mathbb{F}}_{\mathfrak{p}} \arrow[r, "\widetilde{\kappa}(x) \otimes \mathrm{id}"] \arrow[d, "\cong"'] & \widetilde{A} \otimes_R \overline{\mathbb{F}}_{\mathfrak{p}} \arrow[d, "\cong"] \\
A \arrow[r, "\kappa(x)"] & A.
\end{tikzcd}$$

It follows from the first diagram that $\deg^*(\widetilde{f}) = \deg^*(f)$ and combining the two diagrams with the fact that f is a special endomorphism implies $\widetilde{f}$ is a special endomorphism.

Now fix a positive integer m and a triple $(A, \kappa, f) \in \mathscr{Y}^m(\overline{\mathbb{F}}_{\mathfrak{p}})$.

Proposition 10.4.1. *If $p \nmid d_B$ and p is inert in K, then the functor* $\mathrm{Def}(A, \kappa, f)$ *is represented by a local Artinian $\mathscr{W}$-algebra of length* $\frac{1}{2}(\mathrm{ord}_p(m) + 1)$.

Proof. Since $p \nmid d_B$ there is an isomorphism of $\mathbb{Z}_p$-algebras $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \Delta$. Let $\mathcal{O}_L \cong \mathbb{Z}_{p^2}$ be the image of $\kappa : \mathcal{O}_{K,p} \to \Delta$. Fix a uniformizer $\Pi \in \Delta$ satisfying $\Pi u = u^{\iota}\Pi$ for all $u \in \mathcal{O}_L \subset \Delta$, so there is a decomposition of left $\mathcal{O}_L$-modules $\Delta = \mathcal{O}_L \oplus \mathcal{O}_L\Pi$. It follows that $L_p(A, \kappa) = \mathcal{O}_L\Pi$, so for any integer $n \geqslant 1$,

$$\begin{aligned}
f \in \mathcal{O}_L + p^{n-1}\Delta &\iff f \in p^{n-1}\mathcal{O}_L\Pi \\
&\iff \mathrm{ord}_p(\deg^*(f)) \geqslant 2n - 1 \\
&\iff \tfrac{1}{2}(\mathrm{ord}_p(m) + 1) \geqslant n,
\end{aligned}$$

where we are using that $f \in L_p(A, \kappa)$.

As p is inert in K, $\mathscr{W} = W$. The functor $\mathrm{Def}(A, \kappa, f)$ is represented by $W_n = W/(p^n)$ where n is the largest integer such that $f \in \mathrm{End}_{\mathcal{O}_B}(A[p^\infty]) \cong \mathrm{End}(\mathfrak{g})$ lifts to an element of $\mathrm{End}_{W_n}(\mathfrak{G} \otimes_W W_n)$, where $\mathfrak{G}$ is the universal deformation of $\mathfrak{g}$ with its $\mathcal{O}_L$-action to W. By (8.1.1),

$$\mathrm{End}_{W_n}(\mathfrak{G} \otimes_W W_n) \cong \mathcal{O}_L + p^{n-1}\Delta,$$

so the result follows from the above calculation. □

Proposition 10.4.2. *If $p \mid d_B$ then $\mathrm{Def}(A,\kappa,f)$ is represented by a local Artinian $\mathscr{W}$-algebra of length $\frac{1}{2}\mathrm{ord}_p(m)$.*

Proof. Fix a uniformizer $\Pi \in \Delta$ satisfying $\Pi u = u^\iota \Pi$ for all $u \in \mathcal{O}_L \subset \Delta$, where $\mathcal{O}_L$ is the image of the CM action $\mathcal{O}_{K,p} \to \Delta$ on the elliptic curve E such that $A \cong M \otimes_{\mathcal{O}_K} E$. Then there is an isomorphism of $\mathbb{Z}_p$-algebras $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong R$, where

$$R = \left\{ \begin{bmatrix} x & y\Pi \\ py\Pi & x \end{bmatrix} : x, y \in \mathcal{O}_L \right\},$$

so there is a decomposition of left $\mathcal{O}_L$-modules $R = \mathcal{O}_L \oplus \mathcal{O}_L P$, with the first factor embedded diagonally and

$$P = \begin{bmatrix} 0 & \Pi \\ p\Pi & 0 \end{bmatrix}.$$

It follows that $L_p(A,\kappa) = \mathcal{O}_L P$ and hence for any integer $n \geqslant 1$,

$$\begin{aligned} f \in \mathcal{O}_L + p^{n-1}R &\iff f \in p^{n-1}\mathcal{O}_L P \\ &\iff \mathrm{ord}_p(\deg^*(f)) \geqslant 2n \\ &\iff \tfrac{1}{2}\mathrm{ord}_p(m) \geqslant n. \end{aligned}$$

The functor $\mathrm{Def}(A,\kappa,f)$ is represented by $W_n = W/(p^n)$ where n is the largest integer such that $f \in \mathrm{End}_{\mathcal{O}_B}(A[p^\infty]) \cong R$ lifts to an element of $\mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W_n}(\widetilde{A}[p^\infty] \otimes_W W_n)$, where $\widetilde{A}$ is the universal deformation of (A, i, κ) to W. By Lemma 8.2.2,

$$\mathrm{End}_{\mathcal{O}_B \otimes_{\mathbb{Z}} W_n}(\widetilde{A}[p^\infty] \otimes_W W_n) \cong \mathcal{O}_L + p^{n-1}R,$$

so the result follows from the above calculation. □

Proposition 10.4.3. *If $p \nmid d_B$ and p is ramified in K, then $\mathrm{Def}(A,\kappa,f)$ is represented by a local Artinian $\mathscr{W}$-algebra of length $\mathrm{ord}_p(m) + 1$.*

Proof. There is an isomorphism of $\mathbb{Z}_p$-algebras $\mathrm{End}_{\mathcal{O}_B}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \Delta$. Let $\mathcal{O}_L$ be the image of $\kappa : \mathcal{O}_{K,p} \to \Delta$. If $\pi \in \mathcal{O}_{K,p}$ is a uniformizer then $\Pi = \kappa(\pi)$ is a uniformizer of $\mathcal{O}_L$ and of Δ. From Proposition 10.2.2 there is an $\mathcal{O}_{K,p}$-linear isomorphism

$$(\mathcal{O}_{K,p}, \beta_p \cdot \mathrm{N}_{K_p/\mathbb{Q}_p}) \cong (L_p(A,\kappa), \deg^*)$$

with $\beta_p \in \mathbb{Z}_p^\times$, so by $\mathcal{O}_{K,p}$-linearity this isomorphism sends $\pi^n \mathcal{O}_{K,p}$ isomorphically to $\Pi^n L_p(A,\kappa)$. Viewing f both as an element of $L_p(A,\kappa) \subset \Delta$ and as an element of $\mathcal{O}_{K,p}$, we have

$$\begin{aligned} v_\Delta(f) &= \mathrm{ord}_\pi(f) \\ &= \mathrm{ord}_p(\mathrm{N}_{K_p/\mathbb{Q}_p}(f)) \\ &= \mathrm{ord}_p(\beta_p \mathrm{N}_{K_p/\mathbb{Q}_p}(f)) \\ &= \mathrm{ord}_p(m). \end{aligned}$$

There is a decomposition of left $\mathcal{O}_L$-modules $\Delta = \mathcal{O}_L \oplus L_p(A,\kappa)$, so for any integer $n \geqslant 1$,

$$\begin{aligned} f \in \mathcal{O}_L + \Pi^{n-1}\Delta &\iff f \in \Pi^{n-1} L_p(A,\kappa) \\ &\iff v_\Delta(f) \geqslant n-1 \\ &\iff \mathrm{ord}_p(m) + 1 \geqslant n. \end{aligned}$$

The functor $\mathrm{Def}(A,\kappa,f)$ is represented by $\mathscr{W}_n = \mathscr{W}/(\pi^n)$ where n is the largest integer such that $f \in \mathrm{End}_{\mathcal{O}_B}(A[p^\infty]) \cong \mathrm{End}(\mathfrak{g})$ lifts to an element of

$$\mathrm{End}_{\mathscr{W}_n}(\mathfrak{G} \otimes_{\mathscr{W}} \mathscr{W}_n) \cong \mathcal{O}_L + \Pi^{n-1}\Delta,$$

where $\mathfrak{G}$ is the universal deformation of $\mathfrak{g}$ with its $\mathcal{O}_L$-action to $\mathscr{W}$. The result now follows from the above calculation. □

10.5 Final formula

Theorem 10.5.1. *Suppose p is a prime nonsplit in K, let $\mathfrak{p} \subset \mathcal{O}_K$ be the prime over p, and let $m \in \mathbb{Z}^+$. For any $y \in \mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{p})$, the strictly Henselian local ring $\mathscr{O}^{\mathrm{sh}}_{\mathscr{Y}^m,y}$ is Artinian of length*

$$e_p \cdot \frac{\mathrm{ord}_p(m) + \varepsilon_p}{2}.$$

Proof. Using the same argument as in the proof of Theorem 8.3.1, the functor $\mathrm{Def}(A,\kappa,f)$ is represented by the ring $\widehat{\mathscr{O}}^{\mathrm{sh}}_{\mathscr{Y}^m,y}$, where $y = (A,\kappa,f) \in \mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{p})$, so the result follows from Propositions 10.4.1, 10.4.2, 10.4.3. □

Theorem 10.5.2. *Let $m \in \mathbb{Z}^+$ and suppose* $\mathrm{Diff}_B(m) = \{p\}$. *Then*

$$\deg(\mathscr{Y}^m) = 2^{r+s}\log(p) \cdot R(md_B^{-1}p^{(e_p-1)\varepsilon_p - 1}) \cdot (\mathrm{ord}_p(m) + \varepsilon_p).$$

If $\#\operatorname{Diff}_B(m) > 1$ *then* $\deg(\mathscr{Y}^m) = 0$.

Proof. Let $\mathfrak{p} \subset \mathcal{O}_K$ be the prime over p. Since $\mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{q}) = \varnothing$ for all primes $\mathfrak{q} \neq \mathfrak{p}$, for any $y \in \mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{p})$ we have

$$\begin{aligned}\deg(\mathscr{Y}^m) &= \log(|\mathbb{F}_\mathfrak{p}|) \cdot \#[\mathscr{Y}^m(\overline{\mathbb{F}}_\mathfrak{p})] \cdot \operatorname{length}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{Y}^m,y}) \\ &= f_p \cdot \log(p) \cdot 2^{r+s} R(md_B^{-1} p^{(e_p-1)\varepsilon_p - 1}) \cdot e_p \frac{\operatorname{ord}_p(m) + \varepsilon_p}{2} \\ &= 2^{r+s} \log(p) \cdot R(md_B^{-1} p^{(e_p-1)\varepsilon_p - 1}) \cdot (\operatorname{ord}_p(m) + \varepsilon_p)\end{aligned}$$

by Theorems 10.3.5 and 10.5.1. If $\#\operatorname{Diff}_B(m) > 1$ then $\mathscr{Y}^m = \varnothing$. □

Appendix A

Hecke correspondences

In this section we will define the Hecke correspondences T_m on $\mathscr{M}$ and $\mathscr{M}^B$, and prove the equalities (1.1.2) and (1.2.2) in the introduction (we continue with the same notation as in Sections 1.1 and 1.2 of the introduction). We begin by reviewing some intersection theory. For any ring R we write $\mathrm{length}(R)$ for $\mathrm{length}_R(R)$. Suppose X is a Noetherian scheme and $Z \subset X$ is a closed subscheme of codimension 1. Let $Z_1, \ldots, Z_n$ be the irreducible components of Z that are of codimension 1 in X. Set $m_i = \mathrm{length}(\mathscr{O}_{Z,\eta_i})$ where $\eta_i \in Z_i$ is the generic point. There is a divisor $[Z] \in \mathrm{Div}(X)$ associated with Z, defined as

$$[Z] = \sum_{i=1}^{n} m_i Z_i.$$

In particular, $[Z] = Z$ if Z is integral. Now suppose $\mathscr{X}$ is a Noetherian stack and $\mathscr{Z}$ is a closed substack of codimension 1. Using an atlas on $\mathscr{X}$, the previous definition for schemes can be extended to stacks to give a divisor $[\mathscr{Z}] \in \mathrm{Div}(\mathscr{X})$ (see [27, Definition 3.5]). Suppose $h : \mathscr{X} \to \mathscr{X}'$ is a morphism of Noetherian stacks of the same dimension. In the case of h finite and flat there is an induced group homomorphism

$$h^* : \mathrm{Div}(\mathscr{X}') \to \mathrm{Div}(\mathscr{X})$$

defined on prime divisors by $h^*\mathscr{D} = [\mathscr{D} \times_{\mathscr{X}'} \mathscr{X}]$ and extended linearly to all of $\mathrm{Div}(\mathscr{X}')$. If h is proper and representable, there is a notion of the image of h, which is a closed substack of $\mathscr{X}'$, defined through an atlas and the scheme-theoretic image (see [27, Definition 1.7]). For h finite, flat, and representable, this leads to a group homomorphism

$$h_* : \mathrm{Div}(\mathscr{X}) \to \mathrm{Div}(\mathscr{X}')$$

defined by sending a prime divisor $\mathscr{D}$ to $\deg(\mathscr{D}/\mathscr{D}') \cdot [\mathscr{D}']$, where $\mathscr{D}'$ is the image of $\mathscr{D}$ under h and $\deg(\mathscr{D}/\mathscr{D}')$ is the degree of the morphism $\mathscr{D} \to \mathscr{D}'$ (see [27, Definition 3.6]).

Fix a positive integer m. Let $\mathscr{M}(m)$ be the category fibered in groupoids over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{M}(m)(S)$ the category of triples (E_1, E_2, φ) with E_i an object of $\mathscr{M}(S)$ and $\varphi \in \mathrm{Hom}_S(E_1, E_2)$ satisfying $\deg(\varphi) = m$ on every connected component of S. The category $\mathscr{M}(m)$ is a stack, flat of relative dimension 1 over $\mathrm{Spec}(\mathcal{O}_K)$, and there are two finite flat morphisms

$$\begin{tikzcd}\mathscr{M}(m) \arrow[r, shift left, "\pi_1"] \arrow[r, shift right, "\pi_2"'] & \mathscr{M}\end{tikzcd}$$

given by $\pi_i(E_1, E_2, \varphi) = E_i$. Define the m-th Hecke correspondence

$$T_m : \mathrm{Div}(\mathscr{M}) \to \mathrm{Div}(\mathscr{M})$$

by $T_m = (\pi_2)_* \circ (\pi_1)^*$.

For $i \in \{1, 2\}$ let $f_i : \mathscr{C}_i \to \mathscr{M}$ be the finite morphism defined by forgetting the complex multiplication structure. Consider the fiber product $\mathscr{D}_1 = \mathscr{C}_1 \times_{f_1, \mathscr{M}, \pi_1} \mathscr{M}(m)$. An object of $\mathscr{D}_1$ is a tuple $(E, E_1, E_2, \varphi, \psi)$, where E is an object of $\mathscr{C}_1$, (E_1, E_2, φ) is an object of $\mathscr{M}(m)$, and $\psi : E \to E_1$ is an isomorphism of elliptic curves. Up to the obvious isomorphism of stacks, the objects of $\mathscr{D}_1$ can be described as triples (E_1, E_2, φ) with E_1 an object of $\mathscr{C}_1$, E_2 an object of $\mathscr{M}$, and $\varphi : E_1 \to E_2$ a degree m isogeny. Now let g be the composition $\mathscr{D}_1 \to \mathscr{M}(m) \xrightarrow{\pi_2} \mathscr{M}$. The fiber product $\mathscr{X} = \mathscr{D}_1 \times_{g, \mathscr{M}, f_2} \mathscr{C}_2$ has objects $(E_1, E_2, E, \varphi, \psi)$ with E_1 an object of $\mathscr{C}_1$, E an object of $\mathscr{C}_2$, $\varphi : E_1 \to E_2$ a degree m isogeny, and $\psi : E_2 \to E$ an isomorphism of elliptic curves. It follows that there is an isomorphism of stacks $\mathscr{X} \cong \mathscr{T}_m$, with $\mathscr{T}_m$ as in the introduction. Below is a diagram of these spaces and morphisms:

$$\begin{tikzcd}
 & & \mathscr{X} \arrow[dl] \arrow[dr] & \\
 & \mathscr{D}_1 \arrow[dl] \arrow[dr] \arrow[ddrr, bend left, "g"] & & \mathscr{C}_2 \arrow[dd, "f_2"] \\
\mathscr{C}_1 \arrow[dr, "f_1"'] & & \mathscr{M}(m) \arrow[dl, "\pi_1"] \arrow[dr, "\pi_2"'] & \\
 & \mathscr{M} & & \mathscr{M}.
\end{tikzcd} \tag{A.0.1}$$

Viewing $\mathscr{D}_1$ as a closed substack of $\mathscr{M}(m)$ through the image of $\mathscr{D}_1 \to \mathscr{M}(m)$, the divisor $T_m\mathscr{C}_1$ on

$\mathscr{M}$ is $(\pi_2)_*[\mathscr{D}_1]$, so to prove $\deg(\mathscr{T}_m) = I(T_m\mathscr{C}_1, \mathscr{C}_2)$, we need to show

$$\deg(\mathscr{D}_1 \times_{g,\mathscr{M},f_2} \mathscr{C}_2) = I((\pi_2)_*[\mathscr{D}_1], [\mathscr{C}_2]), \tag{A.0.2}$$

where we are writing $[\mathscr{C}_2]$ for the divisor on $\mathscr{M}$ determined by the image of f_2.

Let $k = \overline{\mathbb{F}}_{\mathfrak{P}}$ for $\mathfrak{P} \subset \mathcal{O}_K$ a prime ideal and let $x \in \mathscr{M}(k)$ be a geometric point. For any two prime divisors $\mathscr{X}$ and $\mathscr{X}'$ on $\mathscr{M}$ intersecting properly, define the *Serre intersection multiplicity* at x by

$$I_x^{\mathscr{M}}(\mathscr{X}, \mathscr{X}') = \sum_{i \geqslant 0} (-1)^i \operatorname{length}_{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M},x}} \operatorname{Tor}_i^{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M},x}}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{X},x}, \mathscr{O}^{\mathrm{sh}}_{\mathscr{X}',x})$$

if $x \in (\mathscr{X} \cap \mathscr{X}')(k)$ and set $I_x^{\mathscr{M}}(\mathscr{X}, \mathscr{X}') = 0$ otherwise. Extend this definition bilinearly to all divisors on $\mathscr{M}$. Again, if $\mathscr{X}$ and $\mathscr{X}'$ are prime divisors on $\mathscr{M}$ intersecting properly, there is a way of defining a 0-cycle $\mathscr{X} \cdot \mathscr{X}'$ on $\mathscr{M}$ in such a way that

$$\operatorname{Coef}_x(\mathscr{X} \cdot \mathscr{X}') = I_x^{\mathscr{M}}(\mathscr{X}, \mathscr{X}'),$$

where $\operatorname{Coef}_x(\mathscr{X} \cdot \mathscr{X}')$ is the coefficient in the 0-cycle $\mathscr{X} \cdot \mathscr{X}'$ of the 0-dimensional closed substack determined by the image of $x : \operatorname{Spec}(k) \to \mathscr{M}$ (see [25, Chapter V] and [26, Chapter I]).

With notation as in (A.0.1), let $\mathscr{D}_2 = \mathscr{M}(m) \times_{\pi_2,\mathscr{M},f_2} \mathscr{C}_2$, so $[\mathscr{D}_2] = (\pi_2)^*[\mathscr{C}_2]$. Also, let $x \in \mathscr{M}(m)(k)$ be a geometric point with $x = (E_1, E_2, \varphi)$ where E_i is an object of $\mathscr{C}_i$. We claim

$$\operatorname{Tor}_i^{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M}(m),x}}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_1,x}, \mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_2,x}) = 0 \tag{A.0.3}$$

for all $i > 0$. To prove this, first consider the stack $\mathscr{D}_1' = \mathscr{C}_1 \times_{f_1,\mathscr{M},\pi_2} \mathscr{M}(m)$. This category has objects (E_1, E_2, φ) with E_1 an object of $\mathscr{M}$, E_2 an object of $\mathscr{C}_1$, and $\varphi : E_1 \to E_2$ a degree m isogeny. It follows that there is an isomorphism of stacks $\mathscr{D}_1' \cong \mathscr{D}_1$ and

$$\mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_1,x} \cong \mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_1',x} \cong \mathscr{O}^{\mathrm{sh}}_{\mathscr{M}(m),x} \otimes_{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M},\pi_2(x)}} \mathscr{O}^{\mathrm{sh}}_{\mathscr{C}_1,\pi_1(x)}.$$

We already have

$$\mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_2,x} \cong \mathscr{O}^{\mathrm{sh}}_{\mathscr{M}(m),x} \otimes_{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M},\pi_2(x)}} \mathscr{O}^{\mathrm{sh}}_{\mathscr{C}_2,\pi_2(x)},$$

so from π_2 being flat,

$$\operatorname{Tor}_i^{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M}(m),x}}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_1,x}, \mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_2,x}) \cong \mathscr{O}^{\mathrm{sh}}_{\mathscr{M}(m),x} \otimes_{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M},\pi_2(x)}} \operatorname{Tor}_i^{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M},\pi_2(x)}}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{C}_1,\pi_1(x)}, \mathscr{O}^{\mathrm{sh}}_{\mathscr{C}_2,\pi_2(x)}).$$

As $\mathscr{O}^{\mathrm{sh}}_{\mathscr{M},\pi_2(x)}$ and $\mathscr{O}^{\mathrm{sh}}_{\mathscr{C}_i,\pi_i(x)}$ are regular local rings of dimension 2 and 1, respectively, $\mathscr{O}^{\mathrm{sh}}_{\mathscr{C}_i,\pi_i(x)}$ is a

Cohen-Macaulay $\mathscr{O}^{\mathrm{sh}}_{\mathscr{M},\pi_2(x)}$-module, and thus (A.0.3) holds for all $i > 0$ by [25, p. 111].

There is a projection formula

$$((\pi_2)_*[\mathscr{D}_1]) \cdot [\mathscr{C}_2] = (\pi_2)_*([\mathscr{D}_1] \cdot ((\pi_2)^*[\mathscr{C}_2])),$$

where the $(\pi_2)_*$ on the right side is the induced homomorphism on the group of 0-cycles. This is a special case of a more general formula, but it takes this form in our case since (A.0.3) holds (our situation is complicated by $\mathscr{M}(m)$ not necessarily being regular; see [25, p. 118, formulas (10), (11)]). It follows that for any $y \in \mathscr{M}(k)$,

$$\begin{aligned} I_y^{\mathscr{M}}((\pi_2)_*[\mathscr{D}_1], [\mathscr{C}_2]) &= \mathrm{Coef}_y\big(((\pi_2)_*[\mathscr{D}_1]) \cdot [\mathscr{C}_2]\big) \\ &= \mathrm{Coef}_y\big((\pi_2)_*([\mathscr{D}_1] \cdot ((\pi_2)^*[\mathscr{C}_2]))\big) \\ &= \sum_{x \in \pi_2^{-1}(\{y\})} \mathrm{Coef}_x\big([\mathscr{D}_1] \cdot ((\pi_2)^*[\mathscr{C}_2])\big) \\ &= \sum_{x \in \pi_2^{-1}(\{y\})} I_x^{\mathscr{M}(m)}([\mathscr{D}_1], [\mathscr{D}_2]). \end{aligned}$$

Letting $h_i : \mathscr{D}_i \to \mathscr{M}(m)$ be the natural projection, there is an isomorphism of stacks

$$\mathscr{D}_1 \times_{h_1, \mathscr{M}(m), h_2} \mathscr{D}_2 = \mathscr{D}_1 \times_{h_1, \mathscr{M}(m), h_2} (\mathscr{M}(m) \times_{\pi_2, \mathscr{M}, f_2} \mathscr{C}_2) \cong \mathscr{D}_1 \times_{g, \mathscr{M}, f_2} \mathscr{C}_2.$$

Also, by (A.0.3) we have

$$\begin{aligned} I_x^{\mathscr{M}(m)}([\mathscr{D}_1], [\mathscr{D}_2]) &= \mathrm{length}_{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M}(m),x}}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_1,x} \otimes_{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M}(m),x}} \mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_2,x}) \\ &= \mathrm{length}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_1,x} \otimes_{\mathscr{O}^{\mathrm{sh}}_{\mathscr{M}(m),x}} \mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_2,x}). \end{aligned}$$

Note that there is no distinction here between length of a ring over itself and length as a module over $\mathscr{O}^{\mathrm{sh}}_{\mathscr{M}(m),x}$ or $\mathscr{O}^{\mathrm{sh}}_{\mathscr{M},\pi_2(x)}$ because these rings have residue field k which is algebraically closed. Therefore, for any $y \in \mathscr{M}(k)$,

$$\begin{aligned} \sum_{x \in \pi_2^{-1}(\{y\})} \mathrm{length}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_1 \times_{g,\mathscr{M},f_2} \mathscr{C}_2, x}) &= \sum_{x \in \pi_2^{-1}(\{y\})} \mathrm{length}(\mathscr{O}^{\mathrm{sh}}_{\mathscr{D}_1 \times_{h_1,\mathscr{M}(m),h_2} \mathscr{D}_2, x}) \\ &= \sum_{x \in \pi_2^{-1}(\{y\})} I_x^{\mathscr{M}(m)}([\mathscr{D}_1], [\mathscr{D}_2]) \\ &= I_y^{\mathscr{M}}((\pi_2)_*[\mathscr{D}_1], [\mathscr{C}_2]). \end{aligned}$$

Since $\mathscr{C}_2$ is regular and the local ring at y of any prime divisor appearing in $(\pi_2)_*[\mathscr{D}_1]$ is a 1-dimensional domain, hence Cohen-Macaulay, the Tor_i terms appearing in the sum $I_y^{\mathscr{M}}((\pi_2)_*[\mathscr{D}_1],[\mathscr{C}_2])$ are zero for all $i>0$. Multiplying both sides of the above equality by $\log(|\mathbb{F}_{\mathfrak{P}}|)/|\operatorname{Aut}(y)|$ and summing over all y and over all $\mathfrak{P}$ then gives the equality (A.0.2).

Now we move to the false elliptic curve case. Fix a positive integer m. Let $\mathscr{M}^B(m)$ be the category fibered in groupoids over $\mathrm{Spec}(\mathcal{O}_K)$ with $\mathscr{M}^B(m)(S)$ the category of triples (A_1, A_2, φ) with A_i an object of $\mathscr{M}^B(S)$ and $\varphi \in \mathrm{Hom}_{\mathcal{O}_B}(A_1, A_2)$ satisfying $\deg^*(\varphi) = m$ on every connected component of S. The category $\mathscr{M}^B(m)$ is a stack, flat of relative dimension 1 over $\mathrm{Spec}(\mathcal{O}_K)$, and there are two finite flat morphisms

$$\begin{tikzcd}\mathscr{M}^B(m) \arrow[r, shift left, "\pi_1"] \arrow[r, shift right, "\pi_2"'] & \mathscr{M}^B\end{tikzcd}$$

given by $\pi_i(A_1, A_2, \varphi) = A_i$. Define the m-th Hecke correspondence

$$T_m : \mathrm{Div}(\mathscr{M}^B) \to \mathrm{Div}(\mathscr{M}^B)$$

by $T_m = (\pi_2)_* \circ (\pi_1)^*$. The proof of the equality (1.2.2) in the introduction is exactly the same as the proof of (1.1.2) we just gave because all we used were formal properties of the stacks $\mathscr{M}, \mathscr{M}(m), \mathscr{C}_1$, and $\mathscr{C}_2$, and the corresponding stacks $\mathscr{M}^B, \mathscr{M}^B(m), \mathscr{Y}_1$, and $\mathscr{Y}_2$ have these same properties.

Bibliography

[1] Artin, M. *Néron models.* In *Arithmetic Geometry*, G. Cornell and J. Silverman, eds., Springer-Verlag, New York, 1986, pp. 213-230.

[2] Birkenhake, C. and Lange, H. *Complex Abelian Varieties*, Springer-Verlag, Berlin, 2004, volume 302 of *Grundlehren der Mathematischen Wissenschaften* [Fundamental Principles of Mathematical Sciences].

[3] Boutot, J. F. and Carayol, H. *Uniformisation p-adique des courbes de Shimura; les théorèmes de Čerednik et de Drinfeld.* Astérisque **196-197** (1991), pp. 45-158.

[4] Buzzard, K. *Integral models of certain Shimura curves.* Duke Math Journal, Vol. 87, No. 3, 1997.

[5] Chai, C.-L., Conrad, B., and Oort, F. *Complex Multiplication and Lifting Problems*, American Mathematical Society, 2014. Mathematical Surveys and Monographs, Vol. 195.

[6] Clark, P. *Rational points on Atkin-Lehner quotients of Shimura curves*, Ph.D. Thesis, Harvard, 2003.

[7] Conrad, B. *Gross-Zagier revisited.* In *Heegner points and Rankin L-series*, volume 49 of Math. Sci. Res. Inst. Publ., pp. 67-163. Cambridge Univ. Press, Cambridge, 2004. With an appendix by W. R. Mann.

[8] Goren, E. and Lauter, K. *A Gross-Zagier formula for quaternion algebras over totally real fields.* Algebra and Number Theory, Vol. 7, No. 6, 2013.

[9] Görtz, U. and Wedhorn, T. *Algebraic Geometry I: Schemes with Examples and Exercises*, Vieweg + Teubner Verlag, 2010.

[10] Gross, B. *On canonical and quasicanonical liftings.* Invent. Math., **84** (1986), part 2, pp. 321-326.

[11] Gross, B. and Zagier, D. *On singular moduli.* J. Reine Angew. Math., **355** (1985), pp. 191-220.

[12] Howard, B. *Complex multiplication cycles and Kudla-Rapoport divisors II.* Preprint, to appear in Amer. J. Math.

[13] Howard, B. and Yang, T. *Intersections of Hirzebruch-Zagier divisors and CM cycles*, Springer-Verlag, Berlin, 2011. Lecture Notes in Mathematics, Vol. 2041.

[14] Howard, B. and Yang, T. *Singular moduli refined.* In *Arithmetic Geometry and Automorphic Forms*, volume 19 of *Advanced Lectures in Mathematics*, pp. 367-406. Higher Education Press, Beijing, 2011.

[15] Jordan, B.W. *On the Diophantine arithmetic of Shimura curves*, Ph.D. Thesis, Harvard, 1981.

[16] Kudla, S., Rapoport, M., and Yang, T. *On the derivative of an Eisenstein series of weight one.* Int. Math. Res. Not., **7** (1999), pp. 347-385.

[17] Milne, J.S. *Étale Cohomology*, Princeton University Press, Princeton, 1980.

[18] Milne, J.S. *Points on Shimura varieties* mod p. Proc. Symp. Pure Math., **33** (1979), part 2, pp. 165-184.

[19] Mumford, D. *Abelian Varieties*, Tata inst. of fundamental research, Bombay, 1970.

[20] Mumford, D. *Geometric Invariant Theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Neue Folge, Band 34. Springer-Verlag, Berlin, 1965.

[21] Oort, F. *Which abelian surfaces are products of elliptic curves?.* Math. Ann., **214** (1975), pp. 35-74.

[22] Rapoport, M. and Zink, Th. *Period Spaces for p-divisible Groups*, volume 141 of *Annals of Mathematics Studies.* Princeton University Press, Princeton, NJ, 1996.

[23] Reiner, I. *Maximal Orders*, Oxford University Press, New York, 2003.

[24] Ribet, K. *Bimodules and abelian surfaces.* Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, 1989, pp. 359-407.

[25] Serre, J.-P. *Local Algebra*, Springer-Verlag, Berlin, 2000, Springer Monographs in Mathematics.

[26] Soulé, C. *Lectures on Arakelov Geometry*, Cambridge University Press, Cambridge, 1992, volume 33 of Cambridge Studies in Advanced Mathematics. With the collaboration of D. Abramovich, J.-F. Burnol, and J. Kramer.

[27] Vistoli, A. *Intersection theory on algebraic stacks and their moduli spaces.* Invent. Math., **97** (1989), part 3, pp. 613-670.

[28] Wewers, S. *Canonical and quasi-canonical liftings.* Astérisque **312** (2007), pp. 67-86.