SINGULAR MODULI REFINED

BENJAMIN HOWARD AND TONGHAI YANG

1. Introduction

Let K_1 and K_2 be nonisomorphic quadratic imaginary fields with discriminants d_1 and d_2, respectively, and set $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. Let F be the real quadratic subfield of K, set $D = \mathrm{disc}(F)$, and let $\mathfrak{D} \subset \mathcal{O}_F$ be the different of $F/\mathbb{Q}$. Let $x \mapsto \overline{x}$ denote complex conjugation on K and set $\mathbf{w}_i = |\mathcal{O}_{K_i}^\times|$. Let χ be the quadratic Hecke character of F associated to K, and let σ_1 and σ_2 be the two real embeddings of F. Throughout the introduction we assume that $\gcd(d_1, d_2) = 1$. In particular this implies that K/F is unramified.

Almost one hundred years ago, to construct a holomorphic modular form of (parallel) weight 1 for $\mathrm{SL}_2(\mathcal{O}_F)$, Hecke constructed the following famous Eisenstein series

$$E^*(\tau_1, \tau_2, s) = D^{\frac{s+1}{2}} \left(\pi^{-\frac{s+2}{2}} \Gamma\left(\frac{s+2}{2}\right)\right)^2 \sum_{[\mathfrak{a}] \in \mathrm{CL}(F)} \chi(\mathfrak{a}) \, \mathrm{N}(\mathfrak{a})^{1+s}$$
$$\cdot \sum_{(0,0) \neq (m,n) \in \mathfrak{a}^2 / \mathcal{O}_F^\times} \frac{(v_1 v_2)^{\frac{s}{2}}}{(m(\tau_1, \tau_2) + n)|m(\tau_1, \tau_2) + n|^s}.$$

Here $\mathrm{CL}(F)$ is the ideal class group of F, $[\mathfrak{a}]$ denotes the class of the fractional ideal $\mathfrak{a}$, and

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

Hecke showed that this sum, convergent for $\mathrm{Re}(s) \gg 0$, has meromorphic continuation to all s and defines a (non-holomorphic) Hilbert modular form of weight 1 for $\mathrm{SL}_2(\mathcal{O}_F)$ which is holomorphic at $s = 0$. The value $E^*(\tau_1, \tau_2, 0)$ at $s = 0$ is a holomorphic Hilbert modular form of weight 1 (Hecke's trick). He further computed the Fourier expansion of this holomorphic modular form. Unfortunately, he missed a sign in the calculation, and it turns out that $E^*(\tau_1, \tau_2, 0) = 0$ identically. In the early 1980's, Gross and Zagier took advantage of this fact to compute its central derivative at $s = 0$, and found that the Fourier coefficients of the diagonal restriction to the upper half plane are very closely related to the factorization of singular moduli ([3]). Their result can be rephrased (see [19, Section 3] or Corollary 1.5 below for more details) in terms of arithmetic intersections as follows: if $\mathcal{E}$ is the moduli stack of elliptic curves over $\mathbb{Z}$-schemes then the m-th Fourier coefficient of $E^{*,\prime}(\tau, \tau, 0)$ is the arithmetic intersection on $\mathcal{E} \times \mathcal{E}$ of the m-th Hecke correspondence with the codimension two cycle of points representing pairs $(\mathbf{E}_1, \mathbf{E}_2)$ of elliptic

---

Date: June 1, 2009.

2000 *Mathematics Subject Classification.* 11G15, 11F41, 14K22.

The first author is partially supported by NSF grant DMS-0556174, and by a Sloan Foundation Research Fellowship.

The second author is partially supported by grants NSF DMS-0555503 and NSFC-10628103.

curves with complex multiplication by $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$, respectively. One naturally asks, for $\alpha \in F'$ what is the arithmetic meaning of the α-th Fourier coefficient of the central derivative $E^{*,\prime}(\tau_1, \tau_2, 0)$ itself, before one restricts to the diagonal $\tau_1 = \tau_2$? In another word, is there an arithmetic Siegel-Weil formula ([8], [9]) for this Hecke Eisenstein series? The purpose of this paper is to answer this question positively.

Let $\mathcal{X}$ be the algebraic stack over $\mathbb{Z}$ representing the functor which assigns to every scheme S the category $\mathcal{X}(S)$ of pairs $(\mathbf{E}_1, \mathbf{E}_2)$ in which each $\mathbf{E}_i = (E_i, \kappa_i)$ consists of an elliptic curve E_i over S and an action $\kappa_i : \mathcal{O}_{K_i} \to \mathrm{End}(E_i)$. For $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(S)$ let

$$L(\mathbf{E}_1, \mathbf{E}_2) = \mathrm{Hom}(E_1, E_2)$$

be the $\mathbb{Z}$-module of homomorphisms from E_1 to E_2, equipped with the quadratic form deg. Let $[\,,\,]$ be the bilinear form associated to deg. The maximal order

$$\mathcal{O}_K = \mathcal{O}_{K_1} \otimes_{\mathbb{Z}} \mathcal{O}_{K_2}$$

acts on $L(\mathbf{E}_1, \mathbf{E}_2)$ by

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

($t_i \in \mathcal{O}_{K_i}$) making $L(\mathbf{E}_1, \mathbf{E}_2)$ into an $\mathcal{O}_K$-module. The action satisfies

$$[t \bullet \phi_1, \phi_2] = [\phi_1, \bar{t} \bullet \phi_2]$$

for all $t \in \mathcal{O}_K$, and it follows that if we view $L(\mathbf{E}_1, \mathbf{E}_2)$ as an $\mathcal{O}_F$-module then there is a unique $\mathcal{O}_F$-bilinear form

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

satisfying $[\phi_1, \phi_2] = \mathrm{Tr}_{F/\mathbb{Q}}[\phi_1, \phi_2]_{\mathrm{CM}}$. If $\deg_{\mathrm{CM}}$ is the $\mathcal{O}_F$-quadratic form on $L(\mathbf{E}_1, \mathbf{E}_2)$ corresponding to $[\,,\,]_{\mathrm{CM}}$ then

$$\deg(\phi) = \mathrm{Tr}_{F/\mathbb{Q}} \deg_{\mathrm{CM}}(\phi).$$

For any $\alpha \in F^\times$ let $\mathcal{X}_\alpha$ be the algebraic stack representing the functor which assigns to a scheme S the category $\mathcal{X}_\alpha(S)$ of triples $(\mathbf{E}_1, \mathbf{E}_2, j)$ in which $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(S)$ and $\phi \in L(\mathbf{E}_1, \mathbf{E}_2)$ with $\deg_{\mathrm{CM}}(\phi) = \alpha$. It is clear that $\mathcal{X}_\alpha$ is empty unless α is totally postive.

For $\alpha \in F'$ totally positive define the *Arakelov degree*

$$\deg(\mathcal{X}_\alpha) = \sum_p \log(p) \sum_{x \in [\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})]} e_x^{-1} \cdot \mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x})$$

where $[\mathcal{X}_\alpha(S)]$ is the set of isomorphism classes of objects in the category $\mathcal{X}_\alpha(S)$, $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}$ is the strictly Henselian local ring of $\mathcal{X}_\alpha$ at x, and e_x is the order of the automorphism group of the triple $(\mathbf{E}_1, \mathbf{E}_2, \phi)$ corresponding to x. Define $\mathrm{Diff}(\sqrt{D}, \alpha)$ to be the set of finite primes $\mathfrak{p}$ of F satisfying

$$\chi_{\mathfrak{p}}(\alpha\sqrt{D}) = -1.$$

If $\mathfrak{b}$ is a fractional $\mathcal{O}_F$-ideal we define $\rho(\mathfrak{b})$ to be the number of ideals $\mathfrak{B} \subset \mathcal{O}_K$ satisfying $N_{K/F}(\mathfrak{B}) = \mathfrak{b}$. If ℓ is a rational prime we define $\rho_\ell(\mathfrak{b})$ to be the number of ideals $\mathfrak{B} \subset \mathcal{O}_{K,\ell}$ satisfying $N_{K_\ell/F_\ell}(\mathfrak{B}) = \mathfrak{b}_\ell$. Thus

$$\rho(\mathfrak{b}) = \prod_\ell \rho_\ell(\mathfrak{b}). \tag{1.1}$$

For the proof of the following theorem see Section 2.7.

Theorem 1.1. *If $\alpha \in \mathfrak{D}^{-1}$ is totally positive and* $\mathrm{Diff}(\sqrt{D}, \alpha) = \{\mathfrak{p}\}$*, then $\mathcal{X}_\alpha$ has dimension zero, is supported in characteristic $p = \mathbb{Z} \cap \mathfrak{p}$, and satisfies*

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

Otherwise, one has $\mathcal{X}_\alpha = \emptyset$.

The functional equation forces $E^*(\tau_1, \tau_2, 0) = 0$, and the central derivative has a Fourier expansion

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

where $v_i = \mathrm{Im}(\tau_i)$, $e(x) = e^{2\pi i x}$, and $q^\alpha = e(\sigma_1(\alpha)\tau_1 + \sigma_2(\alpha)\tau_2)$.

Theorem 1.2. *Suppose that $\alpha \in F$ is totally positive. If $\alpha \in \mathfrak{D}^{-1}$ and* $\mathrm{Diff}(\sqrt{D}, \alpha) = \{\mathfrak{p}\}$*, then $a_\alpha = a_\alpha(v_1, v_2)$ is independent of v_i, and*

$$a_\alpha = 2 \cdot \mathrm{ord}_\mathfrak{p}(\alpha\mathfrak{p}\mathfrak{D})\rho(\alpha\mathfrak{D}\mathfrak{p}^{-1}) \log p,$$

where p is the rational prime below $\mathfrak{p}$. Otherwise, one has $a_\alpha = 0$.

Theorem 1.2 is stated in a different form in [3], but without proof. We will give a sketch of the proof in Section 3 (Theorem 3.5). Combining the above theorems we obtain the following.

Theorem 1.3. *Assume $\alpha \in F$ is totally positive. Then $\mathcal{X}_\alpha$ is a stack of dimension zero and*

$$4 \cdot \deg(\mathcal{X}_\alpha) = a_\alpha$$

where a_α is the α-th Fourier coefficient of $E^{*,\prime}(\tau_1, \tau_2, 0)$.

In Section 3 we give a slightly different and more conceptional proof of Theorem 1.3, which we now outline. Assume that $\alpha \in F$ is totally positive. In Section 2 we use Gross's work on canonical liftings of supersingular elliptic curves [2] to study the local rings $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}$. These results are summarized in Theorem 3.8, and include the following theorem.

Theorem 1.4. *Fix a prime p and suppose $x \in \mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$. Then* $\mathrm{Diff}(\sqrt{D}, \alpha)$ *consists of a single prime $\mathfrak{p}$ of F, which lies above p. Moreover*

$$\mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}) = \frac{1}{2}\mathrm{ord}_\mathfrak{p}(\alpha\mathfrak{D}\mathfrak{p}).$$

In particular, the length of the strictly Henselian local ring is independent of x.

By this theorem, one sees that when $\mathcal{X}_\alpha$ is not empty $\mathrm{Diff}(\sqrt{D}, \alpha) = \{\mathfrak{p}\}$ consists of a unique prime, and $\mathcal{X}_\alpha$ is supported at the rational prime p below $\mathfrak{p}$. Moreover, the theorem implies

$$\deg(\mathcal{X}_\alpha) = \frac{1}{2} \log p \cdot \mathrm{ord}_\mathfrak{p}(\alpha\mathfrak{D}\mathfrak{p}) \sum_{(\mathbf{E}_1, \mathbf{E}_2) \in [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]} \sum_{\substack{\phi \in L(\mathbf{E}_1, \mathbf{E}_2) \\ \deg_{\mathrm{CM}}(\phi) = \alpha}} \frac{1}{|\mathrm{Aut}(\mathbf{E}_1, \mathbf{E}_2, \phi)|}. \tag{1.2}$$

We can view the Hecke Eisenstein series as a special case of an incoherent Eisenstein in the sense of Kudla [7]. When $\mathrm{Diff}(\sqrt{D}, \alpha) = \{\mathfrak{p}\}$, one can also write a_α as (see Lemma 3.11)

$$a_\alpha = a_\alpha(\mathfrak{p}) b_\alpha(\mathfrak{p})$$

where $a_\alpha(\mathfrak{p})$ is essentially the central derivative of the local Whittaker function at $\mathfrak{p}$, and $b_\alpha(\mathfrak{p})$ is the α-coefficient of a coherent Eisenstein series. Now explicit calculation gives

$$a_\alpha(\mathfrak{p}) = \frac{1}{2}\log p \cdot \mathrm{ord}_\mathfrak{p}(\alpha\mathfrak{D}\mathfrak{p}).$$

On the other hand, the double sum in (1.2) counts the number of ways to represent α by lattices in the genus of $L(\mathbf{E}_1,\mathbf{E}_2)$ in $V(\mathbf{E}_1,\mathbf{E}_2)$. By the Siegel-Weil formula, it is equal to $\frac{1}{4}b_\alpha(\mathfrak{p})$. This proves Theorem 1.3. In our case, both the double sum and $\frac{1}{4}b_\alpha(\mathfrak{p})$ are easy to compute directly and are equal to $\rho(\alpha\mathfrak{D}\mathfrak{p}^{-1})$, thus the explicit formulae in Theorems 1.1 and 1.2 .

By Theorem 1.3, one sees that the generating function

$$\phi(\tau) = \sum_{\substack{\alpha\in\mathfrak{D}^{-1}\\ \alpha\gg 0}} \deg(\mathcal{X}_\alpha)\cdot q^\alpha$$

is the holomorphic part of a (non)-holomorphic Hilbert modular form of weight 1 for $\mathrm{SL}_2(\mathcal{O}_F)$, namely $E^{*,\prime}(\tau_1,\tau_2,0)$. One can also view the theorem as an arithmetic Siegel-Weil formula in the sense of [8] and [9]—giving an arithmetic interpretation of the central derivative of the incoherent Eisenstein series.

We now explain in what sense Theorems 1.1 and 1.3 are refinements of the earlier work of Gross and Zagier on singular moduli. For a positive integer m let $\mathcal{T}_m$ be the algebraic stack representing the functor which assigns to a scheme S the category of all triples $(\mathbf{E}_1,\mathbf{E}_2,\phi)$ where $(\mathbf{E}_1,\mathbf{E}_2)\in\mathcal{X}(S)$ and $\phi\in\mathrm{Hom}(E_1,E_2)$ satisfies $\deg(\phi)=m$. Directly from the moduli problems we have

$$\mathcal{T}_m = \bigsqcup_{\substack{\alpha\in F\\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha)=m}} \mathcal{X}_\alpha.$$

Combining this decomposition with the formula for $\deg(\mathcal{X}_\alpha)$ of Theorem 1.1 one finds (see Corollary 2.45) a formula for $\deg(\mathcal{T}_m)$. This formula is precisely the main result of [3]:

Corollary 1.5 (Gross-Zagier)**.** *For any positive integer m we have*

$$\deg(\mathcal{T}_m) = \frac{1}{2}\sum_{\substack{\alpha\in\mathfrak{D}^{-1}\\ \mathrm{Tr}_{F/\mathbb{Q}}\alpha=m\\ a\gg 0}}\sum_p \log p\sum_{\mathfrak{p}|p}\mathrm{ord}_\mathfrak{p}(\alpha\mathfrak{D}\mathfrak{p})\rho(\alpha\mathfrak{D}\mathfrak{p}^{-1})$$

where the middle summation is over those rational primes p which are nonsplit in both K_1 and K_2. Furthermore, $\deg(\mathcal{T}_m)$ *is equal to the m-Fourier coefficient of* $\frac{1}{4}E^{*,\prime}(\tau,\tau,0)$.

This work grew out of the authors' attempts to understand Gross and Zagier's work on singular moduli from the perspective of Kudla's program [7, 8, 9] to relate arithmetic intersection multiplicities on Shimura varieties of orthogonal and unitary type to the Fourier coefficients of derivatives of Eisenstein series. On the occasion of his sixtieth birthday the authors wish to express to Steve Kudla both their deepest appreciation for his beautiful mathematics, and their deepest gratitude for his influence on their own lives and work.

2. Moduli spaces of CM elliptic curves

Throughout Section 2 we keep the notation of the introduction, but allow the possibility that $\gcd(d_1, d_2) > 1$. For any sets $Y \subset X$ the characteristic function of Y is denoted $\mathbf{1}_Y$.

2.1. **CM pairs.** Let S be a scheme and R an order in a quadratic imaginary field. An *elliptic curve over S with complex multiplication by R* is a pair $\mathbf{E} = (E, \kappa)$ in which $E \to S$ is an elliptic curve and $\kappa : R \to \mathrm{End}(E)$ is an action of R on E.

Definition 2.1. A *CM pair* over a scheme S is a pair $(\mathbf{E}_1, \mathbf{E}_2)$ in which $\mathbf{E}_1$ and $\mathbf{E}_2$ are elliptic curves over S with complex multiplication by $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$, respectively. An *isomorphism* between CM pairs $(\mathbf{E}'_1, \mathbf{E}'_2) \to (\mathbf{E}_1, \mathbf{E}_2)$ is a pair (f_1, f_2) of isomorphisms of underlying elliptic curves

$$f_1 : E'_1 \to E_1 \qquad f_2 : E'_2 \to E_2$$

which are $\mathcal{O}_{K_1}$ and $\mathcal{O}_{K_2}$ linear, respectively.

To understand the moduli space of CM pairs over schemes we use the language of stacks and groupoids as in [14]. Given a CM pair $(\mathbf{E}_1, \mathbf{E}_2)$ over a scheme S and a morphism of schemes $T \to S$ there is an evident notion of the pullback CM pair $(\mathbf{E}_1, \mathbf{E}_2)_{/T}$. Let $\mathcal{X}$ be the category whose objects are CM pairs over schemes. In the category $\mathcal{X}$ an arrow $(\mathbf{E}'_1, \mathbf{E}'_2) \to (\mathbf{E}_1, \mathbf{E}_2)$ between CM pairs defined over schemes T and S, respectively, is a morphism of schemes $T \to S$ together with an isomorphism (in the sense of Definition 2.1) of CM pairs over T

$$(\mathbf{E}'_1, \mathbf{E}'_2) \cong (\mathbf{E}_1, \mathbf{E}_2)_{/T}.$$

Thus $\mathcal{X}$ is a category fibered in groupoids over the category of schemes. For a scheme S the fiber $\mathcal{X}(S)$ is the category of CM pairs over schemes, and arrows in this category are isomorphisms in the sense of Definition 2.1.

Definition 2.2. Suppose k is a field of characteristic $p > 0$. A CM pair $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(k)$ is *supersingular* if the p-divisible groups of the underlying elliptic curves E_1 and E_2 are connected. In other words, the underlying elliptic curves E_1 and E_2 are supersingular in the usual sense.

Suppose S is a scheme. For every CM pair $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(S)$ we abbreviate

$$L(\mathbf{E}_1, \mathbf{E}_2) = \mathrm{Hom}(E_1, E_2)$$

(where the Hom means homomorphisms between elliptic curves over S in the usual sense) and

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

Assuming that S is connected the $\mathbb{Z}$-module $L(\mathbf{E}_1, \mathbf{E}_2)$ is equipped with the positive definite quadratic form $\deg(\phi)$, and we denote by

$$\begin{aligned} [\phi_1, \phi_2] &= \deg(\phi_1 + \phi_2) - \deg(\phi_1) - \deg(\phi_2) \\ &= \phi_1^\vee \circ \phi_2 + \phi_2^\vee \circ \phi_1 \end{aligned}$$

the associated bilinear form. The $\mathbb{Q}$-algebra $K = K_1 \otimes_{\mathbb{Q}} K_2$ acts on the $\mathbb{Q}$-vector space $V(\mathbf{E}_1, \mathbf{E}_2)$ by

$$(x_1 \otimes x_2) \bullet \phi = \kappa_2(x_2) \circ \phi \circ \kappa_1(\overline{x}_1). \tag{2.1}$$

By a *K-Hermitian* form on $V(\mathbf{E}_1,\mathbf{E}_2)$ we mean a function

$$\langle\cdot,\cdot\rangle : V(\mathbf{E}_1,\mathbf{E}_2)\times V(\mathbf{E}_1,\mathbf{E}_2)\to K$$

which is K-linear in the first variable and satisfies $\langle\phi_1,\phi_2\rangle=\overline{\langle\phi_2,\phi_1\rangle}$.

Proposition 2.3.

(1) *There is a unique F-bilinear form $[\phi_1,\phi_2]_{\mathrm{CM}}$ on $V(\mathbf{E}_1,\mathbf{E}_2)$ which satisfies*

$$[\phi_1,\phi_2]=\mathrm{Tr}_{F/\mathbb{Q}}\;[\phi_1,\phi_2]_{\mathrm{CM}}$$

(2) *The F-quadratic form*

$$\deg_{\mathrm{CM}}(\phi)=\frac{1}{2}\cdot[\phi,\phi]_{\mathrm{CM}}$$

is the unique F-quadratic form on $V(\mathbf{E}_1,\mathbf{E}_2)$ which satisfies

$$\deg(\phi)=\mathrm{Tr}_{F/\mathbb{Q}}\;\deg_{\mathrm{CM}}(\phi).$$

(3) *There is a unique K-Hermitian form $\langle\phi_1,\phi_2\rangle_{\mathrm{CM}}$ on $V(\mathbf{E}_1,\mathbf{E}_2)$ which satisfies*

$$[\phi_1,\phi_2]_{\mathrm{CM}}=\mathrm{Tr}_{K/F}\;\langle\phi_1,\phi_2\rangle_{\mathrm{CM}}.$$

Proof. Suppose $\phi_1,\phi_2\in V(\mathbf{E}_1,\mathbf{E}_2)$. If $x=x_1\otimes x_2\in K$ is nonzero then as elements of $\mathrm{End}(E_1)$ we have

$$\begin{aligned}[x\bullet\phi_1,\phi_2] &= \kappa_1(x_1)^{-1}\circ[x\bullet\phi_1,\phi_2]\circ\kappa_1(x_1)\\ &= \phi_1^\vee\circ\kappa_2(\overline{x}_2)\circ\phi_2\circ\kappa_1(x_1)+\kappa_1(\overline{x}_1)\circ\phi_2^\vee\circ\kappa_2(x_2)\circ\phi_1\\ &= [\phi_1,\overline{x}\bullet\phi_2].\end{aligned}$$

Thus for all $x\in K$ we have $[x\bullet\phi_1,\phi_2]=[\phi_1,\overline{x}\bullet\phi_2]$. All of the claims now follow from this property and some elementary linear algebra; in particular from the fact that if M/L is a finite extension of fields then for any finite dimensional M-vector space V the trace $\mathrm{Tr}_{M/L}$ induces an isomorphism $\mathrm{Hom}_M(V,M)\to\mathrm{Hom}_L(V,L)$. □

Thus the complex multiplication structure on $\mathbf{E}_1$ and $\mathbf{E}_2$ endows the set $V(\mathbf{E}_1,\mathbf{E}_2)$ not only with a K-action, but with an F-quadratic form $\deg_{\mathrm{CM}}$ which refines the usual notion of degree. For every $m\in\mathbb{Q}$ define $\mathcal{T}_m$ to be the category, fibered in groupoids over schemes, of triples $(\mathbf{E}_1,\mathbf{E}_2,\phi)$ in which $(\mathbf{E}_1,\mathbf{E}_2)$ is a CM pair over a scheme S and $\phi\in L(\mathbf{E}_1,\mathbf{E}_2)$ satisfies $\deg(\phi)=m$ on every connected component of S. Similarly for every $\alpha\in F$ define $\mathcal{X}_\alpha$ to be the category of triples $(\mathbf{E}_1,\mathbf{E}_2,\phi)$ in which $(\mathbf{E}_1,\mathbf{E}_2)$ is a CM pair over a scheme and $\phi\in L(\mathbf{E}_1,\mathbf{E}_2)$ satisfies $\deg_{\mathrm{CM}}(\phi)=\alpha$ on every connected component of S. The categories $\mathcal{X}$, $\mathcal{T}_m$, and $\mathcal{X}_\alpha$ are algebraic (Deligne-Mumford) stacks, in the sense of [14], of finite type over $\mathrm{Spec}(\mathbb{Z})$ (briefly, one knows that the category $\mathcal{E}$ of elliptic curves over schemes is an algebraic stack of finite type over $\mathrm{Spec}(\mathbb{Z})$, and the relative representability of each of $\mathcal{X}$, $\mathcal{T}_m$, and $\mathcal{X}_\alpha$ over $\mathcal{E}\times_{\mathbb{Z}}\mathcal{E}$ is proved using the methods and results of [5, Chapter 6]). For every $m\in\mathbb{Q}$ there is a decomposition

$$\mathcal{T}_m=\bigsqcup_{\substack{\alpha\in F\\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha)=m}}\mathcal{X}_\alpha. \tag{2.2}$$

Remark 2.4. For the moment let us write $\mathcal{X}(d_1, d_2)$ (respectively $\mathcal{X}_\alpha(d_1, d_2)$) instead of $\mathcal{X}$ (respectively $\mathcal{X}_\alpha$) to emphasize the dependence of $\mathcal{X}$ and $\mathcal{X}_\alpha$ on the quadratic imaginary fields K_1 and K_2. Similarly write F_{d_1,d_2} instead of F. It is clear that the functor $(\mathbf{E}_1, \mathbf{E}_2) \mapsto (\mathbf{E}_2, \mathbf{E}_1)$ defines an isomorphism of stacks $\mathcal{X}(d_1, d_2) \to \mathcal{X}(d_2, d_1)$. If we identify $K_1 \otimes_{\mathbb{Q}} K_2 \cong K_2 \otimes_{\mathbb{Q}} K_1$ using $x \otimes y \mapsto y \otimes x$ then we may identify $F_{d_1,d_2} \cong F \cong F_{d_2,d_1}$, and for any $\alpha \in F$ the functor $(\mathbf{E}_1, \mathbf{E}_2, \phi) \mapsto (\mathbf{E}_2, \mathbf{E}_1, \phi^\vee)$ defines an isomorphism of stacks

$$\mathcal{X}_\alpha(d_1, d_2) \cong \mathcal{X}_\alpha(d_2, d_1).$$

In this sense the stacks $\mathcal{X}$ and $\mathcal{X}_\alpha$ are each symmetric in d_1 and d_2.

If S is a scheme and $\mathcal{C}$ is any one of $\mathcal{X}$, $\mathcal{T}_m$, or $\mathcal{X}_\alpha$ then $[\mathcal{C}(S)]$ denotes the set of isomorphism classes of objects in the category $\mathcal{C}(S)$.

2.2. **The support of $\mathcal{X}_\alpha$.** Given $\alpha \in F^\times$ define a nondegenerate $\mathbb{Q}$-quadratic form Q_α on K by

$$Q_\alpha(x) = \mathrm{Tr}_{F/\mathbb{Q}}(\alpha x \overline{x}).$$

For each place $\ell \leq \infty$ of $\mathbb{Q}$ let $\mathrm{hasse}_\ell(\cdot)$ be the Hasse invariant on $\mathbb{Q}_\ell$-quadratic spaces and let $(\cdot, \cdot)_\ell$ be the usual Hilbert symbol at ℓ. Define the *local invariant* $\mathrm{inv}_\ell(\alpha) = \pm 1$ by

$$\mathrm{inv}_\ell(\alpha) = \mathrm{hasse}_\ell(K_\ell, Q_\alpha) \cdot (-1, -1)_\ell,$$

the *modified local invariant* of α

$$\mathrm{inv}^*_\ell(\alpha) = \begin{cases} \mathrm{inv}_\ell(\alpha) & \text{if } \ell < \infty \\ -\mathrm{inv}_\ell(\alpha) & \text{if } \ell = \infty, \end{cases}$$

and a finite set of places of $\mathbb{Q}$

$$\mathrm{Sppt}(\alpha) = \{\ell \leq \infty \mid \mathrm{inv}^*_\ell(\alpha) = -1\}.$$

Note that the product formula $\prod_{\ell \leq \infty} \mathrm{inv}_\ell(\alpha) = 1$ implies that $\mathrm{Sppt}(\alpha)$ has odd cardinality.

Lemma 2.5. *Suppose that k is an algebraically closed field of nonzero characteristic. If $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(k)$ is supersingular then for some totally positive $\beta \in F^\times$ there is an isomorphism of F-quadratic spaces*

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

Proof. Set $p = \mathrm{char}(k)$. As all supersingular elliptic curves over k, and all of their endomorphisms, are defined over $\mathbb{F}_p^{\mathrm{alg}}$, we may assume that $k = \mathbb{F}_p^{\mathrm{alg}}$. Let $H = \mathrm{End}(E_1) \otimes_{\mathbb{Z}} \mathbb{Q}$ so that H is a quaternion division algebra over $\mathbb{Q}$ of discriminant p. Fix also an isogeny $f : E_1 \to E_2$. Then $\phi \mapsto f^{-1} \circ \phi \circ f$ defines an isomorphism of $\mathbb{Q}$-algebras

$$\mathrm{End}(E_2) \otimes_{\mathbb{Z}} \mathbb{Q} \to H$$

and $\phi \mapsto f \circ \phi$ defines an isomorphism of $\mathbb{Q}$-vector spaces

$$H \to V(\mathbf{E}_1, \mathbf{E}_2).$$

In particular $V(\mathbf{E}_1, \mathbf{E}_2)$ has dimension 4. Suppose first that $d_1 \neq d_2$ so that K is a field. Then the dimension of $V(\mathbf{E}_1, \mathbf{E}_2)$ as a K-vector space is 1, and any isomorphism of K-vector spaces $V(\mathbf{E}_1, \mathbf{E}_2) \cong K$ identifies the Hermitian form $\langle \cdot, \cdot \rangle_{\mathrm{CM}}$ on $V(\mathbf{E}_1, \mathbf{E}_2)$ with a Hermitian form on K. All such Hermitian forms have the form $\langle x, y \rangle = \beta x \overline{y}$ for some $\beta \in F$. As our isomorphism identifies the $\mathbb{Q}$-quadratic form $Q(x) = \mathrm{Tr}_{F/\mathbb{Q}}(\beta x\overline{x})$ on K with the positive definite quadratic form deg on $V(\mathbf{E}_1, \mathbf{E}_2)$, it follows easily that β is totally positive.

Now suppose that $d_1 = d_2$ so that $F \cong \mathbb{Q} \times \mathbb{Q}$ and $K \cong K_1 \times K_2$. Fix an isomorphism $K_1 \cong K_2$, and call this common field K_0. Using the fact that any two embeddings of K_0 into H are conjugate (by the Noether-Skolem theorem), we may adjust the isogeny f in order to assume that f is K_0-linear. Under the identifications chosen above the embeddings

$$\kappa_i : K_0 \to \mathrm{End}(E_i) \otimes_{\mathbb{Z}} \mathbb{Q} \cong H$$

are equal and action of the orthogonal idempotents in $F \cong \mathbb{Q}\times\mathbb{Q}$ on $V(\mathbf{E}_1, \mathbf{E}_2) \cong H$ induces a splitting $H = H^+ \oplus H^-$ in which H^+ is the image of K_0 and

$$H^- = \{b \in H \mid \forall x \in K_0 \; xb = b\overline{x}\}.$$

Each of $H^\pm$ is a one-dimensional K_0-vector space, and it follows that $V(\mathbf{E}_1, \mathbf{E}_2)$ is free of rank one over $K \cong K_0 \otimes_{\mathbb{Q}} K_0 \cong K_0 \times K_0$. After fixing an isomorphism of K-modules $V(\mathbf{E}_1, \mathbf{E}_2) \cong K$, the remainder of the proof is identical to the case of $d_1 \neq d_2$. □

Proposition 2.6. *If k is an algebraically closed field of characteristic $p \geq 0$, $\alpha \in F^\times$, and $(\mathbf{E}_1, \mathbf{E}_2, \phi) \in \mathcal{X}_\alpha(k)$ then*

(1) *$p > 0$ and the CM pair $(\mathbf{E}_1, \mathbf{E}_2)$ is supersingular,*
(2) *p is nonsplit in both K_1 and K_2,*
(3) *there are isomorphisms of quadratic spaces over $\mathbb{Q}$*

$$(K, Q_\alpha) \cong (V(\mathbf{E}_1, \mathbf{E}_2), \deg) \cong (H, \mathrm{Nm})$$

where H is the rational quaternion algebra over $\mathbb{Q}$ of discriminant p and Nm *is the reduced norm on H,*
(4) $\mathrm{Sppt}(\alpha) = \{p\}$.

Proof. Suppose that $p = 0$. As $\phi : E_1 \to E_2$ is a nonzero isogeny, κ_1, κ_2, and ϕ determine isomorphisms

$$K_1 \cong \mathrm{End}(E_1) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathrm{End}(E_2) \otimes_{\mathbb{Z}} \mathbb{Q} \cong K_2 \tag{2.3}$$

which force $d_1 = d_2$. Furthermore there are isomorphisms of $\mathbb{Q}$-vector spaces

$$\mathrm{End}(E_1) \otimes_{\mathbb{Z}} \mathbb{Q} \cong V(\mathbf{E}_1, \mathbf{E}_2) \cong \mathrm{End}(E_2) \otimes_{\mathbb{Z}} \mathbb{Q},$$

and so $V(\mathbf{E}_1, \mathbf{E}_2)$ is 2-dimensional. As $K \cong K_1 \otimes_{\mathbb{Q}} K_2 \cong K_1 \times K_2$ one of the two orthogonal idempotents in $F \cong \mathbb{Q} \times \mathbb{Q}$ must annihilate $V(\mathbf{E}_1, \mathbf{E}_2)$. Assuming for simplicity that it is $(0, 1)$ which annihilates $V(\mathbf{E}_1, \mathbf{E}_2)$, the F-quadratic form $\deg_{\mathrm{CM}}$ is simply $(\deg, 0)$. Of course this contradicts $\deg_{\mathrm{CM}}(\phi) = \alpha \in F^\times$. Thus k has characteristic $p > 0$. The existence of the isogeny ϕ implies that the elliptic curves E_1 and E_2 are either both supersingular of both ordinary. If they are both ordinary then again (2.3) holds and repeating the above argument gives a contradiction. Thus $(\mathbf{E}_1, \mathbf{E}_2)$ is supersingular. In particular

$$\mathrm{End}(E_1) \otimes_{\mathbb{Z}} \mathbb{Q} \cong H \cong \mathrm{End}(E_2) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

As κ_i gives an embedding of K_i into H, it follows immediately that p is nonsplit in K_i.

By Lemma 2.5 there is an isomorphism of F-quadratic spaces

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

for some $\beta \in F^\times$ which is determined precisely up to multiplication by an element of $\mathrm{Nm}_{K/F}(K^\times)$. By hypothesis the quadratic space on the left represents α, and so there is $u \in K^\times$ such that $\alpha = \beta \cdot \mathrm{Nm}_{K/F}(u)$. Thus we have an isomorphism of F-quadratic spaces

$$(V(\mathbf{E}_1, \mathbf{E}_2), \deg_{\mathrm{CM}}) \cong (K, \alpha \cdot \mathrm{Nm}_{K/F})$$

and so also an isomorphism of $\mathbb{Q}$-quadratic spaces

$$(V(\mathbf{E}_1, \mathbf{E}_2), \deg) \cong (K, Q_\alpha).$$

Fix an isomorphism of $\mathbb{Q}$-algebras $H \cong \mathrm{End}(E_1) \otimes_{\mathbb{Z}} \mathbb{Q}$. The function $f \mapsto f^\vee \circ \phi$ defines an isomorphism of $\mathbb{Q}$-quadratic spaces

$$(V(\mathbf{E}_1, \mathbf{E}_2), \deg) \cong (H, b^{-1} \cdot \mathrm{Nm})$$

where $b = \deg(\phi)$. As the reduced norm $H^\times \to \mathbb{Q}^\times$ is surjective there is an isomorphism of $\mathbb{Q}$-quadratic spaces $(H, b \cdot \mathrm{Nm}) \cong (H, \mathrm{Nm})$. It only remains to prove that $\mathrm{Sppt}(\alpha) = \{p\}$. Using the isomorphism $(K, Q_\alpha) \cong (H, \mathrm{Nm})$ already proved we find

$$\mathrm{inv}_\ell(\alpha) = \mathrm{hasse}_\ell(H_\ell, \mathrm{Nm}) \cdot (-1, -1)_\ell.$$

By direct calculation of the Hasse invariant of (H_ℓ, Nm) it follows that

$$\mathrm{inv}_\ell(\alpha) = \begin{cases} -1 & \text{if } \ell = p, \infty \\ 1 & \text{otherwise.} \end{cases}$$

In particular $\mathrm{inv}^*_\ell(\alpha) = -1$ if and only if $\ell = p$. This completes the proof. □

Corollary 2.7. *Suppose $\alpha \in F^\times$ and that $\mathcal{X}_\alpha$ is nonempty. Then α is totally positive.*

Proof. Suppose that $x \in \mathcal{X}_\alpha(k)$ for some algebraically closed field k. By Proposition 2.6 k has characteristic p and x is a supersingular point. By Lemma 2.5 there is a totally positive $\beta \in F^\times$ and a $u \in K$ such that $\alpha = \beta \cdot \mathrm{Nm}_{K/F}(u)$. Thus α is totally positive. □

Corollary 2.8. *Suppose $\alpha \in F^\times$. If $\mathrm{Sppt}(\alpha) = \{p\}$ for a finite prime p then all geometric points of $\mathcal{X}_\alpha$ lie in characteristic p and are supersingular. If $|\mathrm{Sppt}(\alpha)| > 1$ or if $\mathrm{Sppt}(\alpha) = \{\infty\}$ then $\mathcal{X}_\alpha = \emptyset$.*

Proof. This is immediate from Proposition 2.6. □

2.3. **Group actions.** For $i = 1, 2$ define an algebraic group over $\mathbb{Q}$ by $T_i(A) = (K_i \otimes_{\mathbb{Q}} A)^\times$ for any $\mathbb{Q}$-algebra A. Let $\nu_i : T_i \to \mathbb{G}_m$ be norm $\nu_i(t_i) = t_i \bar{t}_i$ and define

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

Define an algebraic group S over $\mathbb{Q}$ by

$$S(A) = \{z \in (K \otimes_{\mathbb{Q}} A)^\times \mid \mathrm{Nm}_{K/F}(z) = 1\}.$$

There is an evident character $\nu : T \to \mathbb{G}_m$ defined by the relations $\nu_1(t_1) = \nu(t) = \nu_2(t_2)$ for $t = (t_1, t_2) \in T(R)$ and a homomorphism $T \to S$ defined by

$$t \mapsto \frac{t_1 \otimes t_2}{\nu(t)}. \tag{2.4}$$

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

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

and let $V \subset S(\mathbb{A}_f)$ be the image of U under $T(\mathbb{A}_f) \to S(\mathbb{A}_f)$.

Proposition 2.9. *If k is a field of characteristic 0, the ring of adeles $\mathbb{A}$, or the ring of finite adeles $\mathbb{A}_f$ then the sequence*

$$1 \to k^\times \to T(k) \to S(k) \to 1$$

is exact, where $k^\times \to T(k)$ is the diagonal inclusion and $T(k) \to S(k)$ is (2.4).

Proof. Suppose first that k is a field of characteristic 0. Fix an algebraic closure k^{alg}/k and embeddings of E_1 and E_2 into k^{alg}. There is then an isomorphism of k^{alg}-algebras

$$E_i \otimes_{\mathbb{Q}} k^{\mathrm{alg}} \cong k^{\mathrm{alg}} \times k^{\mathrm{alg}}$$

defined by $x_i \otimes 1 \mapsto (x_i, \overline{x}_i)$ which we use to identify $T_i(k^{\mathrm{alg}}) \cong \mathbb{G}_m^2(k^{\mathrm{alg}})$. The group $T(k^{\mathrm{alg}})$ is then identified with

$$T(k^{\mathrm{alg}}) \cong \{(x_1, x_2, y_1, y_2) \in (\mathbb{G}_m^2 \times \mathbb{G}_m^2)(k^{\mathrm{alg}}) \mid x_1 x_2 = y_1 y_2\}.$$

Recalling that $K = K_1 \otimes_{\mathbb{Q}} K_2$ we now identify

$$K \otimes_{\mathbb{Q}} k^{\mathrm{alg}} \cong k^{\mathrm{alg}} \times k^{\mathrm{alg}} \times k^{\mathrm{alg}} \times k^{\mathrm{alg}}$$

using the k^{alg}-isomorphism $(x \otimes y) \otimes 1 \mapsto (xy, \overline{xy}, x\overline{y}, \overline{x}y)$. Under this identification

$$S(k^{\mathrm{alg}}) \cong \{(a_1, a_2, b_1, b_2) \in \mathbb{G}_m^4(k^{\mathrm{alg}}) \mid a_1 a_2 = 1 = b_1 b_2\}$$

and the map $T(k^{\mathrm{alg}}) \to S(k^{\mathrm{alg}})$ takes the form

$$(x_1, x_2, y_1, y_2) \mapsto \left(\frac{x_1}{y_2}, \frac{x_2}{y_1}, \frac{y_2}{x_2}, \frac{y_1}{x_1} \right).$$

Using these explicit formulae one easily verifies the exactness of

$$1 \to \mathbb{G}_m(k^{\mathrm{alg}}) \to T(k^{\mathrm{alg}}) \to S(k^{\mathrm{alg}}) \to 1,$$

and the claim follows by taking $\mathrm{Gal}(k^{\mathrm{alg}}/k)$ cohomology and applying Hilbert's Theorem 90.

If $k = \mathbb{A}$ then the proof is essentially the same: first choose a finite Galois extension $M/\mathbb{Q}$ which contains both K_1 and K_2 (e.g. take $M = K$ if $d_1 \neq d_2$) and then, as above, use $E_i \otimes_{\mathbb{Q}} \mathbb{A}_M \cong \mathbb{A}_M \times \mathbb{A}_M$ to prove the exactness of

$$1 \to \mathbb{A}_M^\times \to T(\mathbb{A}_M) \to S(\mathbb{A}_M) \to 1.$$

The adelic form of Hilbert's Theorem 90 [10, Corollary 8.1.3] then proves the exactness of

$$1 \to \mathbb{A}^\times \to T(\mathbb{A}) \to S(\mathbb{A}) \to 1,$$

and the exactness for $k = \mathbb{A}$ implies the exactness for $k = \mathbb{A}_f$. □

Corollary 2.10. *The homomorphism $T \to S$ defined by (2.4) induces an isomorphism*

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

Proof. This is immediate from Proposition 2.9 and the observation $\mathbb{A}_f^\times \subset T(\mathbb{Q})U$. □

Suppose $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(k)$ with k an algebraically closed field. Define an action of $S(\mathbb{Q})$ on $V(\mathbf{E}_1, \mathbf{E}_2)$ by restricting the action (2.1) from $K^\times$ to the subgroup $S(\mathbb{Q})$. The group $T(\mathbb{Q})$ then also acts on $V(\mathbf{E}_1, \mathbf{E}_2)$ via the homomorphism $T \to S$ defined above, and this action is given by the simple formula

$$t \bullet \phi = \kappa_2(t_2) \circ \phi \circ \kappa_1(t_1)^{-1} \tag{2.5}$$

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

Lemma 2.11. *If $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ is supersingular then the above action of $S(\mathbb{Q})$ on $V(\mathbf{E}_1, \mathbf{E}_2)$ identifies $S(\mathbb{Q})$ with the special orthogonal group of the F-quadratic form $\deg_{\mathrm{CM}}$. The same is true if $\mathbb{Q}$ is replaced by $\mathbb{Q}_\ell$, F is replaced by F_ℓ, and $V(\mathbf{E}_1, \mathbf{E}_2)$ is replaced by $V(\mathbf{E}_1, \mathbf{E}_2) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ for any prime ℓ.*

Proof. By Lemma 2.5 it suffices to show that the special orthogonal group of the F-quadratic space $(K, \mathrm{Nm}_{K/F})$ is $S(\mathbb{Q}) = \{x \in K^\times \mid \mathrm{Nm}_{K/F}(x) = 1\}$. This is well-known; for example [6, Corollary V.6.1.3] implies that every orthogonal transformation of $(K, \mathrm{Nm}_{K/F})$ of determinant 1 is K-linear, so is given by multiplication by an element of $S(\mathbb{Q})$. □

For $i = 1, 2$ let $\mathrm{Pic}(\mathcal{O}_{K_i})$ be the ideal class group of K_i and set

$$\Gamma = \mathrm{Pic}(\mathcal{O}_{K_1}) \times \mathrm{Pic}(\mathcal{O}_{K_2}).$$

Using the isomorphism $\mathrm{Pic}(\mathcal{O}_{K_i}) \cong K_i^\times \backslash \widehat{E}_i^\times / \widehat{\mathcal{O}}_{K_i}^\times$ and the canonical injection

$$T(\mathbb{Q}) \backslash T(\mathbb{A}_f) / U \to (K_1^\times \backslash \widehat{E}_1^\times / \widehat{\mathcal{O}}_{K_1}^\times) \times (K_2^\times \backslash \widehat{E}_2^\times / \widehat{\mathcal{O}}_{K_2}^\times)$$

we identify $T(\mathbb{Q}) \backslash T(\mathbb{A}_f) / U$ with a subgroup $\Gamma_0 \subset \Gamma$. To be explicit, Γ_0 is the image of the injection

$$T(\mathbb{Q}) \backslash T(\mathbb{A}_f) / U \to \Gamma \tag{2.6}$$

which sends $(t_1, t_2) \in T(\mathbb{A}_f)$ to the pair of ideal classes $([\mathfrak{a}_1], [\mathfrak{a}_2])$ defined by $\mathfrak{a}_i \widehat{\mathcal{O}}_{K_i} = t_i \widehat{\mathcal{O}}_{K_i}$. For any scheme S the group Γ acts on the set $[\mathcal{X}(S)]$ on the right by Serre's tensor construction [1, Section 7]

$$(\mathbf{E}_1, \mathbf{E}_2) \otimes ([\mathfrak{a}_1], [\mathfrak{a}_2]) = (\mathbf{E}_1 \otimes_{\mathcal{O}_{K_1}} \mathfrak{a}_1, \mathbf{E}_2 \otimes_{\mathcal{O}_{K_2}} \mathfrak{a}_2).$$

Remark 2.12. The classical theory of complex multiplication implies that the action of Γ on $[\mathcal{X}(\mathbb{C})]$ breaks $[\mathcal{X}(\mathbb{C})]$ into a disjoint union of four simply transitive orbits. The orbits are indexed by the set of all ordered pairs (π_1, π_2) in which

$$\pi_1 : K_1 \to \mathbb{C} \qquad \pi_2 : K_2 \to \mathbb{C}$$

are embeddings of fields. The isomorphism class of a CM pair $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(\mathbb{C})$ lies in the orbit indexed by (π_1, π_2) if and only if the action of K_i on the 1-dimensional $\mathbb{C}$-vector space $\mathrm{Lie}(E_i)$ is through π_i for both $i = 1$ and $i = 2$.

Lemma 2.13. *Let k be an algebraically closed field. Every $x \in [\mathcal{X}(k)]$ has trivial stabilizer in Γ and satisfies*

$$\mathrm{Aut}_{\mathcal{X}(k)}(x) \cong \mathcal{O}_{K_1}^\times \times \mathcal{O}_{K_2}^\times.$$

Proof. Suppose we have a pair $([\mathfrak{a}_1, \mathfrak{a}_2]) \in \Gamma$ and a CM pair $(\mathbf{E}_1, \mathbf{E}_2)$ defined over k with the property that

$$(\mathbf{E}_1, \mathbf{E}_2) \cong (\mathbf{E}_1 \otimes_{\mathcal{O}_{K_1}} \mathfrak{a}_1, \mathbf{E}_2 \otimes_{\mathcal{O}_{K_2}} \mathfrak{a}_2).$$

In particular there is an isomorphism of $\mathcal{O}_{K_i}$-modules

$$\mathrm{Hom}_{\mathcal{O}_{K_i}}(E_i, E_i) \cong \mathrm{Hom}_{\mathcal{O}_{K_i}}(E_i, E_i \otimes_{\mathcal{O}_{K_i}} \mathfrak{a}_i)$$

and hence, by [1, Lemma 7.14],

$$\mathrm{End}_{\mathcal{O}_{K_i}}(E_i) \cong \mathrm{End}_{\mathcal{O}_{K_i}}(E_i) \otimes_{\mathcal{O}_{K_i}} \mathfrak{a}_i.$$

Both as a ring and as an $\mathcal{O}_{K_i}$-module $\mathrm{End}_{\mathcal{O}_{K_i}}(E_i) \cong \mathcal{O}_{K_i}$, and so $\mathfrak{a}_i \cong \mathcal{O}_{K_i}$ as an $\mathcal{O}_{K_i}$-module. Thus $\mathfrak{a}_i$ is a principal ideal. The isomorphism $\mathrm{Aut}_{\mathcal{X}(k)}(x) \cong \mathcal{O}_{K_1}^\times \times \mathcal{O}_{K_2}^\times$ is clear from $\mathrm{Aut}_{\mathcal{O}_{K_i}}(E_i) \cong \mathcal{O}_{K_i}^\times$. □

Proposition 2.14. *If* $\gcd(d_1, d_2) = 1$ *then* $\Gamma_0 = \Gamma$.

Proof. For $i = 1, 2$ fix a fractional $\mathcal{O}_{K_i}$-deal $\mathfrak{a}_i$, set $a_i = \mathrm{Nm}_{K_i/\mathbb{Q}}(\mathfrak{a}_i)$, and define a quadratic form on the $\mathbb{Q}$-vector space K_i

$$Q_i(x) = a_i \cdot \mathrm{Nm}_{K_i/\mathbb{Q}}(x).$$

Let W be the $\mathbb{Q}$-vector space $K_1 \oplus K_2$ endowed with the quadratic form

$$Q(x_1, x_2) = Q_1(x_1) - Q_2(x_2).$$

The claim is that (W, Q) represents 0, and by the Hasse-Minkowski theorem it suffices to prove this everywhere locally. As $W \otimes_{\mathbb{Q}} \mathbb{R}$ has signature $(2, 2)$ it clearly represents 0. Fix a prime $\ell < \infty$. The quadratic space W_ℓ has discriminant $d_1 d_2 \in \mathbb{Q}_\ell^\times / (\mathbb{Q}_\ell^\times)^2$ and Hasse invariant

$$(a_1, d_1)_\ell \cdot (a_2, d_2)_\ell \cdot (d_1, -d_2)_\ell \cdot (-1, -1)_\ell.$$

If $d_1 d_2$ is not a square in $\mathbb{Q}_\ell^\times$ then W_ℓ represents 0 by [12, Chapter IV.2.2]. Thus we may assume that $d_1 = d_2$ up to a square in $\mathbb{Q}_\ell^\times$. As a_i is the norm of a fractional ideal in $K_{i,\ell}$ we may factor $a_i = u_i \cdot b_i$ with b_i equal to the norm of some element in $K_\ell^\times$ and $u_i \in \mathbb{Z}_p^\times$. As we assume that $\gcd(d_1, d_2) = 1$, at least one of K_1 and K_2 is unramified at ℓ. Thus u_1 is either a norm from $K_{1,\ell}^\times$ or a norm from $K_{2,\ell}^\times$, and so either $(u_1, d_1)_\ell = 1$ or $(u_1, d_2)_\ell = 1$. But $(u_1, d_1)_\ell = (u_1, d_2)_\ell$ as $d_1 = d_2$ up to a square. Thus we have

$$(a_1, d_1)_\ell = (u_1, d_1)_\ell = 1.$$

The same argument shows that $(a_2, d_2)_\ell = 1$, and as $(d_1, -d_2)_\ell = 1$ is obvious we find that the Hasse invariant of W_ℓ is $(-1, -1)_\ell$. Again by [12, Chapter IV.2.2] the quadratic space W_ℓ represents 0. Having proved that the quadratic space (W, Q) represents 0, we deduce that there is an $m \in \mathbb{Q}^\times$ which is represented both by Q_1 and by Q_2. Choosing $r_i \in K_i^\times$ such that $Q_1(r_1) = Q_2(r_2)$ we see that the fractional ideal $\mathfrak{b}_i = \mathfrak{a}_i r_i$ lies in the same ideal class as $\mathfrak{a}_i$, and that

$$\mathrm{Nm}_{K_1/\mathbb{Q}}(\mathfrak{b}_1) = \mathrm{Nm}_{K_2/\mathbb{Q}}(\mathfrak{b}_2). \tag{2.7}$$

Thus we have proved that every element of Γ has the form $([\mathfrak{b}_1], [\mathfrak{b}_2])$ with $\mathfrak{b}_1$ and $\mathfrak{b}_2$ satisfying (2.7). Now choose $t_i \in \widehat{K}_i^\times$ satisfying

$$t_i \widehat{\mathcal{O}}_{K,i}^\times = \mathfrak{b}_i \widehat{\mathcal{O}}_{K,i}^\times.$$

The relation (2.7) implies that there is a $u \in \widehat{\mathbb{Z}}^\times$ such that

$$\mathrm{Nm}_{K_1/\mathbb{Q}}(t_1) = u \cdot \mathrm{Nm}_{K_2/\mathbb{Q}}(t_2).$$

The hypothesis $\gcd(d_1, d_2) = 1$ implies that

$$\widehat{\mathbb{Z}}^\times = \mathrm{Nm}_{K_1/\mathbb{Q}}(\widehat{\mathcal{O}}_{K_1}^\times) \cdot \mathrm{Nm}_{K_2/\mathbb{Q}}(\widehat{\mathcal{O}}_{K_2}^\times).$$

Factoring u as the product of the norm of some $v_1^{-1} \in \widehat{\mathcal{O}}_{K_1}^\times$ and the norm of some $v_2 \in \widehat{\mathcal{O}}_{K_2}^\times$ we may then replace t_i by $t_i v_i$ so that $(t_1, t_2) \in T(\mathbb{A}_f)$. This proves the surjectivity of (2.6), and completes the proof that $\Gamma_0 = \Gamma$. $\square$

2.4. **Orbital integrals.** Fix a prime p and a supersingular CM pair $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$. For every prime $\ell < \infty$ define

$$\begin{aligned} L_\ell(\mathbf{E}_1, \mathbf{E}_2) &= L(\mathbf{E}_1, \mathbf{E}_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \\ V_\ell(\mathbf{E}_1, \mathbf{E}_2) &= V(\mathbf{E}_1, \mathbf{E}_2) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell. \end{aligned}$$

Given an $\alpha \in F_p^\times$ the *orbital integral* $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2)$ is defined (using the action (2.5) of $T(\mathbb{Q}_\ell)$ on $V_\ell(\mathbf{E}_1, \mathbf{E}_2)$) to be

$$O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \sum_{t \in \mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell} \mathbf{1}_{L_\ell(\mathbf{E}_1, \mathbf{E}_2)}(t^{-1} \bullet \phi) \tag{2.8}$$

if there exists a $\phi \in V_\ell(\mathbf{E}_1, \mathbf{E}_2)$ satisfying $\deg_{\mathrm{CM}}(\phi) = \alpha$. If no such ϕ exists then set $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = 0$.

Lemma 2.15. *The orbital integral $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2)$ is independent of the choice of ϕ used in its definition. Furthermore if $(\mathbf{E}_1', \mathbf{E}_2') \in [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]$ lies in the same Γ_0-orbit as $(\mathbf{E}_1, \mathbf{E}_2)$ then*

$$O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = O_\ell(\alpha, \mathbf{E}_1', \mathbf{E}_2'). \tag{2.9}$$

Proof. Combining Lemma 2.11 with the surjectivity (Proposition 2.9) of $T(\mathbb{Q}_\ell) \to S(\mathbb{Q}_\ell)$ shows that the group $T(\mathbb{Q}_\ell)$ acts transitively on the set of all $\phi \in V_\ell(\mathbf{E}_1, \mathbf{E}_2)$ for which $\deg_{\mathrm{CM}}(\phi) = \alpha$. The independence of the orbital integral on the choice of ϕ is an immediate consequence of this. For the second claim, fix a $t = (t_1, t_2) \in T(\mathbb{A}_f)$. Set $\mathfrak{a}_i = t_i \widehat{\mathcal{O}}_{K_i}$ and

$$(\mathbf{E}_1', \mathbf{E}_2') = (\mathbf{E}_1 \otimes_{\mathcal{O}_{K_1}} \mathfrak{a}_1, \mathbf{E}_2 \otimes_{\mathcal{O}_{K_2}} \mathfrak{a}_2).$$

There is a K_i-linear quasi-isogeny $f_i \in \mathrm{Hom}(\mathbf{E}_i, \mathbf{E}_i') \otimes_{\mathbb{Z}} \mathbb{Q}$ defined by $f_i(x) = x \otimes 1$ The degree of f_i is $\mathrm{Nm}_{K_i/\mathbb{Q}}(\mathfrak{a}_i)^{-1}$, and in particular

$$\deg(f_1) = \deg(f_2). \tag{2.10}$$

The isomorphism

$$V_\ell(\mathbf{E}_1, \mathbf{E}_2) \cong V_\ell(\mathbf{E}_1', \mathbf{E}_2') \tag{2.11}$$

defined by $\phi \mapsto f_2 \circ \phi \circ f_1^{-1}$ identifies $L_\ell(\mathbf{E}_1', \mathbf{E}_2')$ with the $\mathbb{Z}_\ell$-lattice

$$t \bullet L_\ell(\mathbf{E}_1, \mathbf{E}_2) = \{\kappa_2(t_2) \circ \phi \circ \kappa_1(t_1)^{-1} \mid \phi \in L_\ell(\mathbf{E}_1, \mathbf{E}_2)\}$$

in $V_\ell(\mathbf{E}_1, \mathbf{E}_2)$ (the action $\bullet$ is that of (2.5)). Moreover the isomorphism (2.11) is K_ℓ-linear and respects the F_ℓ-quadratic form $\deg_{\mathrm{CM}}$ on source and target (the isomorphism respects the quadratic form deg by (2.10), and the therefore respects $\deg_{\mathrm{CM}}$ by the uniqueness part of Proposition 2.3) If there is no $\phi \in L_\ell(\mathbf{E}_1, \mathbf{E}_2)$ such that $\deg_{\mathrm{CM}}(\phi) = \alpha$ then the isomorphism (2.11) implies that both sides of (2.9) are 0. If there is such a ϕ then

$$\begin{aligned} O_\ell(\alpha, \mathbf{E}_1', \mathbf{E}_2') &= \sum_{s\in\mathbb{Q}_\ell^\times\backslash T(\mathbb{Q}_\ell)/U_\ell} \mathbf{1}_{L_\ell(\mathbf{E}_1',\mathbf{E}_2')}(s^{-1}\bullet\phi) \\ &= \sum_{s\in\mathbb{Q}_\ell^\times\backslash T(\mathbb{Q}_\ell)/U_\ell} \mathbf{1}_{t\bullet L_\ell(\mathbf{E}_1',\mathbf{E}_2')}(s^{-1}\bullet\phi) \\ &= O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2). \end{aligned}$$

□

Lemma 2.16. *Suppose ℓ is a finite prime different from p which is unramified in at least one of K_1 and K_2, and let $\delta_\ell \in F_\ell^\times$ be any generator of the $\mathcal{O}_{F,\ell}$-ideal $\mathfrak{D}_\ell$. There is an isomorphism of F_ℓ-quadratic spaces*

$$(V_\ell(\mathbf{E}_1,\mathbf{E}_2), \deg_{\mathrm{CM}}) \cong (K_\ell, \delta_\ell^{-1}\cdot \mathrm{Nm}_{K_\ell/F_\ell})$$

which is K_ℓ-linear and takes the $\mathbb{Z}_\ell$-lattice $L_\ell(\mathbf{E}_1,\mathbf{E}_2)$ isomorphically to $\mathcal{O}_{K,\ell}$.

Proof. The existence of the desired isomorphism for some choice of $\delta_\ell^{-1}\in F_\ell^\times$ is clear from Lemma 2.5 and the fact that up to isomorphism the only projective rank one module over $\mathcal{O}_{K_1,\ell}\otimes_{\mathbb{Z}_\ell}\mathcal{O}_{K_2,\ell}\cong\mathcal{O}_{K,\ell}$ is $\mathcal{O}_{K,\ell}$. Such a δ_ℓ^{-1} is uniquely determined up to multiplication by a norm from $\mathcal{O}_{K,\ell}^\times$. To show that $\delta_\ell\mathcal{O}_{F,\ell}=\mathfrak{D}_\ell$ the essential observation is that the $\mathbb{Z}_\ell$-bilinear form $[\cdot,\cdot]$ is a perfect pairing

$$L_\ell(\mathbf{E}_1,\mathbf{E}_2)\times L_\ell(\mathbf{E}_1,\mathbf{E}_2)\to\mathbb{Z}_\ell.$$

Indeed, any choice of $\mathbb{Z}_\ell$ bases for the Tate modules $\mathrm{Ta}_\ell(E_1)$ and $\mathrm{Ta}_\ell(E_2)$ determines an isomorphism of $\mathbb{Z}_\ell$-modules

$$L_\ell(\mathbf{E}_1,\mathbf{E}_2)\cong \mathrm{Hom}_{\mathbb{Z}_\ell}(\mathrm{Ta}_\ell(E_1),\mathrm{Ta}_\ell(E_2))\cong M_2(\mathbb{Z}_\ell)$$

which takes the quadratic form deg to the quadratic form $u\cdot\det$ for some $u\in\mathbb{Z}_p^\times$. After adjusting the choice of basis we may assume that $u=1$, and the isomorphism then identifies the bilinear form $[\phi_1,\phi_2]$ on $L_\ell(\mathbf{E}_1,\mathbf{E}_2)$ with the bilinear form $[X,Y]=\mathrm{Tr}(XY^\iota)$ on $M_2(\mathbb{Z}_\ell)$ (where $Y\mapsto Y^\iota$ is the involution satisfying $YY^\iota=\det(Y)$ for all Y). This latter bilinear form is a perfect pairing.

It follows that the $\mathcal{O}_{F,\ell}$-bilinear form of Proposition 2.3

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

is also a perfect pairing, and hence the F_ℓ-bilinear form $\delta_\ell^{-1}\mathrm{Tr}_{K_\ell/F_\ell}(x\overline{y})$ on K_ℓ restricts to a perfect pairing

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

The hypothesis that ℓ is unramified in either K_1 or K_2 implies that K_ℓ/F_ℓ is unramified, and so the trace form $\mathrm{Tr}_{K_\ell/F_\ell}$ is a perfect pairing $\mathcal{O}_{K,\ell}\times\mathcal{O}_{K,\ell}\to\mathcal{O}_{F,\ell}$. It follows that $\delta_\ell\mathcal{O}_{F,\ell}=\mathfrak{D}_\ell$. This gives the desired isomorphism for some choice of δ_ℓ which generates $\mathfrak{D}_\ell$. As K_ℓ/F_ℓ is unramified any other generator of $\mathfrak{D}_\ell$ differs from δ_ℓ by a norm from $\mathcal{O}_{K,\ell}^\times$, and if $u=\mathrm{Nm}_{K_\ell/F_\ell}(v)$ for some $v\in\mathcal{O}_{E,\ell}^\times$ then multiplication by v^{-1} defines an isomorphism

$$(K_\ell,\delta_\ell^{-1}\cdot\mathrm{Nm}_{K_\ell/F_\ell})\cong(K_\ell,u\delta_\ell^{-1}\cdot\mathrm{Nm}_{K_\ell/F_\ell})$$

which preserves the $\mathbb{Z}_\ell$-lattice $\mathcal{O}_{K,\ell}$. □

Proposition 2.17. *If ℓ is a finite prime not equal to p which is unramified in at least one of K_1 and K_2 then for every $\alpha \in F^\times$*

$$O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \rho_\ell(\alpha\mathfrak{D}).$$

Proof. Fix an isomorphism

$$(V_\ell(\mathbf{E}_1, \mathbf{E}_2), \deg_{\mathrm{CM}}) \cong (K_\ell, \delta_\ell^{-1} \cdot \mathrm{Nm}_{K_\ell/F_\ell})$$

as in Lemma 2.16. Proposition 2.9 implies that $(t_1, t_2) \mapsto \nu(t)^{-1}(t_1 \otimes t_2)$ defines an isomorphism

$$\mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell \to S(\mathbb{Q}_\ell)/V_\ell \tag{2.12}$$

which allows us to rewrite the orbital integral (2.8) as

$$O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \sum_{s \in S(\mathbb{Q}_\ell)/V_\ell} \mathbf{1}_{\mathcal{O}_{K,\ell}}(s^{-1} \cdot \phi) \tag{2.13}$$

where $\phi \in K_\ell$ satisfies $\mathrm{Nm}_{K_\ell/F_\ell}(\phi) = \alpha \cdot \delta_\ell$. If no such ϕ exists then $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = 0$.

Suppose first that ℓ is inert in both K_1 and K_2, so that

$$\mathcal{O}_{K,\ell} \cong \mathbb{Z}_{\ell^2} \times \mathbb{Z}_{\ell^2} \qquad \mathcal{O}_{F,\ell} \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

In this case $\mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell = \{1\}$ and (2.13) shows that $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = 1$ if there is a $\phi \in K_\ell$ satisfying $\mathrm{Nm}_{K_\ell/F_\ell}(\phi) = \alpha \cdot \delta_\ell$. Otherwise $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = 0$. It follows that $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \rho_\ell(\alpha\mathfrak{D})$ as both sides are equal to 1 if $\mathrm{ord}_w(\alpha\delta_\ell)$ is even and nonnegative for both places w of F above ℓ, and otherwise both sides are zero.

Suppose next that ℓ is inert in K_1 and is ramified in K_2. Then $F_\ell/\mathbb{Q}_\ell$ is a ramified field extension and K_ℓ/F_ℓ is an unramified field extension. Again one has $\mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell = \{1\}$ and (2.13) shows that $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = 1$ if there is a $\phi \in K_\ell$ satisfying $\mathrm{Nm}_{K_\ell/F_\ell}(\phi) = \alpha \cdot \delta_\ell$. Otherwise $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = 0$. It follows that $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \rho_\ell(\alpha\mathfrak{D})$, as both sides are equal to 1 if $\mathrm{ord}_w(\alpha\delta_\ell)$ is even and nonnegative for the unique place w of F above ℓ, and otherwise both sides are zero. The case of ℓ ramified in K_1 and inert in K_2 is identical.

Suppose next that ℓ is split in K_1 and nonsplit in K_2. Fix an isomorphism $\mathcal{O}_{K_1,\ell} \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ and a uniformizer $\varpi \in \mathcal{O}_{K_2,\ell}$. Let σ be the nontrivial Galois automorphism of $K_{2,\ell}$ and define

$$t_1 = (1, \mathrm{Nm}_{K_{2,\ell}/\mathbb{Q}_\ell}(\varpi)) \in K_{1,\ell}^\times \qquad t_2 = \varpi^\sigma \in K_{2,\ell}^\times.$$

Then $\mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell$ is the infinite cyclic group generated by $t = (t_1, t_2)$. Now identify

$$K_\ell \cong K_{1,\ell} \otimes_{\mathbb{Q}_\ell} K_{2,\ell} \cong K_{2,\ell} \times K_{2,\ell}$$

via $(x_1, x_2) \otimes y \mapsto (x_1 y, x_2 y^\sigma)$. Then

$$F_\ell \cong \{(a, b) \in K_{2,\ell} \times K_{2,\ell} \mid a = b\} \tag{2.14}$$

and

$$S(\mathbb{Q}_\ell) \cong \{(a, b) \in K_{2,\ell}^\times \times K_{2,\ell}^\times \mid ab = 1\}.$$

Using the isomorphism (2.12) and the above generator $t \in \mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell$ we find that $S(\mathbb{Q}_\ell)/V_\ell$ is the infinite cyclic group generated by (ϖ, ϖ^{-1}). It now follows from (2.13) that

$$O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \sum_{i=-\infty}^{\infty} \mathbf{1}_{\mathcal{O}_{K_2,\ell}}(\varpi^i \phi_1) \cdot \mathbf{1}_{\mathcal{O}_{K_2,\ell}}(\varpi^{-i} \phi_2)$$

where $(\phi_1, \phi_2) \in K_{2,\ell}^\times \times K_{2,\ell}^\times$ is any element which satisfies

$$(\phi_1\phi_2, \phi_1\phi_2) = \alpha\delta_\ell$$

under the identification (2.14). If we let w be the unique place of F above ℓ then $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \rho_\ell(\alpha\mathfrak{D})$ as both sides are $1 + \mathrm{ord}_w(\alpha\mathfrak{D})$ if $\mathrm{ord}_w(\alpha\mathfrak{D}) \geq 0$, and otherwise both sides are zero. The case of ℓ nonsplit in K_1 and split in K_2 is identical.

Finally suppose that ℓ is split in both K_1 and K_2 and fix isomorphisms

$$K_1 \cong \mathbb{Q}_\ell \times \mathbb{Q}_\ell \qquad K_2 \cong \mathbb{Q}_\ell \times \mathbb{Q}_\ell.$$

Define

$$\rho_{i,j} = (\ell^i, \ell^j) \in \mathbb{Q}_\ell^\times \times \mathbb{Q}_\ell^\times.$$

The group $\mathbb{Q}_\ell^\times \backslash T(\mathbb{Q}_\ell)/U_\ell$ is then isomorphic to the quotient of

$$\{(\rho_{a,b}, \rho_{c,d}) \in K_1^\times \times K_2^\times \mid a + b = c + d\}$$

by the subgroup $\{(\rho_{a,b}, \rho_{c,d}) \in K_1^\times \times K_2^\times \mid a = b = c = d\}$. If we identify

$$\mathcal{O}_{K,\ell} \cong \mathcal{O}_{K_1,\ell} \otimes \mathcal{O}_{K_2,\ell} \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell \tag{2.15}$$

via $(x_1, x_2) \otimes (y_1, y_2) \mapsto (x_1y_1, x_2y_2, x_1y_2, x_2y_1)$ then

$$\mathcal{O}_{F,\ell} = \{(z_1, z_2, z_3, z_4) \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell \mid z_1 = z_2, z_3 = z_4\}$$

and

$$S(\mathbb{Q}_\ell) \cong \{(z_1, z_2, z_3, z_4) \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell \mid z_1z_2 = 1, z_3z_4 = 1\}.$$

The isomorphism (2.12) takes $(\rho_{a,b}, \rho_{c,d})$ to the quadruple $(p^i, p^{-i}, p^j, p^{-j}) \in S(\mathbb{Q}_\ell)$ where $i = c - b = a - d$ and $j = d - b = a - c$, and a complete set of coset representatives for $S(\mathbb{Q}_\ell)/V_\ell$ is given by the set $\{(p^i, p^{-i}, p^j, p^{-j}) \mid i, j \in \mathbb{Z}\}$. It now follows from (2.13) that

$$O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \sum_{-\infty < i,j < \infty} \mathbf{1}_{\mathbb{Z}_\ell}(\varpi^i\phi_1) \cdot \mathbf{1}_{\mathbb{Z}_\ell}(\varpi^{-i}\phi_2) \cdot \mathbf{1}_{\mathbb{Z}_\ell}(\varpi^j\phi_3) \cdot \mathbf{1}_{\mathbb{Z}_\ell}(\varpi^{-j}\phi_4)$$

where $(\phi_1, \phi_2, \phi_3, \phi_4) \in \mathbb{Z}_\ell \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell \times \mathbb{Z}_\ell \cong \mathcal{O}_{F,\ell}$ satisfies

$$(\phi_1\phi_2, \phi_1\phi_2, \phi_3\phi_4, \phi_3\phi_4) = \alpha\delta_\ell$$

under (2.15). If we let w_1, w_2 be the two places of F above ℓ then $O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \rho_\ell(\alpha\mathfrak{D})$ as both sides are

$$(1 + \mathrm{ord}_{w_1}(\alpha\mathfrak{D}))(1 + \mathrm{ord}_{w_2}(\alpha\mathfrak{D}))$$

if $\mathrm{ord}_{w_1}(\alpha\mathfrak{D}) \geq 0$ and $\mathrm{ord}_{w_2}(\alpha\mathfrak{D}) \geq 0$, and otherwise both sides are zero. □

Proposition 2.18. *For any totally positive $\alpha \in F^\times$ and any prime p*

$$\sum_{x \in [\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})]} \frac{1}{|\mathrm{Aut}_{\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})}(x)|} = \frac{1}{2} \sum_{(\mathbf{E}_1, \mathbf{E}_2)} \prod_{\ell < \infty} O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2)$$

where the sum on the right is over the supersingular points $(\mathbf{E}_1, \mathbf{E}_2) \in [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]/\Gamma_0$.

Proof. Using Lemma 2.13 for the final equality we have

$$\sum_{x\in[\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})]} \frac{1}{|\mathrm{Aut}_{\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})}(x)|}$$

$$= \sum_{\substack{(\mathbf{E}_1,\mathbf{E}_2)\in[\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})] \\ \text{supersingular}}} \sum_{\substack{\phi\in V(\mathbf{E}_1,\mathbf{E}_2) \\ \deg_{\mathrm{CM}}(\phi)=\alpha}} \frac{\mathbf{1}_{L(\mathbf{E}_1,\mathbf{E}_2)}(\phi)}{|\mathrm{Aut}(\mathbf{E}_1,\mathbf{E}_2)|}$$

$$= \frac{1}{\mathbf{w}_1\mathbf{w}_2} \sum_{(\mathbf{E}_1,\mathbf{E}_2)} \sum_{([\mathfrak{a}_1],[\mathfrak{a}_2])\in\Gamma_0} \sum_{\substack{\phi\in V(\mathbf{E}_1\otimes\mathfrak{a}_1,\mathbf{E}_2\otimes\mathfrak{a}_2) \\ \deg_{\mathrm{CM}}(\phi)=\alpha}} \mathbf{1}_{L(\mathbf{E}_1\otimes\mathfrak{a}_1,\mathbf{E}_2\otimes\mathfrak{a}_2)}(\phi) \tag{2.16}$$

in which the outer sum is over the supersingular points $(\mathbf{E}_1,\mathbf{E}_2)\in[\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]/\Gamma_0$. For every pair of ideal classes $([\mathfrak{a}_1],[\mathfrak{a}_2])\in\Gamma_0$ fix a $t=(t_1,t_2)\in T(\mathbb{A}_f)$ whose image under (2.6) is $([\mathfrak{a}_1],[\mathfrak{a}_2])$, and set $\mathfrak{a}_i = t_i\widehat{\mathcal{O}}_{K_i}$. There are quasi-isogenies

$$f_1:\mathbf{E}_1\to\mathbf{E}_1\otimes\mathfrak{a}_1 \qquad f_2:\mathbf{E}_2\to\mathbf{E}_2\otimes\mathfrak{a}_2$$

both defined by $f_i(x)=x\otimes 1$. The isomorphism

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

defined by $\phi\mapsto f_2\circ\phi\circ f_1^{-1}$ identifies $\widehat{L}(\mathbf{E}_1\otimes\mathfrak{a}_1,\mathbf{E}_2\otimes\mathfrak{a}_2)$ with the $\widehat{\mathbb{Z}}$-lattice

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

in $\widehat{V}(\mathbf{E}_1,\mathbf{E}_2)$ (the action $\bullet$ is that of (2.5)). This gives the first equality in

$$\sum_{([\mathfrak{a}_1],[\mathfrak{a}_2])\in\Gamma_0} \sum_{\substack{\phi\in V(\mathbf{E}_1\otimes\mathfrak{a}_1,\mathbf{E}_2\otimes\mathfrak{a}_2) \\ \deg_{\mathrm{CM}}(\phi)=\alpha}} \mathbf{1}_{L(\mathbf{E}_1\otimes\mathfrak{a}_1,\mathbf{E}_2\otimes\mathfrak{a}_2)}(\phi)$$

$$= \sum_{t\in T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U} \sum_{\substack{\phi\in V(\mathbf{E}_1,\mathbf{E}_2) \\ \deg_{\mathrm{CM}}(\phi)=\alpha}} \mathbf{1}_{t\bullet\widehat{L}(\mathbf{E}_1,\mathbf{E}_2)}(\phi)$$

$$= \sum_{s\in S(\mathbb{Q})\backslash S(\mathbb{A}_f)/V} \sum_{\substack{\phi\in V(\mathbf{E}_1,\mathbf{E}_2) \\ \deg_{\mathrm{CM}}(\phi)=\alpha}} \mathbf{1}_{s\bullet\widehat{L}(\mathbf{E}_1,\mathbf{E}_2)}(\phi). \tag{2.17}$$

Let us assume that there is some $\phi_0\in V(\mathbf{E}_1,\mathbf{E}_2)$ for which $\deg_{\mathrm{CM}}(\phi_0)=\alpha$. By Lemma 2.11 the group $S(\mathbb{Q})$ acts simply transitively on the set of all such ϕ_0. Thus the above sum may be rewritten as

$$\sum_{s\in S(\mathbb{Q})\backslash S(\mathbb{A}_f)/V} \sum_{\substack{\phi\in V(\mathbf{E}_1,\mathbf{E}_2) \\ \deg_{\mathrm{CM}}(\phi)=\alpha}} \mathbf{1}_{s\bullet\widehat{L}(\mathbf{E}_1,\mathbf{E}_2)}(\phi) = \sum_{s\in S(\mathbb{Q})\backslash S(\mathbb{A}_f)/V} \sum_{\gamma\in S(\mathbb{Q})} \mathbf{1}_{s\bullet\widehat{L}(\mathbf{E}_1,\mathbf{E}_2)}(\gamma^{-1}\phi_0)$$

$$= |S(\mathbb{Q})\cap V| \sum_{s\in S(\mathbb{A}_f)/V} \mathbf{1}_{s\bullet\widehat{L}(\mathbf{E}_1,\mathbf{E}_2)}(\phi_0)$$

$$= \frac{\mathbf{w}_1\mathbf{w}_2}{2}\prod_\ell O_\ell(\alpha,\mathbf{E}_1,\mathbf{E}_2). \tag{2.18}$$

In the final equality we have used

$$|S(\mathbb{Q})\cap V| = |(T(\mathbb{Q})\cap U)/\{\pm1\}| = \frac{\mathbf{w}_1\mathbf{w}_2}{2}.$$

If no such ϕ_0 exists then both the first and last expression in (2.18) vanish. Combining (2.16), (2.17), and (2.18) completes the proof.

□

2.5. **Local calculations I.** Fix a prime p. For a positive integer d let $\mathbb{F}_{p^d} \subset \mathbb{F}_p^{\mathrm{alg}}$ be the subfield of p^d elements and let

$$\mathbb{Z}_{p^d} = W(\mathbb{F}_{p^d}) \qquad W = W(\mathbb{F}_p^{\mathrm{alg}})$$

be the Witt vectors of $\mathbb{F}_{p^d}$ and $\mathbb{F}_p^{\mathrm{alg}}$, respectively. Denote by $\sigma : W \to W$ the continuous ring automorphism of W which reduces to $x \mapsto x^p$ on the residue field $W/pW \cong \mathbb{F}_p^{\mathrm{alg}}$. Let $\mathbb{Q}_{p^d}$ be the fraction field of $\mathbb{Z}_{p^d}$.

Hypothesis 2.19. Throughout Section 2.5 we assume that p is inert in both K_1 and K_2. This hypothesis implies that

$$\mathcal{O}_{K,p} \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \qquad \mathcal{O}_{F,p} \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

but we do not (yet) fix such isomorphisms. This hypothesis also implies that all CM pairs over $\mathbb{F}_p^{\mathrm{alg}}$ are supersingular.

Fix a supersingular CM pair $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$. The action of $\mathcal{O}_{K_i}$ on $\mathrm{Lie}(E_i)$ is through some ring homomorphism $\tilde{\pi}_i : \mathcal{O}_{K_i} \to \mathbb{F}_p^{\mathrm{alg}}$, and as we assume that p is inert in K_i there is a unique ring homomorphism $\pi_i : \mathcal{O}_{K_i} \to \mathbb{Z}_{p^2}$ such that $\tilde{\pi}_i$ is equal to the composition

$$\mathcal{O}_{K_i} \xrightarrow{\pi_i} \mathbb{Z}_{p^2} \to \mathbb{F}_{p^2} \to \mathbb{F}_p^{\mathrm{alg}}.$$

Recalling that $K = K_1 \otimes_{\mathbb{Q}_p} K_2$ define a $\mathbb{Q}$-algebra homomorphism

$$\rho : K \to \mathbb{Q}_{p^2}$$

by $\rho(x_1 \otimes x_2) = \pi_2(x_2) \cdot \pi_1(x_1)$. Let $\mathfrak{q}$ be the prime of E such that ρ factors through the completion $\rho : K_{\mathfrak{q}} \to \mathbb{Q}_{p^2}$.

Definition 2.20. The prime $\mathfrak{p}$ of F lying below $\mathfrak{q}$ is the *reflex prime* of the CM pair $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$.

Define another $\mathbb{Q}$-algebra homomorphism

$$\rho' : K \to \mathbb{Q}_{p^2}$$

by $\rho'(x_1 \otimes x_2) = \pi_2(x_2) \cdot \pi_1(\overline{x}_1)$. Let $\mathfrak{q}'$ be the prime of K above p such that ρ' factors though an isomorphism $\rho' : \mathcal{O}_{K,\mathfrak{q}'} \to \mathbb{Z}_{p^2}$ and let $\mathfrak{p}'$ be the prime of F below $\mathfrak{q}'$. One can check that $\mathfrak{p} \neq \mathfrak{p}'$.

Let $\mathfrak{g}$ be a connected p-Barsotti-Tate group of dimension one and height two over $\mathbb{F}_p^{\mathrm{alg}}$. Up to isomorphism there is a unique such $\mathfrak{g}$, and $\mathfrak{g}$ is isomorphic to the p-Barsotti-Tate group of any supersingular elliptic curve over $\mathbb{F}_p^{\mathrm{alg}}$. Fix isomorphisms of p-Barsotti-Tate groups

$$f_1 : E_1[p^\infty] \to \mathfrak{g} \qquad f_2 : E_2[p^\infty] \to \mathfrak{g}. \tag{2.19}$$

Set $\Delta = \mathrm{End}(\mathfrak{g})$ so that Δ is the maximal order in a quaternion division algebra over $\mathbb{Q}_p$. Fix an embedding of $\mathbb{Z}_p$-algebras $\mathbb{Z}_{p^2} \to \Delta$. After possibly pre-composing this embedding with $\sigma : \mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}$ we may assume that the restriction to $\mathbb{Z}_{p^2}$ of the action of Δ on $\mathrm{Lie}(\mathfrak{g})$ is given by the composition

$$\mathbb{Z}_{p^2} \to \mathbb{F}_{p^2} \to \mathbb{F}_p^{\mathrm{alg}} \cong \mathrm{End}_{\mathbb{F}_p^{\mathrm{alg}}}(\mathrm{Lie}(\mathfrak{g})).$$

If we fix a uniformizing parameter $\Pi \in \Delta$ with the property that $x\Pi = \Pi x^\sigma$ for every $x \in \mathbb{Z}_{p^2}$ then there is a decomposition of $\mathbb{Z}_p$-modules

$$\Delta = \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}\Pi \tag{2.20}$$

which is orthogonal with respect to the quadratic form Nm (the reduced norm on Δ). We identify the $\mathbb{Z}_p$-modules

$$\Delta \cong L_p(\mathbf{E}_1, \mathbf{E}_2) \tag{2.21}$$

via $\phi \mapsto f_2^{-1} \circ \phi \circ f_1$ and identify $\Delta \cong \mathrm{End}(E_i[p^\infty])$ via $\phi \mapsto f_i^{-1} \circ \phi \circ f_i$.

Lemma 2.21. *The isomorphisms (2.19) may be chosen in such a way that the isomorphism (2.21) identifies the quadratic form* deg *on* $L_p(\mathbf{E}_1, \mathbf{E}_2)$ *with the quadratic form* Nm *on* Δ*, and so that the images of*

$$\kappa_i : \mathcal{O}_{K_i,p} \to \mathrm{End}(E_i[p^\infty]) \cong \Delta$$

for $i = 1, 2$ *are both equal to* $\mathbb{Z}_{p^2}$*. With these choices the diagram*

$$\begin{array}{ccc} \mathcal{O}_{K_i,p} & \xrightarrow{\pi_i} & \mathbb{Z}_{p^2} \\ & \searrow^{\kappa_i} & \downarrow \\ & & \Delta \end{array} \tag{2.22}$$

is commutative, where the vertical arrow is the inclusion $\mathbb{Z}_{p^2} \to \Delta$.

Proof. By the Noether-Skolem theorem there is an $\eta_i \in (\Delta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)^\times$ with the property that $\eta_i \kappa_i \eta_i^{-1} : K_{i,p} \to \Delta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ has image $\mathbb{Q}_{p^2}$. Multiplying η_i on the left by a multiple of Π does not change the image of this embedding, and so we may assume that $\eta_i \in \Delta^\times$. If we then replace f_i by $\eta_i \circ f_i$ then the resulting $\kappa_i : \mathcal{O}_{K_i,p} \to \Delta$ has image $\mathbb{Z}_{p^2}$.

By examining the Dieudonné module of $\mathfrak{g}$ one can show that $\mathfrak{g}$ admits a principal polarization $\mathfrak{g} \cong \mathfrak{g}^\vee$ which is unique up to multiplication by $\mathbb{Z}_p^\times$. After fixing such a polarization the resulting Rosati involution on Δ is equal to the main involution $\phi \mapsto \phi^\iota$ and the automorphism $\deg(f_i) = f_i \circ f_i^\vee$ of $\mathfrak{g}$ lies in $\mathbb{Z}_p^\times \subset \Delta^\times$ (here we identify $E_i[p^\infty]$ with its dual p-Barsotti-Tate group using the canonical principal polarization of E_i). Under the isomorphism (2.21) the quadratic form deg on $L_p(\mathbf{E}_1, \mathbf{E}_2)$ is identified with the $\mathbb{Z}_p$-quadratic form

$$\begin{aligned} Q(\phi) &= (f_2^{-1} \circ \phi \circ f_1) \circ (f_2^{-1} \circ \phi \circ f_1)^\vee \\ &= \deg(f_1) \cdot \deg(f_2)^{-1} \cdot \mathrm{Nm}(\phi) \end{aligned}$$

on Δ. If we choose a $u_i \in \mathbb{Z}_{p^2}^\times$ such that $\mathrm{Nm}(u_i) = \deg(f_i)^{-1}$ and replace f_i by $u_i \circ f_i$ then $\deg(f_i) = 1$, and the isomorphism (2.21) now identifies deg with Nm.

As $\kappa_i : \mathcal{O}_{K_i,p} \to \Delta$ has image $\mathbb{Z}_{p^2}$, to prove the commutativity of the diagram (2.22) it suffices to prove that the reductions

$$\mathcal{O}_{K_i,p} \to \mathbb{Z}_{p^2} \to \mathbb{F}_{p^2}$$

of κ_i and π_i are equal. This follows from our normalization of the inclusion $\mathbb{Z}_{p^2} \to \Delta$, as both reductions agree with the map

$$\mathcal{O}_{K_i,p} \to \mathbb{F}_p^{\mathrm{alg}} \cong \mathrm{End}_{\mathbb{F}_p^{\mathrm{alg}}}(\mathrm{Lie}(\mathfrak{g}))$$

describing the action of $\mathcal{O}_{K_i,p}$ on the Lie algebra of $\mathfrak{g}$ (identified with the Lie algebra of $E_i[p^\infty]$ using the isomorphism f_i). □

¿From now on we assume that f_1 and f_2 have been chosen as in Lemma 2.21. The isomorphism of $\mathbb{Z}_p$-quadratic spaces (2.21) is an isomorphism of $\mathcal{O}_{K,p}$-modules where the action of $\mathcal{O}_{K,p} \cong \mathcal{O}_{K_1,p} \otimes_{\mathbb{Z}_p} \mathcal{O}_{K_2,p}$ on Δ is through

$$(x_1 \otimes x_2) \bullet \phi = \kappa_2(x_2) \cdot \phi \cdot \kappa_1(\overline{x}_1). \tag{2.23}$$

This action preserves each summand in the decomposition (2.20): the action of $x \in \mathcal{O}_{K,p}$ on the summand $\mathbb{Z}_{p^2}$ is through left multiplication by $\rho'(x)$, and the action on the summand $\mathbb{Z}_{p^2}\Pi$ is through left multiplication by $\rho(x)$. Expressed differently, if we identify

$$\mathcal{O}_{K,p} \cong \mathcal{O}_{K,\mathfrak{p}'} \times \mathcal{O}_{K,\mathfrak{p}}$$

then the action of $(z', z) \in \mathcal{O}_{K,p}$ on Δ is through left multiplication by $\rho'(z')$ on the summand $\mathbb{Z}_{p^2}$ and through left multiplication by $\rho(z)$ on the summand $\mathbb{Z}_{p^2}\Pi$. This shows that Δ is free of rank one over $\mathcal{O}_{K,p}$ and has $1 + \Pi$ as a basis. Under the identification

$$\mathcal{O}_{K,p} \cong \mathcal{O}_{K,\mathfrak{p}'} \times \mathcal{O}_{K,\mathfrak{p}} \cong \Delta$$

defined by $(z', z) \mapsto \rho'(z') + \rho(z)\Pi$ the quadratic form Nm on Δ is identified with the quadratic form

$$x \mapsto \mathrm{Tr}_{F_p/\mathbb{Q}_p}\big(\beta \cdot \mathrm{Nm}_{K_p/F_p}(x)\big)$$

on $\mathcal{O}_{K,p}$ where

$$\beta = (1, \mathrm{Nm}(\Pi)) \in \mathcal{O}_{F,\mathfrak{p}'} \times \mathcal{O}_{F,\mathfrak{p}} \cong \mathcal{O}_{F,p}.$$

We have proved the existence of a $\mathcal{O}_{K,p}$-linear isomorphism of $\mathbb{Z}_p$-quadratic space

$$(\Delta, \mathrm{Nm}) \cong (\mathcal{O}_{K,p}, \mathrm{Tr}_{F_p/\mathbb{Q}_p}\beta \cdot \mathrm{Nm}_{K_p/F_p}). \tag{2.24}$$

Proposition 2.22. *Let $\beta \in F_p^\times$ be any element satisfying*

$$\mathrm{ord}_{\mathfrak{p}}(\beta) = 1 \qquad \mathrm{ord}_{\mathfrak{p}'}(\beta) = 0. \tag{2.25}$$

There is an isomorphism of F_p-quadratic spaces

$$(V_p(\mathbf{E}_1, \mathbf{E}_2), \deg_{\mathrm{CM}}) \cong (K_p, \beta \cdot \mathrm{Nm}_{K_p/F_p})$$

which is K_p-linear and takes the $\mathbb{Z}_p$-lattice $L_p(\mathbf{E}_1, \mathbf{E}_2)$ isomorphically to $\mathcal{O}_{K,p}$.

Proof. Combining (2.21) with (2.24) shows that for some β satisfying (2.25) there is an K_p-linear isomorphism of $\mathbb{Q}_p$-quadratic spaces

$$(V_p(\mathbf{E}_1, \mathbf{E}_2), \deg) \cong (K_p, \mathrm{Tr}_{F_p/\mathbb{Q}_p}\beta \cdot \mathrm{Nm}_{K_p/F_p})$$

which takes the $\mathbb{Z}_p$-lattice $L_p(\mathbf{E}_1, \mathbf{E}_2)$ isomorphically to $\mathcal{O}_{K,p}$. Two quadratic forms Q_1 and Q_2 on a finite free F_p-module are equal if and only if the $\mathbb{Q}_p$-quadratic forms $\mathrm{Tr}_{F_p/\mathbb{Q}_p}Q_1$ and $\mathrm{Tr}_{F_p/\mathbb{Q}_p}Q_2$ are equal, and it follows that the above isomorphism is also an isomorphism of F_p-quadratic spaces

$$(V_p(\mathbf{E}_1, \mathbf{E}_2), \deg_{\mathrm{CM}}) \cong (K_p, \beta \cdot \mathrm{Nm}_{K_p/F_p}).$$

This proves the claim for some β satisfying (2.25). The claim for all β satisfying (2.25) follows (as in the proof of Lemma 2.16) from the fact that E_p/F_p is unramified, which implies that the norm map is surjective on units. □

Proposition 2.23. *For any $\alpha \in F_p^\times$*

$$O_p(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \rho_p(\alpha\mathfrak{D}\mathfrak{p}^{-1}).$$

Proof. After choosing isomorphisms $K_{1,p} \cong \mathbb{Q}_{p^2}$ and $K_{2,p} \cong \mathbb{Q}_{p^2}$ one sees that

$$\mathbb{Q}_p^\times \backslash T(\mathbb{Q}_p)/U_p = \{1\},$$

and so by (2.8) the orbital integral $O_p(\alpha, \mathbf{E}_1, \mathbf{E}_2)$ is 1 if there is a $\phi \in L_p(\mathbf{E}_1, \mathbf{E}_2)$ satisfying $\deg_{\mathrm{CM}}(\phi) = \alpha$ and is 0 otherwise. Using the model of Proposition (2.22) we see that $O_p(\alpha, \mathbf{E}_1, \mathbf{E}_2) = 1$ if and only if there is a $\phi \in \mathcal{O}_{K,p}$ satisfying

$$\mathrm{Nm}_{K_p/F_p}(\phi) = \alpha\beta^{-1},$$

and after choosing isomorphisms

$$K_p \cong \mathbb{Q}_{p^2} \times \mathbb{Q}_{p^2} \qquad F_p \cong \mathbb{Q}_p \times \mathbb{Q}_p$$

we see that such a ϕ exists if and only if $\mathrm{ord}_w(\alpha\beta^{-1})$ is even and nonnegative for both places w of F above p. Using $\mathrm{ord}_w(\alpha\beta^{-1}) = \mathrm{ord}_w(\alpha\mathfrak{D}\mathfrak{p}^{-1})$ we find that both sides of the desired equality are 1 if $\mathrm{ord}_w(\alpha\mathfrak{D}\mathfrak{p}^{-1})$ is even and nonnegative for both places w of F above p, and otherwise both sides of the equality are 0. □

Corollary 2.24. *Suppose that* $\gcd(d_1, d_2) = 1$. *For every* $\alpha \in F^\times$

$$\prod_{\ell<\infty} O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \rho(\alpha\mathfrak{D}\mathfrak{p}^{-1}).$$

Proof. This is clear from Proposition 2.17, Proposition 2.23, and (1.1). □

Return to the action of K_p on $\Delta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ defined by (2.23). The orthogonal idempotents $(1,0)$ and $(0,1)$ in

$$F_p \cong F_{\mathfrak{p}'} \times F_{\mathfrak{p}} \cong \mathbb{Q}_p \times \mathbb{Q}_p \tag{2.26}$$

act as the projections to the first and second summands, respectively, in

$$\Delta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_{p^2} \oplus \mathbb{Q}_{p^2}\Pi,$$

and the function

$$\mathrm{Nm}_{\mathrm{CM}}(a + b\Pi) = (aa^\sigma, bb^\sigma\mathrm{Nm}(\Pi)) \in \mathbb{Q}_p \times \mathbb{Q}_p$$

is an F_p-quadratic form (using the identification (2.26)) on $\Delta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ which satisfies

$$\mathrm{Nm} = \mathrm{Tr}_{F_p/\mathbb{Q}_p}\mathrm{Nm}_{\mathrm{CM}}.$$

Using the isomorphism (2.21) and Lemma 2.21 we see that there is a K_p-linear isomorphism of F_p-quadratic spaces

$$(V_p(\mathbf{E}_1, \mathbf{E}_2), \deg_{\mathrm{CM}}) \cong (\Delta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p, \mathrm{Nm}_{\mathrm{CM}}) \tag{2.27}$$

which takes the $\mathbb{Z}_p$-lattice $L_p(\mathbf{E}_1, \mathbf{E}_2)$ isomorphically to Δ.

Let $\mathcal{CLN}$ be the category of complete local Noetherian W-algebras with residue field $\mathbb{F}_p^{\mathrm{alg}}$. For any $\mathbb{Z}_p$-subalgabra $\mathcal{O} \subset \Delta$ consider the functor $\mathrm{Def}(\mathfrak{g}, \mathcal{O})$ from $\mathcal{CLN}$ to the category of sets which assigns to an object A of $\mathcal{CLN}$ the set of isomorphism classes deformations of $\mathfrak{g}$, with its $\mathcal{O}$-action, to A. More formally, to an object A we assign the set $\mathrm{Def}(\mathfrak{g}, \mathcal{O})(A)$ of isomorphism classes of triples $(\mathfrak{G}, j, \rho)$ in which $\mathfrak{G}$ is a p-Barsotti-Tate group over A, $\rho : \mathfrak{G}_{/\mathbb{F}_p^{\mathrm{alg}}} \to \mathfrak{g}$ is an isomorphism from the special fiber of $\mathfrak{G}$ to $\mathfrak{g}$, and $j : \mathcal{O} \to \mathrm{End}(\mathfrak{G})$ is an action of $\mathcal{O}$ lifting the action of $\mathcal{O} \subset \Delta$ on $\mathfrak{g} \cong \mathfrak{G}_{/\mathbb{F}_p^{\mathrm{alg}}}$.

Proposition 2.25 (Gross). *The deformation functor* $\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2})$ *is represented by* W. *For any* $\phi = a + b\Pi \in \Delta$ *with* $b \neq 0$ *the deformation functor* $\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2}[\phi])$ *is represented by* $W/p^m W$ *where*

$$m = \frac{\mathrm{ord}_p(bb^\sigma) + 2}{2}. \tag{2.28}$$

Proof. By [13, Theorem 3.8] the deformation functor $\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2})$ is represented by the complete local Noetherian W-algebra W. Let $\mathfrak{G}$ be the universal deformation of $\mathfrak{g}$ over W. If we set $W_k = W/p^k W$ and $\mathfrak{G}_k = \mathfrak{G}_{/W_k}$ then according to a result of Gross [2, Proposition 3.3] (see also [17, Theorem 1.4]) the reduction map $\mathrm{End}(\mathfrak{G}_k) \to \mathrm{End}(\mathfrak{g})$ identifies

$$\mathrm{End}(\mathfrak{G}_k) \cong \mathbb{Z}_{p^2} + p^{k-1}\Delta.$$

An endomorphism $\phi = a + b\Pi \in \Delta$ therefore lifts to an endomorphism of $\mathfrak{G}_k$ if and only if $b\Pi \in p^{k-1}\Delta$, or equivalently if and only if

$$\mathrm{ord}_p(bb^\sigma) \geq 2k - 2.$$

In other words the endomorphism ϕ lifts to $\mathfrak{G}_m$ but not to $\mathfrak{G}_{m+1}$ where m is defined by (2.28). It follows from the rigidity theorem [11, Proposition 2.9] that the functor $\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2}[\phi])$ is represented by a quotient of W, and by the above discussion that quotient is precisely $W/p^m W$. □

Proposition 2.26. *For any supersingular* $x = (\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ *the completion of the strictly Henselian local ring of* $\mathcal{X}$ *at* x *is isomorphic to* W.

Proof. The completion of the strictly Henselian local ring of $\mathcal{X}$ at x represents the functor on $\mathcal{CLR}$ which assigns to every object A of $\mathcal{CLR}$ the set of isomorphism classes deformations of the CM pair $(\mathbf{E}_1, \mathbf{E}_2)$ to A. Using the isomorphisms (2.19) and the Serre-Tate theorem [1, Theorem 3.3] this functor is identified with the deformation functor

$$\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2}) \times \mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2}).$$

This latter functor is represented by $W \cong W \widehat{\otimes}_W W$, by the first part of Proposition 2.25. □

Corollary 2.27. *Suppose* $\mathfrak{p}$ *is either prime of* F *above* p *and let* $X_\mathfrak{p} \subset [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]$ *denote the set of supersingular points with reflex prime* $\mathfrak{p}$. *Then* $|X_\mathfrak{p}| = 2 \cdot |\Gamma|$.

Proof. Fix a continuous embedding of $\mathbb{Z}_p$-algebras $W \to \mathbb{C}_p$ and an isomorphism between the algebraic closures of $\mathbb{Q}$ in $\mathbb{C}_p$ and $\mathbb{C}$. By the theory of complex multiplication every CM pair $(\mathbf{E}_1, \mathbf{E}_2)$ defined over $\mathbb{C}$ or $\mathbb{C}_p$ admits a model over $\mathbb{Q}^{\mathrm{alg}}$, and there are canonical bijections

$$[\mathcal{X}(\mathbb{C})] \cong [\mathcal{X}(\mathbb{Q}^{\mathrm{alg}})] \cong [\mathcal{X}(\mathbb{C}_p)].$$

All CM pairs over $\mathbb{C}_p$ have good reduction modulo p, and so there is a well defined reduction map $[\mathcal{X}(\mathbb{C}_p)] \to [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]$. It follows from Proposition 2.26 that the reduction map is a bijection, and that there are canonical bijections

$$[\mathcal{X}(\mathbb{C}_p)] \cong [\mathcal{X}(\mathcal{O}_{\mathbb{C}_p})] \cong [\mathcal{X}(W)] \cong [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})].$$

By Remark 2.12 the set $[\mathcal{X}(\mathbb{C})]$ has $4 \cdot |\Gamma|$ elements, and so the same is true of $[\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]$.

Let $\mathfrak{p}$ and $\mathfrak{p}'$ be the two primes of F above p. It now suffices to show that the number of supersingular CM pairs $(\mathbf{E}_1, \mathbf{E}_2)$ over $\mathbb{F}_p^{\mathrm{alg}}$ with reflex prime $\mathfrak{p}$ is equal to the number of such pairs with reflex prime $\mathfrak{p}'$. If $\mathbf{E} = (E, \kappa)$ is a CM pair over any scheme define the *conjugate* CM pair $\mathbf{E}' = (E, \kappa')$ where $\kappa'(x) = \kappa(\overline{x})$. That is, the conjugate CM pair has the same underlying elliptic curve but the complex multiplication is replaced by its complex conjugate. One easily checks that $(\mathbf{E}_1, \mathbf{E}_2) \mapsto (\mathbf{E}_1, \mathbf{E}_2')$ establishes a bijection from $[\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]$ to itself which interchanges CM pairs of reflex prime $\mathfrak{p}$ with CM pairs of reflex prime $\mathfrak{p}'$. $\square$

Proposition 2.28. *Suppose* $\alpha \in F^\times$ *and*

$$x = (\mathbf{E}_1, \mathbf{E}_2, \phi) \in \mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}}).$$

Then the strictly Henselian local ring of $\mathcal{X}_\alpha$ *at* x *is Artinian of length*

$$\nu_{\mathfrak{p}}(\alpha) = \frac{\mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{D}) + 1}{2}$$

where $\mathfrak{p}$ *is the reflex prime of* $(\mathbf{E}_1, \mathbf{E}_2)$.

Proof. Under the isomorphism (2.21) ϕ corresponds to some $\phi = a + b\Pi \in \Delta$, and using the isomorphism (2.27) we have the equalities

$$\mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(\phi)) = \mathrm{ord}_{\mathfrak{p}}(\mathrm{Nm}_{\mathrm{CM}}(\phi)) = 1 + \mathrm{ord}_p(bb^\sigma).$$

Consider the functor

$$\mathfrak{Z} = \mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2}) \times \mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2}).$$

of pairs of deformations of $\mathfrak{g}$ with its $\mathbb{Z}_{p^2}$-action. This functor is represented by $W \cong W \widehat{\otimes}_W W$, by the first part of Proposition 2.25, and in particular the diagonal inclusion $\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2}) \to \mathfrak{Z}$ is an isomorphism. The subfunctor $\mathfrak{Z}_\phi \to \mathfrak{Z}$ of pairs of deformations $(\mathfrak{G}_1, \mathfrak{G}_2)$ of $\mathfrak{g}$ for which the endomorphism ϕ lifts to an isogeny $\mathfrak{G}_1 \to \mathfrak{G}_2$ is therefore isomorphic to the deformation functor $\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2}[\phi])$. By Proposition 2.25 the deformation functor $\mathfrak{Z}_\phi \cong \mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2}[\phi])$ is represented by an Artinian W-algebra of length $\nu_{\mathfrak{p}}(\alpha)$.

The completion of the strictly Henselian local ring of $\mathcal{X}_\alpha$ at x represents the functor on $\mathcal{CLR}$ which assigns to every object A of $\mathcal{CLR}$ the set of isomorphism classes deformations of the triple $(\mathbf{E}_1, \mathbf{E}_2, \phi)$ to A. Using the isomorphisms (2.19) and the Serre-Tate theorem [1, Theorem 3.3] this functor is identified with the deformation functor $\mathfrak{Z}_\phi$, which we have just seen is represented by an Artinian local ring of length $\nu_{\mathfrak{p}}(\alpha)$. $\square$

Proposition 2.29. *Suppose that* $\gcd(d_1, d_2) = 1$. *For every totally positive* $\alpha \in F^\times$

$$\sum_{x \in [\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})]} e_x^{-1} \cdot \mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}) = \frac{1}{2} \cdot \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{D}\mathfrak{p}) \cdot \rho(\alpha\mathfrak{D}\mathfrak{p}^{-1})$$

where the sum is over the two primes of F *above* p *and* $e_x = |\mathrm{Aut}_{\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})}(x)|$.

Proof. Recall that all points in $\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$ are supersingular by Corollary 2.8. Given a supersingular point $x \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ let $\mathfrak{p}_x$ be the reflex prime of x. A minor refinement of Proposition 2.18 (in (2.16) one restricts to points with reflex prime $\mathfrak{p}$, and the remainder of the argument holds verbatim) shows that for each prime $\mathfrak{p} \mid p$ of F

$$\sum_{\substack{x \in [\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})] \\ \mathfrak{p}_x = \mathfrak{p}}} e_x^{-1} = \frac{1}{2} \sum_{\substack{x \in [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]/\Gamma_0 \\ x \text{ supersingular} \\ \mathfrak{p}_x = \mathfrak{p}}} \prod_{\ell < \infty} O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2)$$

where $(\mathbf{E}_1, \mathbf{E}_2)$ is the CM pair represented by x. Combining Corollary 2.24, Corollary 2.27, and Proposition 2.28 yields

$$\begin{aligned}
\sum_{x\in[\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})]} e_x^{-1}\cdot \mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x}) &= \sum_{\mathfrak{p}} \nu_{\mathfrak{p}}(\alpha)\cdot \sum_{\substack{x\in[\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})]\\ x \text{ supersingular}\\ \mathfrak{p}_x=\mathfrak{p}}} e_x^{-1} \\
&= \sum_{\mathfrak{p}} \frac{\nu_{\mathfrak{p}}(\alpha)}{2}\cdot \sum_{\substack{x\in[\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]/\Gamma_0\\ x \text{ supersingular}\\ \mathfrak{p}_x=\mathfrak{p}}} \prod_{\ell<\infty} O_\ell(\alpha,\mathbf{E}_1,\mathbf{E}_2) \\
&= \sum_{\mathfrak{p}} \frac{\nu_{\mathfrak{p}}(\alpha)}{2}\cdot \sum_{\substack{x\in[\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]/\Gamma_0\\ x \text{ supersingular}\\ \mathfrak{p}_x=\mathfrak{p}}} \rho(\alpha\mathfrak{D}\mathfrak{p}^{-1}) \\
&= \sum_{\mathfrak{p}} \nu_{\mathfrak{p}}(\alpha)\cdot[\Gamma:\Gamma_0]\cdot\rho(\alpha\mathfrak{D}\mathfrak{p}^{-1}).
\end{aligned}$$

Now use Proposition 2.14. □

2.6. **Local calculations II.** Fix a prime p and let $\mathbb{Z}_{p^d}$, $\mathbb{Q}_{p^d}$, W, and σ have the same meaning as in Section 2.5

Hypothesis 2.30. Throughout Section 2.6 we assume that p is inert in K_1 and ramified in K_2. This hypothesis also implies that all CM pairs over $\mathbb{F}_p^{\mathrm{alg}}$ are supersingular.

Our hypothesis implies that $F_p/\mathbb{Q}_p$ is a ramified field extension of degree 2 and that K_p/F_p is an unramified extension of degree 2. Let $\mathfrak{p}$ denote the unique prime of F above p. Set

$$\mathcal{W} = W\otimes_{\mathbb{Z}_p}\mathcal{O}_{K_2,p}.$$

If we fix a uniformizer $\varpi\in\mathcal{O}_{K_2,p}$ then ϖ is also a uniformizing parameter of the complete discrete valuation ring $\mathcal{W}$.

Fix a supersingular CM pair $(\mathbf{E}_1,\mathbf{E}_2)\in\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$. Let $\mathfrak{g}$ be the connected p-Barsotti-Tate group of dimension one and height two over $\mathbb{F}_p^{\mathrm{alg}}$. Thus the p-Barsotti-Tate group of every supersingular elliptic curve over $\mathbb{F}_p^{\mathrm{alg}}$ is isomorphic to $\mathfrak{g}$. Fix isomorphisms

$$f_1 : E_1[p^\infty]\to\mathfrak{g} \qquad f_2 : E_2[p^\infty]\to\mathfrak{g} \tag{2.29}$$

Set $\Delta = \mathrm{End}(\mathfrak{g})$ so that Δ is the maximal order in a quaternion division algebra over $\mathbb{Q}_p$. We identify

$$\Delta\cong L_p(\mathbf{E}_1,\mathbf{E}_2) \tag{2.30}$$

via $\phi\mapsto f_2^{-1}\circ\phi\circ f_1$ and view $\kappa_i:\mathcal{O}_{K_i,p}\to\mathrm{End}(E_i[p^\infty])$ as a ring homomorphism

$$\kappa_i:\mathcal{O}_{K_i,p}\to\Delta$$

using the isomorphism of $\mathbb{Z}_p$-modules $\Delta\to\mathrm{End}(E_i[p^\infty])$ defined by $\phi\mapsto f_i^{-1}\circ\phi\circ f_i$. Fix an isomorphism of $\mathbb{Z}_p$-algebras $\kappa_1(\mathcal{O}_{K_1,p})\cong\mathbb{Z}_{p^2}$, and use this to view $\mathbb{Z}_{p^2}$ as a subring of Δ. Set $\Pi=\kappa_2(\varpi)$, so that Π is a uniformizer of Δ and

$$\Delta = \mathbb{Z}_{p^2}+\Pi\Delta.$$

Lemma 2.31. *The isomorphisms (2.29) may be chosen in such a way that the isomorphism (2.30) identifies the quadratic form* deg *on* $L_p(\mathbf{E}_1, \mathbf{E}_2)$ *with the quadratic form* Nm *(the reduced norm) on* Δ.

Proof. The proof of Lemma 2.21 shows that the isomorphism (2.30) identifies the quadratic form deg on $L_p(\mathbf{E}_1, \mathbf{E}_2)$ with the quadratic form $u \cdot \mathrm{Nm}$ on Δ for some $u \in \mathbb{Z}_p^\times$. If f_1 is replaced by $v \circ f_2$ with $v \in \Delta^\times$ then the constant u is replaced by $u \cdot \mathrm{Nm}(v)^{-1}$, and as the reduced norm $\Delta^\times \to \mathbb{Z}_p^\times$ is surjective we may choose v in such a way that $u \cdot \mathrm{Nm}(v)^{-1} = 1$. □

¿From now on we assume that f_1 and f_2 have been chosen as in Lemma 2.31.

Proposition 2.32. *If* $\beta \in F_p^\times$ *is any element satisfying*

$$\mathrm{ord}_{\mathfrak{p}}(\beta\mathfrak{D}) = 1$$

then there is an isomorphism of F_p*-quadratic spaces*

$$(V_p(\mathbf{E}_1, \mathbf{E}_2), \deg_{\mathrm{CM}}) \cong (K_p, \beta \cdot \mathrm{Nm}_{K_p/F_p})$$

which is K_p*-linear and takes the* $\mathbb{Z}_p$*-lattice* $L_p(\mathbf{E}_1, \mathbf{E}_2)$ *isomorphically to* $\mathcal{O}_{K,p}$.

Proof. Using the isomorphism (2.30) the $\mathbb{Z}_p$-bilinear form $[\cdot, \cdot]$ on $L_p(\mathbf{E}_1, \mathbf{E}_2)$ corresponds to the bilinear form $[\phi_1, \phi_2] = \mathrm{Tr}(\phi_1 \phi_2^\iota)$ on Δ, where Tr is the reduced trace and $x \mapsto x^\iota$ is the main involution. The dual lattice of Δ with respect to this bilinear form, defined by

$$\Delta^\vee = \{\phi \in \Delta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \mid [\phi_1, \phi_2] \in \mathbb{Z}_p \ \forall \phi_2 \in \Delta\},$$

is equal to $\Delta^\vee = \Pi^{-1}\Delta$, and in particular $[\Delta^\vee : \Delta] = p^2$. This implies that the $\mathbb{Z}_p$-lattice $L_p(\mathbf{E}_1, \mathbf{E}_2)$ has index p^2 in its dual lattice

$$L_p(\mathbf{E}_1, \mathbf{E}_2)^\vee = \{\phi \in V_p(\mathbf{E}_1, \mathbf{E}_2) \mid [\phi_1, \phi_2] \in \mathbb{Z}_p \ \forall \phi_2 \in L_p(\mathbf{E}_1, \mathbf{E}_2)\}. \tag{2.31}$$

By Lemma 2.5, for some choice of $\beta \in F_p^\times$ there is a K_p-linear isomorphism of F_p-quadratic spaces

$$(V_p(\mathbf{E}_1, \mathbf{E}_2), \deg_{\mathrm{CM}}) \cong (K_p, \beta \cdot \mathrm{Nm}_{K_p/F_p}).$$

As in the proof of Lemma 2.16 this map may be chosen to identify $L_p(\mathbf{E}_1, \mathbf{E}_2)$ with $\mathcal{O}_{K,p}$. In particular the isomorphism identifies the F_p-bilinear form $[\phi_1, \phi_2]_{\mathrm{CM}}$ on the left with the bilinear form $\beta \cdot \mathrm{Tr}_{K_p/F_p}(\phi_1 \overline{\phi}_2)$ on the right. The dual lattice (2.31) has the alternate description

$$L_p(\mathbf{E}_1, \mathbf{E}_2)^\vee = \{\phi \in V_p(\mathbf{E}_1, \mathbf{E}_2) \mid [\phi_1, \phi_2]_{\mathrm{CM}} \in \mathfrak{D}_p^{-1} \ \forall \phi_2 \in L_p(\mathbf{E}_1, \mathbf{E}_2)\},$$

and hence $\mathcal{O}_{K,p}$ has index p^2 in the dual lattice

$$\mathcal{O}_{K,p}^\vee = \{x \in K_p \mid \beta \cdot \mathrm{Tr}_{K_p/F_p}(x\overline{y}) \in \mathfrak{D}_p^{-1} \ \forall y \in \mathcal{O}_{K,p}\}.$$

As the dual lattice is stable under the action of $\mathcal{O}_{K,p}$ the only possibility is $\mathcal{O}_{K,p}^\vee = \varpi^{-1}\mathcal{O}_{K,p}$. But using the fact that K_p/F_p is unramified we have

$$\mathcal{O}_{K,p} = \{x \in K_p \mid \mathrm{Tr}_{K_p/F_p}(x\overline{y}) \in \mathcal{O}_{F,p} \ \forall y \in \mathcal{O}_{K,p}\}$$

from which it follows that

$$\mathcal{O}_{K,p}^\vee = \beta^{-1}\mathfrak{D}_p^{-1}\mathcal{O}_{K,p}.$$

Hence $\mathrm{ord}_\varpi(\beta\mathfrak{D}) = 1$. This shows that the conclusion of the proposition holds for some $\beta \in F_p^\times$ satisfying $\mathrm{ord}_{\mathfrak{p}}(\beta\mathfrak{D}) = 1$, and the conclusion holds for any such β as in the proof of Lemma 2.16 (using the fact that K_p/F_p is unramified). □

Proposition 2.33. *For any* $\alpha \in F_p^\times$

$$O_p(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \rho_p(\alpha\mathfrak{D}\mathfrak{p}^{-1}).$$

Proof. The hypothesis that p is inert in K_1 and ramified in K_2 implies that

$$\mathbb{Q}_p^\times \backslash T(\mathbb{Q}_p)/U_p = \{1\}.$$

Thus $O_p(\alpha, \mathbf{E}_1, \mathbf{E}_2) = 1$ if there is a $\phi \in L_p(\mathbf{E}_1, \mathbf{E}_2)$ such that $\deg_{\mathrm{CM}}(\phi) = \alpha$, and otherwise $O_p(\alpha, \mathbf{E}_1, \mathbf{E}_2) = 0$. Using Proposition 2.32 we see that such a ϕ exists if and only if there is an $x \in \mathcal{O}_{K,p}$ such that $\beta \cdot \mathrm{Nm}_{K_p/F_p}(x) = \alpha$, where $\mathrm{ord}_\mathfrak{p}(\beta\mathfrak{D}) = 1$. As K_p/F_p is an unramified field extension, both sides of the desired equality are equal to 1 if $\mathrm{ord}_\mathfrak{p}(\alpha\mathfrak{D}\mathfrak{p}^{-1})$ is even and nonnegative. Otherwise both sides are 0. □

Corollary 2.34. *Suppose that* $\gcd(d_1, d_2) = 1$*. For every* $\alpha \in F^\times$

$$\prod_{\ell<\infty} O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) = \rho(\alpha\mathfrak{D}\mathfrak{p}^{-1}).$$

Proof. This is immediate from Propositions 2.17 and 2.33. □

As in Section 2.5 let $\mathcal{CLN}$ be the category of complete local Noetherian W-algebras with residue field $\mathbb{F}_p^{\mathrm{alg}}$, and for any $\mathbb{Z}_p$-subalgebra $\mathcal{O} \subset \Delta$ let $\mathrm{Def}(\mathfrak{g}, \mathcal{O})$ be the functor which assigns to an object A of $\mathcal{CLR}$ the set of isomorphism classes of deformations $(\mathfrak{G}, j, \rho)$ of $\mathfrak{g}$, with its action of $\mathcal{O}$, to A. If $\phi \in \Delta$ let $\mathfrak{Z}_\phi$ be the functor which assigns to an object A of $\mathcal{CLN}$ the subset

$$\mathfrak{Z}_\phi(A) \subset \mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2})(A) \times \mathrm{Def}(\mathfrak{g}, \mathbb{Z}_p[\Pi])(A)$$

of pairs of deformations $(\mathfrak{G}_1, \mathfrak{G}_2)$ for which the endomorphism $\phi : \mathfrak{g} \to \mathfrak{g}$ lifts to an isogeny $\mathfrak{G}_1 \to \mathfrak{G}_2$.

Let ord_Δ be the valuation on Δ defined by

$$\mathrm{ord}_\Delta(\phi) = m \iff \phi \in \Pi^m \Delta^\times.$$

Proposition 2.35 (Gross)**.** *The functor* $\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2})$ *is represented by* W *and the functor* $\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_p[\Pi])$ *is represented by* $\mathcal{W}$*. For any nonzero* $\phi \in \Delta$ *the functor* $\mathfrak{Z}_\phi$ *is represented by* $\mathcal{W}/\varpi^{m+1}\mathcal{W}$ *where* $m = \mathrm{ord}_\Delta(\phi)$*.*

Proof. The claims about $\mathrm{Def}(\mathfrak{g}, \mathcal{O})$ for $\mathcal{O} = \mathbb{Z}_{p^2} \cong \mathcal{O}_{K_1,p}$ and $\mathcal{O} = \mathbb{Z}_p[\Pi] \cong \mathcal{O}_{K_2,p}$ are found in [13, Theorem 3.8]. Let $(\mathfrak{G}_1, j_1, \rho_1)$ be the universal deformation of $\mathfrak{g}$, with its $\mathbb{Z}_{p^2}$-action, to W. Similarly let $(\mathfrak{G}_2, j_2, \rho_2)$ be the universal deformation of $\mathfrak{g}$, with its $\mathbb{Z}_p[\Pi]$-action, to $\mathcal{W}$. Abbreviate $\mathcal{W}_k = \mathcal{W}/\varpi^k\mathcal{W}$. Let $\mathfrak{Z}$ be the functor on $\mathcal{CLR}$ defined by

$$\mathfrak{Z}(A) = \mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2})(A) \times \mathrm{Def}(\mathfrak{g}, \mathbb{Z}_p[\Pi])(A), \tag{2.32}$$

so that $\mathfrak{Z}$ is represented by $\mathcal{W} \cong W\widehat{\otimes}_W\mathcal{W}$. By the rigidity theorem [11, Proposition 2.9] the subfunctor $\mathfrak{Z}_\phi$ is represented by a quotient of $\mathcal{W}$. We will prove by induction on $m = \mathrm{ord}_\Delta(\phi)$ that this quotient is $\mathcal{W}_{m+1}$

Suppose first that $m = 0$ so that $\phi \in \Delta^\times$, and assume that ϕ lifts to an isogeny

$$\Phi : \mathfrak{G}_{1/\mathcal{W}_k} \to \mathfrak{G}_{2/\mathcal{W}_k}.$$

Then Φ is necessarily an isomorphism of p-Barsotti-Tate groups. As the endomorphism Π of $\mathfrak{g}$ lifts to an an endomorphism $\mathfrak{G}_{2/\mathcal{W}_k}$, the endomorphism $\phi^{-1}\Pi\phi$ of $\mathfrak{g}$ lifts to an endomorphism of $\mathfrak{G}_{2/\mathcal{W}_k}$. But $\mathbb{Z}_{p^2}$ and $\phi^{-1}\Pi\phi$ generate Δ as a $\mathbb{Z}_p$-algebra, and hence the full endomorphism ring $\Delta = \mathrm{End}(\mathfrak{g})$ lifts to the deformation

$\mathfrak{G}_{1/\mathcal{W}_k}$. From this it follows that the full endomorphism ring $\Delta = \phi\Delta\phi^{-1}$ also lifts to $\mathfrak{G}_{2/\mathcal{W}_k}$, and a calculation of Gross [2, Proposition 3.3] (see also [17, Theorem 1.4]) shows that this can only happen when $k = 1$. Thus when $m = 0$ the isogeny ϕ lifts to an isogeny $\mathfrak{G}_{1/\mathcal{W}_1} \to \mathfrak{G}_{2/\mathcal{W}_1}$ but not to an isogeny $\mathfrak{G}_{1/\mathcal{W}_2} \to \mathfrak{G}_{2/\mathcal{W}_2}$, proving that $\mathfrak{Z}_\phi$ is represented by $\mathcal{W}_1$.

The induction step of the argument is provided by [17, Proposition 5.2]: if ϕ lifts to an isogeny $\mathfrak{G}_{1/\mathcal{W}_k} \to \mathfrak{G}_{2/\mathcal{W}_k}$ but not to an isogeny $\mathfrak{G}_{1/\mathcal{W}_{k+1}} \to \mathfrak{G}_{2/\mathcal{W}_{k+1}}$ then $\Pi\circ\phi$ lifts to an isogeny $\mathfrak{G}_{1/\mathcal{W}_{k+1}} \to \mathfrak{G}_{2/\mathcal{W}_{k+1}}$ but not to an isogeny $\mathfrak{G}_{1/\mathcal{W}_{k+2}} \to \mathfrak{G}_{2/\mathcal{W}_{k+2}}$. Thus the functor $\mathfrak{Z}_\phi$ is represented by $\mathcal{W}_{\mathrm{ord}_\Delta(\phi)+1}$. □

Proposition 2.36. *For any $x \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ the completion of the strictly Henselian local ring of $\mathcal{X}$ at x is isomorphic to $\mathcal{W}$.*

Proof. The completion of the strictly Henselian local ring of $\mathcal{X}$ at x represents the functor on $\mathcal{CLR}$ which assigns to an object A of $\mathcal{CLR}$ the set of isomorphism classes of deformations of the CM pair $(\mathbf{E}_1, \mathbf{E}_2)$. Using the isomorphisms (2.29) and the Serre-Tate theorem [1, Theorem 3.3] this functor is isomorphic to the functor

$$\mathrm{Def}(\mathfrak{g}, \mathbb{Z}_{p^2}) \times \mathrm{Def}(\mathfrak{g}, \mathbb{Z}_p[\Pi]).$$

This latter functor is represented by $\mathcal{W} \cong W\widehat{\otimes}_W\mathcal{W}$, by Proposition 2.35. □

Corollary 2.37. *There are $2 \cdot |\Gamma|$ isomorphism classes of objects in $\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$.*

Proof. Fix a continuous embedding of $\mathbb{Z}_p$-algebras $W \to \mathbb{C}_p$ and an isomorphism between the algebraic closures of $\mathbb{Q}$ in $\mathbb{C}_p$ and $\mathbb{C}$. By the theory of complex multiplication every CM pair $(\mathbf{E}_1, \mathbf{E}_2)$ defined over $\mathbb{C}$ or $\mathbb{C}_p$ admits a model over $\mathbb{Q}^{\mathrm{alg}}$, and there are canonical bijections

$$[\mathcal{X}(\mathbb{C})] \cong [\mathcal{X}(\mathbb{Q}^{\mathrm{alg}})] \cong [\mathcal{X}(\mathbb{C}_p)].$$

All CM pairs over $\mathbb{C}_p$ have good reduction modulo p, and so there is a well defined reduction map $[\mathcal{X}(\mathbb{C}_p)] \to [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]$. It follows from Proposition 2.36 that the reduction map is 2-to-1: every point $x \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ deforms uniquely to $\mathcal{W}$, and the two W-algebra embeddings $\mathcal{W} \to \mathbb{C}_p$ give the two points of $\mathcal{X}(\mathbb{C}_p)$ which reduce to x. By Remark 2.12 the set $[\mathcal{X}(\mathbb{C})]$ has $4 \cdot |\Gamma|$ elements, and so $[\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]$ has $2 \cdot |\Gamma|$ elements. □

Proposition 2.38. *For any $\alpha \in F^\times$ and $x \in \mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$ the strictly Henselian local ring of $\mathcal{X}_\alpha$ at x is Artinian of length*

$$\nu_\mathfrak{p}(\alpha) = \frac{\mathrm{ord}_\mathfrak{p}(\alpha\mathfrak{D}) + 1}{2}.$$

Proof. Using the isomorphism (2.30) we may identify $\phi \in L_p(\mathbf{E}_1, \mathbf{E}_2)$ with an element of Δ. Using the isomorphisms (2.29) and the Serre-Tate theorem [1, Theorem 3.3] the completion of the strictly Henselian local ring of $\mathcal{X}_\alpha$ at x represents the deformation functor $\mathfrak{Z}_\phi$ of (2.32). By Proposition 2.35 the strictly Henselian local ring of $\mathcal{X}_\alpha$ at x is therefore Artinian of length $\mathrm{ord}_\Delta(\phi) + 1$, and it only remains to prove the equality

$$\mathrm{ord}_\Delta(\phi) = \frac{\mathrm{ord}_\mathfrak{p}(\deg_{\mathrm{CM}}(\phi)) + \mathrm{ord}_\mathfrak{p}(\mathfrak{D}\mathfrak{p}^{-1})}{2}. \tag{2.33}$$

First suppose that $\phi \in \Delta^\times$. Equivalently (by Lemma 2.31) suppose that $\deg(\phi) \in \mathbb{Z}_p^\times$. Recalling that ϖ was a uniformizing parameter of F_p satisfying $\kappa_2(\varpi) = \Pi$, we also view $\varpi = 1 \otimes \varpi$ as a uniformizer of K_p. By the K_p-linearity of the isomorphism of Proposition 2.32 the multiples of ϖ in $L_p(\mathbf{E}_1, \mathbf{E}_2)$ are carried bijectively to the multiples of ϖ in $\mathcal{O}_{K,p}$, and so the condition $\deg(\phi) \in \mathbb{Z}_p^\times$ implies that the image of ϕ in $\mathcal{O}_{K,p}$ lies in $\mathcal{O}_{K,p}^\times$. Again using Proposition 2.32 we see that $\deg_{\mathrm{CM}}(\phi) = \beta \cdot u$ for some $u \in \mathcal{O}_{F,p}^\times$ and some $\beta \in F_p^\times$ satisfying $\mathrm{ord}_{\mathfrak{p}}(\beta\mathfrak{D}) = 1$. In other words

$$\mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(\phi)) = -\mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}\mathfrak{p}^{-1})$$

proving (2.33) in the special case $\phi \in \Delta^\times$. For an arbitrary ϕ factor $\phi = \Pi^m \phi_0$ with $\phi_0 \in \Delta^\times$. By Proposition 2.32

$$\begin{aligned} \deg_{\mathrm{CM}}(\phi) &= \deg_{\mathrm{CM}}(\kappa_2(\varpi^m) \circ \phi_0) \\ &= \mathrm{Nm}_{K_p/F_p}(\varpi^m) \cdot \deg_{\mathrm{CM}}(\phi_0) \\ &= \mathrm{Nm}_{K_{2,p}/\mathbb{Q}_p}(\varpi^m) \cdot \deg_{\mathrm{CM}}(\phi_0). \end{aligned}$$

As both $K_{2,p}/\mathbb{Q}_p$ and $F_{\mathfrak{p}}/\mathbb{Q}_p$ are ramified of degree 2 we see that

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(\phi)) &= 2m + \mathrm{ord}_{\mathfrak{p}}(\deg_{\mathrm{CM}}(\phi_0)) \\ &= 2m - \mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}\mathfrak{p}^{-1}) \\ &= 2\mathrm{ord}_{\Delta}(\phi) - \mathrm{ord}_{\mathfrak{p}}(\mathfrak{D}\mathfrak{p}^{-1}) \end{aligned}$$

proving (2.33) in the general case. □

Proposition 2.39. *Suppose that* $\gcd(d_1, d_2) = 1$. *For every totally positive* $\alpha \in F^\times$

$$\sum_{x \in [\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})]} e_x^{-1} \cdot \mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha}) = \frac{1}{2} \cdot \mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{D}\mathfrak{p}) \cdot \rho(\alpha\mathfrak{D}\mathfrak{p}^{-1})$$

where $e_x = |\mathrm{Aut}_{\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})}(x)|$.

Proof. Combining Proposition 2.18, Corollary 2.34, Corollary 2.37, and Proposition 2.38 yields

$$\begin{aligned} \sum_{x \in [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]} e_x^{-1} \cdot \mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x}) &= \nu_{\mathfrak{p}}(\alpha) \sum_{x \in [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]} e_x^{-1} \\ &= \frac{\nu_{\mathfrak{p}}(\alpha)}{2} \sum_{x \in [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]/\Gamma_0} \prod_{\ell < \infty} O_\ell(\alpha, \mathbf{E}_1, \mathbf{E}_2) \\ &= \frac{\nu_{\mathfrak{p}}(\alpha)}{2} \sum_{x \in [\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})]/\Gamma_0} \rho(\alpha\mathfrak{D}\mathfrak{p}^{-1}) \\ &= \nu_{\mathfrak{p}}(\alpha) \cdot [\Gamma : \Gamma_0] \cdot \rho(\alpha\mathfrak{D}\mathfrak{p}^{-1}). \end{aligned}$$

Now use Proposition 2.14. □

2.7. **Final formula.** Throughout Section 2.7 we assume that $\gcd(d_1, d_2) = 1$. If $\mathfrak{b}$ is any fractional $\mathcal{O}_F$-ideal and p is a prime which is nonsplit in both K_1 and K_2 we set

$$f_p(\mathfrak{b}) = \sum_{\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}\mathfrak{p}) \cdot \rho(\mathfrak{b}\mathfrak{p}^{-1})$$

where the sum is over the primes $\mathfrak{p}$ of F above p. If p is a prime which splits in either K_1 or K_2 we set $f_p(\mathfrak{b}) = 0$. It is clear from the definition that $f_p(\mathfrak{b}) = 0$ unless $\mathfrak{b} \subset \mathcal{O}_F$.

Lemma 2.40. *For every fractional $\mathcal{O}_F$-ideal $\mathfrak{b}$ there is at most one p for which $f_p(\mathfrak{b}) \neq 0$.*

Proof. The hypothesis $\gcd(d_1, d_2) = 1$ implies that E/F is an unramified field extension, and that if p is a rational prime which is nonsplit in both K_1 and K_2 then every prime of F lying above p is inert in E. If p and q are primes for which $f_p(\mathfrak{b}) \neq 0$ and $f_q(\mathfrak{b}) \neq 0$ then there are primes $\mathfrak{p}$ and $\mathfrak{q}$ of F lying above p and q, respectively, such that

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}\mathfrak{p}) \cdot \rho(\mathfrak{b}\mathfrak{p}^{-1}) \neq 0 \qquad \mathrm{ord}_{\mathfrak{q}}(\mathfrak{b}\mathfrak{q}) \cdot \rho(\mathfrak{b}\mathfrak{q}^{-1}) \neq 0.$$

The condition $\rho(\mathfrak{b}\mathfrak{p}^{-1}) \neq 0$ implies that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b})$ is odd and that $\mathrm{ord}_{\mathfrak{q}}(\mathfrak{b}\mathfrak{p}^{-1})$ is even. Similarly the condition $\rho(\mathfrak{b}\mathfrak{q}^{-1}) \neq 0$ implies that $\mathrm{ord}_{\mathfrak{q}}(\mathfrak{b})$ is odd and that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{b}\mathfrak{q}^{-1})$ is even. The only way this can happen is if $\mathfrak{p} = \mathfrak{q}$. □

Definition 2.41. Suppose $\alpha \in F^\times$ and k is an algebraically closed field. For every $x \in \mathcal{X}_\alpha(k)$ abbreviate $e_x = |\mathrm{Aut}_{\mathcal{X}_\alpha(k)}(x)|$. Define the *Arakelov degree*

$$\deg(\mathcal{X}_\alpha) = \sum_p \log(p) \sum_{x \in [\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})]} e_x^{-1} \cdot \mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x})$$

where $\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}$ is the strictly Henselian local ring of $\mathcal{X}_\alpha$ at x. For $m \in \mathbb{Q}^\times$ we define $\deg(\mathcal{T}_m)$ similarly.

Proposition 2.42. *For every finite prime p and every totally positive $\alpha \in F^\times$*

$$\sum_{x \in [\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})]} e_x^{-1} \cdot \mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x}) = \frac{1}{2} \cdot f_p(\alpha\mathfrak{D}). \tag{2.34}$$

Proof. If p is split in either K_1 or K_2 then $\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ contains no supersingular points. On the other hand every point of $\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$ is supersingular by Corollary 2.8. We deduce that $[\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})] = \emptyset$ and both sides of (2.34) are zero. If p is inert in both K_1 and K_2 then (2.34) is a restatement of Proposition 2.29. If p is inert in K_1 and ramified in K_2 then (2.34) is a restatement of Proposition 2.39. If p is ramified in K_1 and inert in K_2 then we simply reverse the roles of K_1 and K_2: by Remark 2.4 the left hand side of (2.34) is unchanged if the fields K_1 and K_2 are interchanged, and it is clear that the same is true of the right hand side. □

Recall that χ is the quadratic Hecke character associated to the extension K/F and that $\mathrm{Diff}(\sqrt{D}, \alpha)$ is the set of all finite primes $\mathfrak{p}$ of F such that $\chi_{\mathfrak{p}}(\alpha\mathfrak{D}) = -1$.

Proposition 2.43. *If $\mathrm{Diff}(\sqrt{D}, \alpha) = \{\mathfrak{p}\}$ then $\mathcal{X}_\alpha$ is supported in characteristic $p = \mathbb{Z} \cap \mathfrak{p}$ and*

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

If $|\mathrm{Diff}(\sqrt{D}, \alpha)| \neq 1$ then $\mathcal{X}_\alpha = \emptyset$.

Proof. Suppose $\mathcal{X}_\alpha \neq \emptyset$ and let p be a rational prime for which $\mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}}) \neq \emptyset$. By Proposition 2.6 the stack $\mathcal{X}_\alpha$ is supported at a single prime p which is nonsplit in K_1 and K_2 and satisfies $\mathrm{Sppt}(\alpha) = \{p\}$. Proposition 2.42 gives

$$\deg(\mathcal{X}_\alpha) = \frac{1}{2} \log(p) \sum_{\mathfrak{p} | p} \mathrm{ord}_{\mathfrak{p}}(\alpha\mathfrak{D}\mathfrak{p}) \rho(\alpha\mathfrak{D}\mathfrak{p}^{-1}).$$

The proof of Lemma 2.40 shows that only one $\mathfrak{p}$ can contribute to the sum. As p is nonsplit in both K_1 and K_2 the prime $\mathfrak{p}$ is inert in K, and so satisfies $\chi_\mathfrak{p}(\mathfrak{p}) = -1$. But

$$\rho(\alpha\mathfrak{D}\mathfrak{p}^{-1}) \neq 0 \implies \chi_\mathfrak{p}(\alpha\mathfrak{D}\mathfrak{p}^{-1}) = 1 \implies \chi_\mathfrak{p}(\alpha\mathfrak{D}) = -1$$

proving that $\mathfrak{p} \in \mathrm{Diff}(\sqrt{D}, \alpha)$. Every prime $\mathfrak{q} \in \mathrm{Diff}(\sqrt{D}, \alpha)$ is inert in K and so satisfies $\chi_\mathfrak{q}(\mathfrak{q}) = -1$. If we let $\mathfrak{r}$ be the product of all primes in $\mathrm{Diff}(\sqrt{D}, \alpha)$ then $\chi_\mathfrak{q}(\alpha\mathfrak{D}\mathfrak{r}^{-1}) = 1$ for every prime $\mathfrak{q}$ of F, and so $\rho(\alpha\mathfrak{D}\mathfrak{r}^{-1}) \neq 0$. It now follows that

$$\chi_v(\alpha\mathfrak{D}\mathfrak{p}^{-1}) = 1 \qquad \chi_v(\alpha\mathfrak{D}\mathfrak{r}^{-1}) = 1$$

for every finite place v of F, and so $\chi_v(\mathfrak{r}\mathfrak{p}^{-1}) = 1$ for every finite place v. It follows that $\mathfrak{r} = \mathfrak{p}$ and hence $\mathrm{Diff}(\sqrt{D}, \alpha) = \{\mathfrak{p}\}$. □

Theorem 2.44. *For any totally positive $\alpha \in F^\times$ the stack $\mathcal{X}_\alpha$ has Arakelov degree*

$$\deg(\mathcal{X}_\alpha) = \frac{1}{2} \cdot \sum_p f_p(\alpha\mathfrak{D}) \log(p).$$

Proof. This is immediate from Proposition 2.42. □

Corollary 2.45. *For every $m \in \mathbb{Q}^\times$*

$$\deg(\mathcal{T}_m) = \frac{1}{2} \cdot \sum_{\substack{\alpha \in \mathfrak{D}^{-1} \\ \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) = m \\ \alpha \gg 0}} \sum_p f_p(\alpha\mathfrak{D}) \log(p).$$

Proof. This is immediate from Corollary 2.7, Theorem 2.44, and (2.2). □

3. Eisenstein Series

Throughout this section, we assume that $\gcd(d_1, d_2) = 1$. Let $\psi_\mathbb{Q} = \prod_p \psi_{\mathbb{Q}_p}$ be the 'canonical' unramified additive character of $\mathbb{Q}\backslash\mathbb{A}$ with $\psi_\mathbb{R}(x) = e(x) = e^{2\pi i x}$, and let $\psi_F = \psi_\mathbb{Q} \circ \mathrm{Tr}_{F/\mathbb{Q}}$. Let σ_1 and σ_2 be the two real embeddings of F. Let χ be the quadratic Hecke character of F associated to K.

Let $W = K$ with the F-quadratic form $Q(x) = \frac{1}{\sqrt{D}} x\bar{x}$. Let $\mathcal{C} = \otimes \mathcal{C}_v$ be the incoherent system of binary local F_v-quadratic spaces given by $\mathcal{C}_v = W_v$ for finite primes v of F, and $\mathcal{C}_{\sigma_i}$ is of signature $(2, 0)$ for the two infinite primes σ_1 and σ_2 of F. By means of the Weil representation $\omega = \omega_{\mathcal{C}, \psi_F}$, one has an $\mathrm{SL}_2(\mathbb{A}_F)$-equivariant map

$$\lambda : S(\mathcal{C}) = \otimes S(\mathcal{C}_v) \to I(0, \chi), \quad \lambda(\phi)(g) = \omega(g)\phi(0).$$

Here $I(s, \chi) = \mathrm{Ind}_{B(\mathbb{A}_F)}^{\mathrm{SL}_2(\mathbb{A}_F)}(\chi)$ is the induced representation on $\mathrm{SL}_2(\mathbb{A}_F)$ consisting of smooth functions $\Phi(g, s)$ satisfying

$$\Phi(n(b)m(a)g, s) = \chi(a)|a|_\mathbb{A}^{s+1} \Phi(g, s), \quad b \in \mathbb{A}_F, a \in \mathbb{A}_F^\times,$$

and

$$B = NM = \{n(b)m(a) = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : b \in F, a \in F^\times\}.$$

We say $\Phi \in I(s, \chi)$ is standard if $\Phi(g, s)$ is independent of s for g in the maximal compact subgroup $\mathrm{SL}_2(\widehat{\mathcal{O}}_F) \times \mathrm{SO}_2(F_\infty)$. We say Φ is factorizable if $\Phi = \otimes \Phi_v$ is the product of local sections. For a factorizable standard section $\Phi \in I(s, \chi)$, its Eisenstein series

$$E(g, s, \Phi) = \sum_{\gamma \in B(F)\backslash \mathrm{SL}_2(F)} \Phi(\gamma g, s)$$

is absolutely convergent when $\mathrm{Re}(s)$ is big and has meromorphic continuation with a functional equation for $s \mapsto -s$. Moreover, it is holomorphic at the unitary axis $\mathrm{Re}(s) = 0$.

For $\phi \in S(\mathcal{C})$, let $\Phi_\phi \in I(s, \chi)$ be the standard section associated to $\lambda(\phi)$, i.e., $\Phi_\phi(g, 0) = \lambda(\phi)$. Denote $E(g, s, \phi) = E(g, s, \Phi_\phi)$.

We take $\phi_v^+ = \mathbf{1}_{\mathcal{O}_{E_v}}$ for $v < \infty$, and $\phi_{\sigma_i}^+ = e^{-2\pi Q_{\sigma_i}(x)}$, where Q_{σ_i} is the quadratic form on $\mathcal{C}_{\sigma_i}$. We define $\phi^{\mathcal{C}} = \prod_v \phi_v^+ \in S(\mathcal{C})$. Let Φ_v^+ be the standard section associated to ϕ_v^+. The following is well-known, see for example [18].

Lemma 3.1.

(1) *For all s, $\Phi_{\sigma_i}^+(g, s)$ is the normalized eigenfunction of $\mathrm{SO}_2(F_{\sigma_i})$ of weight 1, i.e.,*

$$\Phi_{\sigma_i}^+(gk_\theta, s) = \Phi_{\sigma_i}^+(g, s) \cdot e^{i\theta}, \quad k_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \quad \Phi_{\sigma_i}^+(1) = 1.$$

(2) *For all s and all $v < \infty$, $\Phi_v^+(g, s)$ is the spherical section in $I(s, \chi_v)$, i.e,*

$$\Phi_v^+(gk, s) = \Phi_v^+(g, s), \quad k \in \mathrm{SL}_2(\mathcal{O}_{F_v}), \quad \Phi_v^+(1) = 1.$$

For $\tau = (\tau_1, \tau_2) \in \mathbb{H}^2$ set $g_{\tau_j} = n(u_j) \cdot m(\sqrt{v_j}) \in \mathrm{SL}_2(\mathbb{R})$, and view $g_\tau = (g_{\tau_1}, g_{\tau_2})$ as an element of $\mathrm{SL}_2(F_\infty) \subset \mathrm{SL}_2(\mathbb{A}_F)$. Let

$$E^*(\tau, s, \phi^{\mathcal{C}}) = \Lambda(s+1, \chi)(v_1 v_2)^{-\frac{1}{2}} E(g_\tau, s, \phi^{\mathcal{C}})$$

be the normalized Eisenstein series of weight 1, where

$$\Lambda(s, \chi) = D^{\frac{s}{2}} \Gamma_{\mathbb{R}}(s+1)^2 L(s, \chi) = \Lambda(s, \chi_1)\Lambda(s, \chi_2).$$

Here χ_j is the Dirichlet quadratic character associated to K_j,

$$\Gamma_{\mathbb{R}}(s) = \pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}),$$

and

$$\Lambda(s, \chi_j) = |d_j|^{\frac{s}{2}} \Gamma_{\mathbb{R}}(s+1) L(s, \chi_j).$$

This Eisenstein series is, up to scalar normalization, Hecke's famous Eisenstein series. Indeed, Lemma 3.1 together with the usual unfolding gives the following proposition.

Proposition 3.2. *One has*

$$E^*(\tau, s, \phi^{\mathcal{C}}) = D^{\frac{s+1}{2}} \Gamma_{\mathbb{R}}(s+2)^2 \sum_{[\mathfrak{a}] \in \mathrm{CL}(F)} \chi(\mathfrak{a}) \, \mathrm{N}(\mathfrak{a})^{1+s}$$
$$\cdot \sum_{(0,0) \neq (m,n) \in \mathfrak{a}^2/\mathcal{O}_F^\times} \frac{(v_1 v_2)^{\frac{s}{2}}}{(m(\tau_1, \tau_2) + n)|m(\tau_1, \tau_2) + n|^s}.$$

3.1. **Notation.** We first set up some notation. One has the Fourier expansion:

$$E^*(\tau, s, \phi^{\mathcal{C}}) = \sum_{\alpha \in F} E_\alpha^*(\tau, s, \phi^{\mathcal{C}}),$$

where for $\alpha \neq 0$

$$E_\alpha^*(\tau, s, \phi_0) = \prod_{v < \infty} W_{\alpha, v}^*(1, s, \phi_v^+) \prod_{i=1}^{2} W_{\alpha, \sigma_i}^*(\tau_i, s, \phi_{\sigma_i}^+),$$

and

$$E_0^*(\tau, s, \phi^{\mathcal{C}}) = \Lambda(s+1, \chi)(v_1 v_2)^{\frac{s}{2}} + \prod_{v<\infty} W_{0,v}^*(1, s, \phi_v^+) \prod_{i=1}^{2} W_{0,\sigma_i}^*(\tau_i, s, \phi_{\sigma_i}^+).$$

Here

$$\begin{aligned} W_{\alpha,v}^*(1, s, \phi_v^+) &= L(s+1, \chi_v)|D|_v^{-\frac{s+1}{2}} W_{\alpha,v}(1, s, \phi_v^+) \\ &= L(s+1, \chi_v)|D|_v^{-\frac{s+1}{2}} \int_{F_v} \Phi_v^+(wn(b), s)\psi_{F_v}(-\alpha_v b)\, db, \end{aligned}$$

where db is the Haar measure on F_v self-dual with respect to ψ_{F_v}. and

$$W_{\alpha,\sigma_j}^*(\tau_j, s, \phi_{\sigma_j}^+) = (v_1 v_2)^{-\frac{1}{2}} L_{\mathbb{R}}(s+1, \chi) W_{\alpha,\sigma_j}(g_{\tau_j}, s, \Phi_{\sigma_j}^+).$$

3.2. **Explicit Calculations.** We now record the following two propositions from [18, Propositions 2.1, 2.2] for the convenience of the reader.

Proposition 3.3. *Let v be a finite place of F.*

(1) *One has*

$$W_{\alpha,v}^*(1, s, \phi_v^+) = |D|_v^{-\frac{s}{2}} \mathbf{1}_{\mathfrak{D}^{-1}}(\alpha)\rho_v(\alpha\mathfrak{D}, s).$$

Here

$$\rho_v(\mathfrak{a}, s) = \sum_{r=0}^{\mathrm{ord}_v(\mathfrak{a})} (\chi_v(\pi_v) q_v^{-s})^r,$$

where π_v is a uniformizer of F_v and $q_v = |\pi_v|^{-1}$ is the cardinality of the residue field of v. In particular,

$$W_{0,v}^*(1, s, \phi_v^+) = |D|_v^{-\frac{s}{2}} L(s, \chi_v).$$

(2) *Let $\rho_v(\mathfrak{a}) = \rho_v(\mathfrak{a}, 0)$. One has for $\alpha \in \mathfrak{D}^{-1}$,*

$$W_{\alpha,v}^*(1, 0, \phi_v^+) = \rho_v(\alpha\mathfrak{D}).$$

It is zero if and only if $\chi_v(\alpha\sqrt{D}) = \chi_v(\alpha\mathfrak{D}) = -1$, i.e., K/F is inert at v and $\mathrm{ord}_v(\alpha\mathfrak{D})$ is odd. In such a case, one has

$$W_{\alpha,v}^{*,\prime}(1, 0, \phi_v^+) = -\frac{1}{2}(\mathrm{ord}_v(\alpha\mathfrak{D}) + 1) \log q_v.$$

Proof. (sketch) Let $\psi_v'(x) = \psi_{F_v}(\frac{1}{\sqrt{D}} x)$. Then ψ_v' is an unramified additive character of F_v. So

$$\begin{aligned} W_{\alpha,v}(g, s, \phi_v^+, \psi_{F_v}) &= \int_{F_v} \Phi_v^+(n(b)g, s)\psi_{F_v}(-\alpha b)\, d_{\psi_{F_v}} b \\ &= |D|^{\frac{1}{2}} \int_{F_v} \Phi_v^+(n(b)g, s)\psi_v(-\alpha\sqrt{D} b)\, d_{\psi_v'} b \\ &= |D|^{\frac{1}{2}} W_{\alpha\sqrt{D},v}(g, s, \Phi_v^+, \psi_v'). \end{aligned}$$

Here we add another variable ψ_v to indicate the dependence of the Whittaker function on the additive character, and $d_\psi b$ is the Haar measure with respect to ψ. Now the proposition follows from [18, Proposition 2.1]. □

Proposition 3.4. *(*[18, Proposition 2.4]*) For $\tau = u + iv$ in the upper half plane $\mathbb{H}$, let $g_\tau = n(u)m(\sqrt{v})$.*

(1) *One has*

$$W^*_{\alpha,\sigma_j}(\tau,0,\Phi^+_{\sigma_j}) = \begin{cases} -2ie(\sigma_j(\alpha)\tau_j) & \text{if} \sigma_j(\alpha) > 0, \\ -i & \text{if} \alpha = 0, \\ 0 & \text{if} \sigma_j(\alpha) < 0. \end{cases}$$

(2) *When* $\sigma_j(\alpha) < 0$, *one has*

$$W^{*,\prime}_{\alpha,\sigma_j}(\tau,0,\Phi^+_{\sigma_j}) = -ie(\sigma_j(\alpha)\tau_j)\beta_1(4\pi|\sigma_j(\alpha)|v_j),$$

where

$$\beta_1(x) = \int_1^\infty e^{-ux}\frac{du}{u} = -Ei(-x), \quad x > 0$$

is a partial Gamma function.

(3) *One has*

$$W^*_{0,\sigma_j}(\tau_j, s, \Phi^+_{\sigma_j}) = v_j^{-\frac{s}{2}}\Gamma_{\mathbb{R}}(s).$$

Define for every positive definite $\alpha \in F$

$$\mathrm{Diff}(\sqrt{D},\alpha) = \{ \text{ finite prime } v \text{ of } F : \chi_v(\alpha\sqrt{D}) = -1\}$$

Then

$$\mathrm{Diff}(\sqrt{D},\alpha) \cup \{\sigma_2\} = \mathrm{Diff}(\mathcal{C},\alpha)$$

is the Diff set first defined by Kudla in [7]. For an ideal of $\mathfrak{a}$ of F, define

$$\rho(\mathfrak{a}) = \#\{\mathfrak{A} \subset \mathcal{O}_K : \mathrm{N}_{K/F}(\mathfrak{A}) = \mathfrak{a}\}.$$

It is easy to see that

$$\rho(\mathfrak{a}) = \prod_{v<\infty} \rho_v(\mathfrak{a}).$$

Simple calculation using the above propositions gives the following theorem (see also [3, Page 215]).

Theorem 3.5. *One has* $E^*(\tau,0,\phi^{\mathcal{C}}) = 0$, *and*

$$E^{*,\prime}(\tau,0,\phi^{\mathcal{C}}) = \sum_{\alpha\in\mathfrak{D}^{-1}} a_\alpha(v)q^\alpha$$

where $q^\alpha = e(\sigma_1(\alpha)\tau_1 + \sigma_2(\alpha)\tau_2)$, *and* $a_\alpha(v)$ *are given as follows.*

(1) *When* α *is totally positive, there is* $v_0 \in \mathrm{Diff}(\sqrt{D},\alpha)$, *and* $a_\alpha = a_\alpha(v)$ *is independent of the imaginary part* v *of* τ*:*

$$a_\alpha = 2(\mathrm{ord}_{v_0}(\alpha\mathfrak{D}) + 1)\rho(\alpha\mathfrak{D}\mathfrak{p}_{v_0}^{-1})\log p,$$

where $\mathfrak{p}_{v_0}$ *is the prime ideal of* F *associated to* v_0, *and* p *is the rational prime below* $\mathfrak{p}_0$.

(2) *When* $\sigma_i(\alpha) > 0 > \sigma_j(\alpha)$ *with* $\{i,j\} = \{1,2\}$, *one has*

$$a_\alpha(v) = 2\rho(\alpha\mathfrak{D})\beta_1(4\pi|\sigma_j(\alpha)|v_j).$$

(3) *The constant term is*

$$a_0(v) = 2\Lambda(0,\chi)\left(-\frac{\Lambda'(0,\chi)}{\Lambda(0,\chi)} + \frac{1}{2}\log(v_1v_2)\right).$$

(4) *When* α *is totally negative,* $a_\alpha(v) = 0$.

3.3. **A conceptional proof of Theorem 1.3.** In this subsection we rephrase the proof of Theorem 1.3 in a more structured way. Since $\gcd(d_1, d_2) = 1$, every finite prime of F is unramified in E.

For a finite prime v of F inert in K, let W_v^- be the binary quadratic space K_v over F_v with quadratic form

$$Q_v^-(x) = \frac{\pi_v}{\sqrt{D}} x\bar{x},$$

where π_v is a uniformizer of F_v, and denote $W_v^+ = W_v$ for convenience. Let $(W^{(v)}, Q^{(v)})$ be the global F-quadratic space obtained from $\mathcal{C}$ by changing $\mathcal{C}_v = W_v^+$ to W_v^- and leaving other local quadratic spaces $\mathcal{C}_{v'}$ unchanged.

Let $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ be such that both $\mathbf{E}_i$ are supersingular. If p is split in F, we defined the reflex prime of $(\mathbf{E}_1, \mathbf{E}_2)$ at the beginning of Section 2.5. When p is nonsplit in F, we simply call the prime of F above p the reflex prime of $(\mathbf{E}_1, \mathbf{E}_2)$ for convenience.

Lemma 3.6.

(1) *Let $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ be such that both $\mathbf{E}_i$ are supersingular, and let v be the reflex prime of $(\mathbf{E}_1, \mathbf{E}_2)$. Then there is an isomorphism of $F \otimes \mathbb{A}_f$-quadratic spaces*

$$(V(\mathbf{E}_1, \mathbf{E}_2) \otimes \mathbb{A}_f, \deg_{\mathrm{CM}}) \cong (W^{(v)} \otimes \mathbb{A}_f, Q^{(v)})$$

which maps $L(\mathbf{E}_1, \mathbf{E}_2) \otimes \widehat{\mathbb{Z}}$ onto $\widehat{\mathcal{O}}_K$. In particular, there is an isomorphism between the F-quadratic space between $V(\mathbf{E}_1, \mathbf{E}_2)$ and $W^{(v)}$.

(2) *If $(\mathbf{E}_1, \mathbf{E}_2, j) \in \mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$, then $\mathrm{Diff}(\sqrt{D}, \alpha) = \{v\}$, where v is the prime of F above p and is the reflex prime of $(\mathbf{E}_1, \mathbf{E}_2)$. In particular, if $|\mathrm{Diff}(\sqrt{D}, \alpha)| > 1$, then $\mathcal{X}_\alpha$ is empty.*

Proof. By Lemma 2.16, one sees for $l \neq p$

$$L(\mathbf{E}_1, \mathbf{E}_2) \otimes \mathbb{Z}_l \cong (\mathcal{O}_{K_l}, Q_l^{(v)}).$$

For $l = p$, there are two cases.

Case 1: p is inert in K_1 and K_2. In this case, $p = vv'$ is split in F with v chosen to be the reflex prime of $(\mathbf{E}_1, \mathbf{E}_2)$. Then Proposition 2.22 asserts

$$L(\mathbf{E}_1, \mathbf{E}_2) \otimes \mathbb{Z}_p \cong (\mathcal{O}_{K_v}, \pi_v \mathrm{N}_{K_v/F_v}) \times (\mathcal{O}_{K_{v'}}, \mathrm{N}_{K_{v'}/F_{v'}}) \cong (\mathcal{O}_{K_p}, Q_p^{(v)}).$$

Case 2: p is inert in one of K_i and ramified in the other. In this case, $p = v^2$ is ramified in F, and K/F is still unramified at v. We still call v the reflex prime of $(\mathbf{E}_1, \mathbf{E}_2)$ for convenience. By Proposition 2.32, one sees that

$$L(\mathbf{E}_1, \mathbf{E}_2) \otimes \mathbb{Z}_p \cong (\mathcal{O}_{K_v}, \mathrm{N}_{K_v/F_v}) \cong (\mathcal{O}_{K_v}, Q_v^{(v)}).$$

This proves (1).

Next, $(\mathbf{E}_1, \mathbf{E}_2, j) \in \mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$ implies that there is a $j \in L(\mathbf{E}_1, \mathbf{E}_2)$ with $\deg_{\mathrm{CM}}(j) = \alpha$. By (2), one has then that there is $z \in \widehat{K}$ such that $Q^{(v)}(z) = \alpha$. This implies that $\mathrm{Diff}(\sqrt{D}, \alpha) = \{v\}$. □

Now we assume that $\alpha \in F$ is totally positive and $\mathrm{Diff}(\sqrt{D}, \alpha) = \{v\}$. Fix one $(\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ with reflex prime v, which always exists by Corollary 2.27. We identify $V(\mathbf{E}_1, \mathbf{E}_2)$ with $W^{(v)}$ so that $\deg_{\mathrm{CM}} = Q^{(v)}$. Moreover, there is $h_0 \in S(\mathbb{A}_f)$

such that $h_0 L(\mathbf{E}_1, \mathbf{E}_2) \otimes \widehat{\mathbb{Z}} = \widehat{\mathcal{O}}_K$. Write $\phi_{\mathbf{E}_1,\mathbf{E}_2} = \mathbf{1}_{(L(\mathbf{E}_1,\mathbf{E}_2)\otimes\widehat{\mathbb{Z}})}$ and $\phi_f^{(v)} = \mathbf{1}_{\widehat{\mathcal{O}}_K}$. Then $\phi_{\mathbf{E}_1,\mathbf{E}_2}(x) = \phi_f^{(v)}(h_0^{-1}x)$. Let

$$\phi^{(v)} = \phi_f^{(v)} \phi_{\sigma_1}^+ \phi_{\sigma_2}^+ \in S(W^{(v)}(\mathbb{A})),$$

and let

$$\theta(g, \phi^{(v)}) = \int_{S(\mathbb{Q})\backslash S(\mathbb{A})} \theta(g, h, \phi^{(v)})\, dh$$

be the associated theta integral. Here

$$\theta(g, h, \phi^{(v)}) = \sum_{j \in W^{(v)}} \omega_{W^{(v)},\psi_F}(g) \phi^{(v)}(h^{-1}x)$$

is the theta kernel, $S = \mathrm{Res}_{F/\mathbb{Q}} \mathrm{SO}(W^{(v)}) = \mathrm{Res}_{F/\mathbb{Q}} K^1$ is the algebraic group defined in Section 2.3, dh is the Tamagama measure on $S(\mathbb{A})$ so that $\mathrm{Vol}(S(\mathbb{R})) = 1$ and $\mathrm{Vol}(S(\mathbb{Q})\backslash S(\mathbb{A}_f)) = 2$ (see for example [16]). We further write for $\tau \in \mathbb{H}^2$

$$\theta(\tau, \phi^{(v)}) = (v_1 v_2)^{-\frac{1}{2}} \theta(g_\tau, \phi^{(v)}),$$

which is a weight 1 Hilbert modular form. It has the Fourier expansion

$$\theta(\tau, \phi^{(v)}) = \sum_{\alpha} \theta_\alpha(\phi^{(v)}) \cdot q^\alpha$$

with

$$\theta_\alpha(\phi^{(v)}) = \int_{S(\mathbb{Q})\backslash S(\mathbb{A}_f)} \sum_{\substack{j \in W^{(v)} \\ Q^{(v)}(j) = \alpha}} \phi_f(h^{-1}j)\, dh.$$

Recall that $T(\mathbb{A}_f) = \{t = (t_1, t_2) \in \widehat{K}_1^\times \times \widehat{K}_2^\times : t_1 \bar{t}_1 = t_2 \bar{t}_2\}$ acts on $\mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ via

$$t.(\mathbf{E}_1, \mathbf{E}_2) = (\mathbf{E}_1 \otimes \mathfrak{a}_1, \mathbf{E}_2 \otimes \mathfrak{a}_2)$$

where $\mathfrak{a}_i \widehat{\mathcal{O}}_{K_i} = t_i \widehat{\mathcal{O}}_{K_i}$. The group T also acts on $V(\mathbf{E}_1, \mathbf{E}_2)$ via

$$(t_1, t_2) \bullet j = \frac{1}{t_1 \bar{t}_1} \kappa(t_2) \circ j \circ \kappa(\bar{t}_1).$$

This action factors through S (acting on $W^{(v)}$), and gives the exact sequence

$$1 \to \mathbb{G}_m \to T \to S \to 1.$$

Moreover, one has for $t \in T(\mathbb{A}_f)$

$$L(t.(\mathbf{E}_1, \mathbf{E}_2)) = t \bullet L(\mathbf{E}_1, \mathbf{E}_2).$$

Here

$$t \bullet L(\mathbf{E}_1, \mathbf{E}_2) = V(\mathbf{E}_1, \mathbf{E}_2) \cap \{t \bullet j : j \in L(\mathbf{E}_1, \mathbf{E}_2) \otimes \widehat{\mathbb{Z}}\}$$

Lemma 3.7. *Assume* $\mathrm{Diff}(\sqrt{D}, \alpha) = \{v\}$*, and* $x = (\mathbf{E}_1, \mathbf{E}_2) \in \mathcal{X}(\mathbb{F}_p^{\mathrm{alg}})$ *with reflex prime* v*. Then*

$$\sum_{t \in \Gamma_0} \sum_{j \in L(t.x)} \frac{1}{|\mathrm{Aut}_{\mathcal{X}_\alpha}(t.x, j)|} = \frac{h_1 h_2}{2 \mathbf{w}_1 \mathbf{w}_2} \theta_\alpha(\phi^{(v)}).$$

Here $\Gamma_0 = T(\mathbb{Q})\backslash T(\mathbb{A}_f)/U$ *has (by Proposition 2.14) cardinality* $h_1 h_2$*, where* h_i *is the ideal class number of* K_i*.*

Proof. Notice that $\phi^{(v)}$ is U-invariant. Recall the exact sequence

$$1 \to \mathbb{Q}^\times\backslash\mathbb{A}_f^\times \to T(\mathbb{Q})\backslash T(\mathbb{A}_f) \to S(\mathbb{Q})\backslash S(\mathbb{A}_f) \to 1,$$

$\mathrm{Vol}(\mathbb{Q}^\times\backslash\mathbb{A}_f^\times) = \frac{1}{2}$, and $W^{(v)} \cong V(\mathbf{E}_1, \mathbf{E}_2)$. So we have

$$\begin{aligned} \theta_\alpha(\phi^{(v)}) &= \int_{S(\mathbb{Q})\backslash S(\mathbb{A}_f)} \sum_{\substack{z\in V^{(v)} \\ Q^{(v)}(z)=\alpha}} \phi_f^{(v)}(h^{-1}z)\, dh \\ &= \int_{S(\mathbb{Q})\backslash S(\mathbb{A}_f)} \sum_{\substack{j\in V(x) \\ \deg_{\mathrm{CM}}(j)=\alpha}} \phi_{\mathbf{E}_1,\mathbf{E}_2}(h^{-1}\bullet j)\, dh \\ &= 2\int_{T(\mathbb{Q})\backslash T(\mathbb{A}_f)} \sum_{\substack{j\in V(x) \\ \deg_{\mathrm{CM}}(j)=\alpha}} \phi_{\mathbf{E}_1,\mathbf{E}_2}(t^{-1}\bullet j)\, dt \\ &= 2\frac{\mathrm{Vol}(U)}{|U\cap T(\mathbb{Q})|} \sum_{t\in\Gamma_0} \sum_{\substack{j\in V(x) \\ \deg_{\mathrm{CM}}(j)=\alpha}} \phi^{(v)}_{\mathbf{E}_1,\mathbf{E}_2}(t^{-1}\bullet j). \end{aligned}$$

Notice that $\phi_{\mathbf{E}_1,\mathbf{E}_2}(t^{-1}\bullet j) = 0$ or 1. It is 1 if and only if $t^{-1}\bullet j \in L(\mathbf{E}_1,\mathbf{E}_2)\otimes\widehat{\mathbb{Z}}$, i.e.,

$$j \in (t\bullet L(\mathbf{E}_1,\mathbf{E}_2)\otimes\widehat{\mathbb{Z}}) \cap V(\mathbf{E}_1,\mathbf{E}_2) = L(t.(\mathbf{E}_1,\mathbf{E}_2)).$$

Since $|\mathrm{Aut}_{\mathcal{X}_\alpha}(t.(\mathbf{E}_1,\mathbf{E}_2), j)| = \mathbf{w}_1\mathbf{w}_2$, one sees

$$\theta_\alpha(\phi^{(v)}) = 2\mathbf{w}_1\mathbf{w}_2\frac{\mathrm{Vol}(U)}{|U\cap T(\mathbb{Q})|} \sum_{t\in\Gamma_0} \sum_{\substack{j\in L(t.x) \\ \deg_{\mathrm{CM}}(j)=\alpha}} \frac{1}{|\mathrm{Aut}_{\mathcal{X}_\alpha}(t.x, j)|}.$$

Finally,

$$\mathrm{Vol}(T(\mathbb{Q})\backslash T(\mathbb{A}_f)) = \mathrm{Vol}(\mathbb{Q}^\times\backslash\mathbb{A}_f^\times)\cdot\mathrm{Vol}(S(\mathbb{Q})\backslash S(\mathbb{A}_f)) = 1$$

implies

$$1 = \frac{\mathrm{Vol}(U)}{|U\cap T(\mathbb{Q})|}\sum_{t\in\Gamma_0} 1.$$

So

$$\frac{\mathrm{Vol}(U)}{|U\cap T(\mathbb{Q})|} = \frac{1}{|\Gamma_0|} = \frac{1}{h_1h_2}$$

by Proposition 2.14. □

We also summarize Propositions 2.28 and 2.38 as the following theorem.

Theorem 3.8. *If $x = (\mathbf{E}_1,\mathbf{E}_2, j) \in \mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$, then $\mathrm{Diff}(\sqrt{D},\alpha) = \{v\}$ consists of a single element v, and v is the reflex prime of $(\mathbf{E}_1,\mathbf{E}_2)$. Furthermore,*

$$\mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha,x}) = \frac{1}{2}(\mathrm{ord}_v(\alpha\mathfrak{D}) + 1)$$

is independent of choice of x!

Proof. Suppose $x = (\mathbf{E}_1,\mathbf{E}_2, j) \in \mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$, then $j \in L(\mathbf{E}_1,\mathbf{E}_2)$ with $\deg_{\mathrm{CM}}(j) = \alpha$. Lemma 2.16 implies that for all $\ell \neq p$, $V_\ell(\mathbf{E}_1,\mathbf{E}_2)$ is isomorphic to $\mathcal{C}_\ell = \prod_{v|\ell}\mathcal{C}_v$ as F'_ℓ-quadratic spaces. So C_v represents α for all $v \nmid p$, i.e., $v \notin \mathrm{Diff}(\sqrt{D},\alpha)$. If $p = v^2$ is ramified in F, then $V_v(\mathbf{E}_1,\mathbf{E}_2)$ is not isomorphic to $\mathcal{C}_v$, otherwise $\mathcal{C}$ is isomorphic to $V(\mathbf{E}_1, \mathbf{E}_2)$ and is thus coherent. When $p = v_1 v_2$ is split, the same argument implies that for exactly one of v_i, the two local F_{v_i}-quadratic spaces are isomorphic, so $\mathrm{Diff}(\sqrt{D}, \alpha)$ consists of exactly one element. To see that v is the reflex of $(\mathbf{E}_1, \mathbf{E}_2)$, one uses Proposition 2.22. The formula for $\mathrm{length}(\mathcal{O}^{\mathrm{sh}}_{\mathcal{X}_\alpha, x})$ is given by Propositions 2.28 and 2.38.

□

Proposition 3.9. *Assume that $\alpha \in F$ is totally positive with* $\mathrm{Diff}(\sqrt{D}, \alpha) = \{v\}$

$$\deg(\mathcal{X}_\alpha) = \frac{h_1 h_2}{2\mathbf{w}_1 \mathbf{w}_2} (\mathrm{ord}_v(\alpha \mathfrak{D}) + 1) \theta_\alpha(\phi^{(v)}).$$

In particular, $\deg(\mathcal{X}_\alpha) = 0$ *if* $\alpha \notin \mathfrak{D}^{-1}$.

Proof. When $\alpha \notin \mathfrak{D}^{-1}$, $\theta_\alpha(\phi^{(v)}) = 0$ and $\mathcal{X}_\alpha$ is empty by Lemma 3.7. When $\alpha \in \mathfrak{D}^{-1}$, $\theta_\alpha(\phi^{(v)}) \neq 0$ if and only if $\mathcal{X}_\alpha$ is not empty. Suppose $x = (\mathbf{E}_1, \mathbf{E}_2, j) \in \mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$, then the reflex prime of $(\mathbf{E}_1, \mathbf{E}_2)$ is v and p lies below v by Theorem 3.8. Notice in general that $x = (\mathbf{E}_1, \mathbf{E}_2, j) \in \mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$ implies that $\bar{x} = (\bar{\mathbf{E}}_1, \bar{\mathbf{E}}_2, j) \in \mathcal{X}_\alpha(\mathbb{F}_p^{\mathrm{alg}})$, where $\bar{\mathbf{E}}_j$ is the same elliptic curve with the $\mathcal{O}_{K_j}$-action $\bar{\kappa}_j(a) = \kappa_j(\bar{a})$. Moreover, $\bar{x}$ and x are not in the same Γ-orbit. So Theorem 3.8 and Corollaries 2.27 and 2.37 imply

$$\deg(\mathcal{X}_\alpha) = (\mathrm{ord}_v(\alpha \mathfrak{D}) + 1) \sum_{t \in \Gamma} \sum_{\substack{j' \in L(t.(\mathbf{E}_1, \mathbf{E}_2)) \\ \deg_{\mathrm{CM}}(j') = \alpha}} \frac{1}{|\mathrm{Aut}(t.(\mathbf{E}_1, \mathbf{E}_2), j')|}.$$

Since $\gcd(d_1, d_2) = 1$, $\Gamma_0 = \Gamma$ by Proposition 2.14. So Lemma 3.7 implies the Proposition. □

One the one hand, one has by [18, Lemma 2.2]

Lemma 3.10. *Let v be a finite place of F. Then $W^*_{\alpha,v}(1, 0, \phi_v^-) = 0$ unless $\alpha \in \mathfrak{D}^{-1} \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v}$. In such a case, one has*

$$W^*_{\alpha,v}(1, 0, \phi_v^-) = \begin{cases} -1 & \text{if } \mathrm{ord}_v(\alpha \mathfrak{D}) \equiv 1 \pmod 2, \\ 0 & \text{if } \mathrm{ord}_v(\alpha \mathfrak{D}) \equiv 0 \pmod 2. \end{cases}$$

Lemma 3.11. *Assume $\alpha \in \mathfrak{D}^{-1}$ is totally positive, and* $\mathrm{Diff}(\sqrt{D}, \alpha) = \{v\}$. *Then*

$$E^{*,\prime}_\alpha(\tau, 0, \phi^{\mathcal{C}}) = \frac{W^{*,\prime}_{\alpha,v}(1, 0, \phi_v^+)}{W^*_{\alpha,v}(1, 0, \phi_v^-)} E^*_\alpha(\tau, 0, \phi^{(v)}).$$

When $\alpha \notin \mathfrak{D}^{-1}$, one has $E^{*,\prime}_\alpha(\tau, 0, \phi^{\mathcal{C}}) = 0$.

Proof. The condition $\mathrm{Diff}(\sqrt{D}, \alpha) = \{v\}$ implies that $\mathrm{ord}_v(\alpha \mathfrak{D})$ is odd and

$$\begin{aligned} W^*_{\alpha,v}(1, 0, \phi_v^+) &= 0 \\ W^*_{\alpha,v}(1, 0, \phi_v^-) &= -1. \end{aligned}$$

Therefore

$$\begin{aligned} E^{*,\prime}_\alpha(\tau, 0, \phi^{\mathcal{C}}) &= \frac{W^{*,\prime}_{\alpha,v}(1, 0, \phi_v^+)}{W^*_{\alpha,v}(1, 0, \phi_v^-)} W^*_{\alpha,v}(1, 0, \phi_v^-) \prod_{w \nmid v\infty} W^*_{\alpha,w}(1, 0, \phi_w^+) \prod_{w \mid \infty} W^*_{\alpha,w}(\tau, 0, \phi_w^+) \\ &= \frac{W^{*,\prime}_{\alpha,v}(1, 0, \phi_v^+)}{W^*_{\alpha,v}(1, 0, \phi_v^-)} E^*_\alpha(\tau, 0, \phi^{(v)}). \end{aligned}$$

□

Looking at Lemma 3.11 and Proposition 3.9, one sees that to prove Theorem 1.3, it is sufficient to prove

Proposition 3.12. *Assume* $\alpha \in \mathfrak{D}^{-1}$ *is totally positive, and* $\mathrm{Diff}(\sqrt{D}, \alpha) = \{v\}$. *Let* p *be the prime below* v. *Then*

(1) *One has*

$$\frac{W^{*,\prime}_{\alpha,v}(1,0,\phi_v^+)}{W^*_{\alpha,v}(1,0,\phi_v^-)} = \frac{1}{2}(\mathrm{ord}_v(\alpha\mathfrak{D}) + 1).$$

(2) *One has*

$$E^*(\tau, 0, \phi^{(v)}) = \frac{4h_1h_2}{\mathbf{w}_1\mathbf{w}_2}\theta(\tau, \phi^{(v)}).$$

Proof. Part (1) follows from Proposition 3.3 and Lemma 3.10. Part (2) is the well-known Siegel-Weil formula. Indeed, the Siegel-Weil formula [15] gives

$$E^*(\tau, 0, \phi^{(v)}) = \Lambda(1, \chi)E(\tau, 0, \phi^{(v)}) = \Lambda(0, \chi)\theta(\tau, \phi^{(v)}).$$

On the other hand, the class number formula gives

$$\Lambda(0, \chi) = \Lambda(0, \chi_1)\Lambda(0, \chi_2) = \frac{4h_1h_2}{\mathbf{w}_1\mathbf{w}_2}.$$

□

References

[1] B. Conrad. Gross-Zagier revisited. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 67–163. Cambridge Univ. Press, Cambridge, 2004. With an appendix by W. R. Mann.

[2] B. Gross. On canonical and quasicanonical liftings. *Invent. Math.*, 84(2):321–326, 1986.

[3] B. Gross and D. Zagier. On singular moduli. *J. Reine Angew. Math.*, 355:191–220, 1985.

[4] B. Gross and D. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[5] H. Hida. *p-adic automorphic forms on Shimura varieties.* Springer Monographs in Mathematics. Springer-Verlag, New York, 2004.

[6] M. Knus. *Quadratic and Hermitian forms over rings*, volume 294 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1991. With a foreword by I. Bertuccioni.

[7] S. Kudla. Central derivatives of Eisenstein series and height pairings. *Ann. of Math. (2)* 146 (1997), 545–646.

[8] S. Kudla. Special cycles and derivatives of Eisenstein series, in Heegner points and Rankin L-series, 243-270, *Math. Sci. Res. Inst. Publ., 49*, Cambridge Univ. Press, Cambridge, 2004.

[9] S. Kudla, M. Rapoport, and T.H. Yang. Modular forms and special cycles on Shimura curves, *Annals of Mathematics Sutdies Series 161*, Princeton University Press, 2006.

[10] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2000.

[11] M. Rapoport and Th. Zink. *Period spaces for p-divisible groups*, volume 141 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1996.

[12] J.-P. Serre. *A Course in Arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[13] E. Viehmann and K. Ziegler. Formal moduli of formal $\mathcal{O}_{\mathrm{K}}$-modules. *Astérisque*, (312):57–66, 2007.

[14] A. Vistoli. Intersection theory on algebraic stacks and on their moduli spaces. *Invent. Math.*, 97(3):613–670, 1989.

[15] A. Weil. Sur la formule de Siegel dans la théorie des groupes classiques *Acta. Math.*, (123): 1–87, 1965.
[16] A, Weil. Adeles and algebraic groups. With appendices by M. Demazure and Takashi Ono. Progress in Mathematics, 23. Birkhuser, Boston, Mass., 1982.
[17] S. Wewers. Canonical and quasi-canonical liftings. *Astérisque*, (312):67–86, 2007.
[18] T. H. Yang. CM number fields and modular forms, Quarterly Jour. *Pure Appl. Math. special issue in memory of A. Borel* 1(2005), 305-340
[19] T. H. Yang. An arithmetic intersection formula on Hilbert modular surface. *To appear in Amer. J. Math.*, pp32.

Department of Mathematics, Boston College, Chestnut Hill, MA, 02467
E-mail address: howardbe@bc.edu

Department of Mathematics, University of Wisconsin Madison, Van Vleck Hall, Madison, WI 53706, USA
E-mail address: thyang@math.wisc.edu