Algebra & Number Theory

Volume 7

2013

No. 6

A Gross–Zagier formula for quaternion algebras over totally real fields

Eyal Z. Goren and Kristin E. Lauter

msp

ALGEBRA AND NUMBER THEORY 7:6 (2013)
dx.doi.org/10.2140/ant.2013.7.1405

A Gross–Zagier formula for quaternion algebras over totally real fields

Eyal Z. Goren and Kristin E. Lauter

We prove a higher dimensional generalization of Gross and Zagier's theorem on the factorization of differences of singular moduli. Their result is proved by giving a counting formula for the number of isomorphisms between elliptic curves with complex multiplication by two different imaginary quadratic fields K and K' when the curves are reduced modulo a supersingular prime and its powers. Equivalently, the Gross–Zagier formula counts optimal embeddings of the ring of integers of an imaginary quadratic field into particular maximal orders in $B_{p,\infty}$, the definite quaternion algebra over $\mathbb{Q}$ ramified only at p and infinity. Our work gives an analogous counting formula for the number of simultaneous embeddings of the rings of integers of primitive CM fields into superspecial orders in definite quaternion algebras over totally real fields of strict class number 1. Our results can also be viewed as a counting formula for the number of isomorphisms modulo $\mathfrak{p} \mid p$ between abelian varieties with CM by different fields. Our counting formula can also be used to determine which superspecial primes appear in the factorizations of differences of values of Siegel modular functions at CM points associated to two different CM fields and to give a bound on those supersingular primes that can appear. In the special case of Jacobians of genus-2 curves, this provides information about the factorizations of numerators of Igusa invariants and so is also relevant to the problem of constructing genus-2 curves for use in cryptography.

1. Introduction

The celebrated theorem of Gross and Zagier [1985] gives a factorization of norms of differences of singular moduli: values of the modular j-function evaluated at CM points associated to imaginary quadratic fields. Let K and K' be two imaginary quadratic fields with relatively prime fundamental discriminants d and d'. For τ and τ' running through equivalence classes of imaginary quadratic integers in the upper half-plane modulo $\mathrm{SL}_2(\mathbb{Z})$ with $\mathrm{disc}(\tau) = d$, $\mathrm{disc}(\tau') = d'$, and w and w'

MSC2010: primary 11G15, 11G16; secondary 11G18, 11R27.
Keywords: CM abelian varieties, singular moduli, quaternion algebras, superspecial orders.

equal to the number of roots of unity in K and K', respectively, define

$$J(d,d') = \left(\prod_{[\tau],[\tau']} (j(\tau) - j(\tau')) \right)^{4/(ww')}.$$

Then the Gross–Zagier thereom states that if λ is a prime of $\mathbb{O}_K$ of characteristic p,

$$\operatorname{ord}_\lambda J(d,d') = \frac{1}{2} \sum_{x\in\mathbb{Z}} \sum_{n\geq 1} \delta(x) R\left(\frac{dd'-x^2}{4p^n} \right),$$

where $R(m)$ is the number of ideals of $\mathbb{O}_K$ of norm m and $\delta(x) = 1$ unless x is divisible by d, in which case it is 2. Their results can also be viewed as a counting formula for the number of isomorphisms between the reductions modulo primes and their powers of elliptic curves with complex multiplication by two different imaginary quadratic fields K and K'. This in turn is equivalent to counting optimal embeddings of the ring of integers of an imaginary quadratic field into particular maximal orders in $B_{p,\infty}$, the definite quaternion algebra over $\mathbb{Q}$ ramified only at p and infinity. Gross and Zagier gave an algebraic proof of this result under the additional assumption that d is prime, and the algebraic proof of the theorem was extended to arbitrary fundamental, relatively prime discriminants in a series of papers by Dorman [1988; 1989a; 1989b].

In this paper, we prove a generalization to higher dimensions of Gross and Zagier's theorem, which can also be viewed in three ways: (1) a statement about primes in the factorization of differences of values of Siegel modular functions at CM points associated to two different CM fields, (2) a counting formula for isomorphisms modulo p between abelian varieties with CM by different fields, and (3) a counting formula for simultaneous embeddings of the rings of integers of two primitive CM fields into superspecial orders in certain definite quaternion algebras over a totally real field.

First we explain our interest in these three contexts. Assume throughout that K and K' are primitive CM fields with a common totally real subfield $K^+ = K'^+ = L$ and $[L:\mathbb{Q}] = g$, where L has strict class number 1. In the special case of $g = 2$, we are inspired by some concrete calculations of values of certain Siegel modular functions at CM points associated to primitive quartic CM fields. Let C and C' be two genus-2 curves whose Jacobians J and J' have complex multiplication (CM) by K and K'. In analogy with the modular j-invariant for elliptic curves, for genus-2 curves Igusa defined ten modular invariants. Equality of these ten invariants determines whether two curves are isomorphic geometrically, so primes appearing in the factorization of all ten differences correspond to primes where the curves become isomorphic when reduced modulo that prime. Concrete calculations and the tables of van Wamelen [1999] suggest that such primes are "small". An explicit

characterization of such primes gives information about the numerators of Igusa invariants and thus has some value computationally as well.

Thus, we are led to be interested in counting the number of isomorphisms modulo various primes and their powers between abelian varieties with CM by two different CM fields K and K'. The existence of an isomorphism modulo p between abelian varieties with CM by two different CM fields K and K' with $K^+ = K'^+$ implies supersingular reduction modulo p. Fixing an abelian variety A with CM by K, each isomorphism modulo p with an abelian variety A' with CM by K' gives an embedding of $\mathcal{O}_{K'}$ into $\mathrm{End}_{\mathcal{O}_L}(A)$. In the case of superspecial reduction, we can give a very explicit description of the orders $\mathrm{End}_{\mathcal{O}_L}(A)$, which allows us to derive a formula that counts such embeddings.

Nicole introduced the notion of superspecial orders in definite quaternion algebras over totally real fields as a generalization of maximal orders in definite quaternion algebras over $\mathbb{Q}$; see [Nicole 2005; 2008]. These orders were further studied in [Charles et al. 2009a; 2009b; Goren and Lauter 2009], where related Ramanujan graphs were constructed and certain cryptographic applications suggested. Throughout this paper, assume that p is a prime number that is unramified in the totally real field L of degree g and strict class number $h^+(L) = 1$. Under these assumptions, a *superspecial order* in $B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L$ is an Eichler order of level p. The connection with geometry is given in the thesis of Nicole, where it is shown that $\mathrm{End}_{\mathcal{O}_L}(A)$ is a superspecial order for A a principally polarized superspecial abelian variety with RM over $\bar{\mathbb{F}}_p$. Conversely, every superspecial order arises in this way from such an abelian variety A.

Next we give an overview of the results of the paper. The core of the paper is the generalization of Dorman's work constructing and classifying superspecial orders in $B_{p,L}$ with an optimal embedding of a CM number field K with $K^+ = L$. First, Section 3 is devoted to giving a description of the quaternion algebra $B_{p,L}$ with a fixed embedding of the CM field K for *superspecial primes*, i.e., unramified primes p such that an abelian variety with CM by K has superspecial reduction modulo a prime $\mathfrak{P} \mid p$ in a field of definition of the abelian variety. Sections 4 and 5 establish a classification of superspecial orders with an optimal embedding of K, giving both an explicit construction of all such superspecial orders and a bijection (up to conjugation by elements of $K^\times$) with the class group of K (Theorem 5.7). These three sections together establish the generalization to $g > 1$ of Dorman's work on orders [1989a] and fix several gaps in his proofs.

Section 6 gives a method for counting embeddings by counting elements of the superspecial orders with a prescribed trace and norm in a way that generalizes the Gross–Zagier formula. Our method is very similar to Gross–Zagier's and Dorman's; their results are the special case $g = 1$. To make the link between the algebraic and the geometric sides of the story, we include the determination of endomorphism

rings of superspecial abelian varieties in Section 7. Section 8 connects the counting formula for isomorphisms between CM abelian varieties with the counting formula for embeddings into superspecial orders.

The main result of the paper is an explicitly computable counting formula for the number of isomorphisms modulo $\mathfrak{P} \mid p$ between abelian varieties with CM by two different CM fields K and K' with $K^+ = K'^+$ (Theorems 6.5 and 8.2). This formula can be viewed as an intersection number under the assumption that a reasonable lemma in intersection theory holds (Section 9). Less precisely, we refer to this value as a "coincidence number". It also has an algebraic interpretation as the number of "optimal triples" of embeddings of $\mathbb{O}_K$ and $\mathbb{O}_{K'}$ into superspecial orders (Section 8.4).

For primes of supersingular reduction for CM abelian varieties, a separate computation of the endomorphism rings is given in Section 10. In Section 11, a volume argument such as was used in [Goren and Lauter 2007] is given to establish a bound on primes p of either supersingular or superspecial reduction, where isomorphisms exist modulo p between CM points associated to K and K'. In Section 12, an example of two Galois CM fields is given and all primes dividing the differences of the Igusa invariants are examined and compared with our counting formula.

The authors thank the referee for helpful comments to improve the paper.

2. Preliminaries

2.1. ***Quadratic reciprocity for number fields.*** Let L be a number field and γ and δ prime elements of L that are nonassociates such that $(\gamma\delta, 2) = 1$. Define

$$\left(\frac{\gamma}{\delta}\right) = \begin{cases} 1 & \text{if } \gamma = \square \bmod \delta, \\ -1 & \text{else.} \end{cases}$$

Let $B := \left(\frac{\gamma,\delta}{L}\right)$ be the quaternion algebra over L defined by the elements γ and δ. For any place η of L, including the infinite places, define

$$(\gamma, \delta)_\eta := \begin{cases} 1 & \text{if } B \otimes_L L_\eta \text{ is split,} \\ -1 & \text{else,} \end{cases}$$

and we have the following analogue of quadratic reciprocity for the number field L:

Proposition 2.1. (1) *If η is a finite prime such that $\eta \nmid 2$, then $(\gamma, \delta)_\eta = 1$ if and only if $x^2 - \gamma y^2 - \delta z^2 = 0$ has a nontrivial solution modulo η.*

(2) *If η is complex, then $(\gamma, \delta)_\eta = 1$.*

(3) *If η is real ($\eta : L \to \mathbb{R}$), then $(\gamma, \delta)_\eta = 1$ if and only if $\eta(\gamma) > 0$ or $\eta(\delta) > 0$. That is, $(\gamma, \delta)_\eta = -1$ if and only if both $\eta(\gamma)$ and $\eta(\delta)$ are negative.*

$$\left(\frac{\gamma}{\delta}\right)\left(\frac{\delta}{\gamma}\right) = (-1)^{r(\gamma,\delta)} \cdot \prod_{\eta|2} (\gamma, \delta)_\eta, \tag{4}$$

where $r(\gamma, \delta)$ equals the number of real places η such that both $\eta(\gamma)$ and $\eta(\delta)$ are negative. In particular, if either γ or δ are totally positive, then

$$\left(\frac{\gamma}{\delta}\right)\left(\frac{\delta}{\gamma}\right) = (\gamma, \delta)_2 := \prod_{\eta|2} (\gamma, \delta)_\eta.$$

$$\left(\frac{-1}{\gamma}\right)(-1, \gamma)_2 = (-1)^{r(\gamma)}, \tag{5}$$

where $r(\gamma)$ is the number of real places η such that $\eta(\gamma)$ is negative.

Proof. We prove (1). By [Vignéras 1980, Chapter II, Corollary 1.2], $(\gamma, \delta)_\eta = 1$ if and only if $x^2 - \gamma y^2 - \delta z^2 = 0$ has a nontrivial solution in L_η, where by "nontrivial" we mean a solution where at least one of the variables with nonzero coefficients is nonzero. Suppose that $x^2 - \gamma y^2 - \delta z^2 = 0$ has a nontrivial solution in L_η. By multiplying by a common denominator, we can assume $x, y, z \in \mathbb{O}_{L_\eta}$ and one of them is a unit. Then reducing modulo η, we get a nontrivial solution to $x^2 - \gamma y^2 - \delta z^2 \equiv 0 \bmod \eta$. Conversely, suppose $x^2 - \gamma y^2 - \delta z^2 \equiv 0 \bmod \eta$ has a nontrivial solution. By Hensel's lemma, we can lift the solution to $\mathbb{O}_{L_\eta}$.

Part (2) is clear, and (3) follows from loc. cit. because $x^2 - \eta(\gamma) y^2 - \eta(\delta) z^2 = 0$ has a nontrivial solution in $\mathbb{R}^3$ if and only if either $\eta(\gamma) > 0$ or $\eta(\delta) > 0$.

To prove (4), first note that $(\gamma, \delta)_\gamma = 1$ if and only if $x^2 - \gamma y^2 - \delta z^2 = 0$ has a nontrivial solution modulo γ if and only if $\delta = (x/z)^2$ for some nonzero $x, z \in \mathbb{O}_L/(\gamma)$ if and only if $\left(\frac{\delta}{\gamma}\right) = 1$. By the product formula,

$$1 = \prod_\eta (\gamma, \delta)_\eta = (-1)^{r(\gamma,\delta)} (\gamma, \delta)_2 \left(\frac{\delta}{\gamma}\right)\left(\frac{\gamma}{\delta}\right) \prod_{\substack{\eta \text{ finite} \\ \eta \nmid 2\gamma\delta}} (\gamma, \delta)_\eta.$$

But for $\eta \nmid 2\gamma\delta$, $x^2 - \gamma y^2 - \delta z^2 = 0$ has a nontrivial solution modulo η, so $(\gamma, \delta)_\eta = 1$.

Similarly for (5), for any real place η, $\eta(\gamma) > 0$ if and only if $(-1, \gamma)_\eta = 1$, so it follows from the product formula that

$$1 = \prod_\eta (-1, \gamma)_\eta = (-1)^{r(\gamma)} \left(\frac{-1}{\gamma}\right)(-1, \gamma)_2. \qquad \square$$

2.2. ***The ring of integers in CM fields.*** Let K be a CM field with a totally real subfield $K^+ = L$. Assume that L has strict class number 1. Let $\mathfrak{D}_{K/L}$ be the different of the extension, and let η denote a prime ideal of $\mathbb{O}_L$.

Lemma 2.2. (1) $\mathbb{O}_K = \mathbb{O}_L[t]$, *where $t^2 + at + b = 0$ for some $a, b \in \mathbb{O}_L$, and $\mathfrak{D}_{K/L}^{-1} = (1/\sqrt{d})$ with $d = a^2 - 4b$ a totally negative element of $\mathbb{O}_L$.*

(2) *Assume for $\eta|2$ that if $\eta|a$ then b is not a square modulo η. Then $(d,2)=1$, and d is square-free.*

Proof. Part (1) is proved in [Goren and Lauter 2006, Lemma 3.1].

We now prove (2). Since $\mathbb{O}_K = \mathbb{O}_L[t]/(t^2+at+b)$, the prime decomposition of every prime η is determined by the prime factorization of $t^2+at+b \bmod \eta$. If η is ramified, that implies that $t^2+at+b \equiv (t-c)^2 \bmod \eta$ for some $c \in \mathbb{O}_L/(\eta)$. But since $\eta|2$, we have

$$(t-c)^2 \equiv t^2-c^2 \equiv t^2+c^2 \bmod \eta,$$

so

$$t^2+at+b \equiv (t-c)^2 \bmod \eta \iff \eta|a \text{ and } b = \square \bmod \eta.$$

Thus, our condition implies that $\mathbb{O}_K$ is unramified over all primes $\eta|2$. It follows that $(d,2)=1$.

Next we prove that d is square-free. Let η be a prime of $\mathbb{O}_L$ not dividing 2. For $\eta|d$, we have $\mathbb{O}_K \otimes_{\mathbb{O}_L} \mathbb{O}_{L_\eta} = \mathbb{O}_{L_\eta}[\sqrt{d}]$ because $\mathbb{O}_K = \mathbb{O}_L[(-a+\sqrt{d})/2]$. Write $\mathbb{O}_{L_\eta}[\sqrt{d}] = \mathbb{O}_{L_\eta}[\sqrt{u\cdot\alpha_\eta^r}]$, where u is a unit at η and $\alpha_\eta^r|d$. If $r>1$, then

$$\mathbb{O}_{L_\eta}\big[\sqrt{u\cdot\alpha_\eta^r}\big] = \mathbb{O}_{L_\eta} + \mathbb{O}_{L_\eta}\cdot\sqrt{u\cdot\alpha_\eta^r}$$

has no element of valuation 1, which is not possible. Indeed, if π is a uniformizer of $\mathbb{O}_{K_\eta}$ with valuation normalized so that $\mathrm{val}_\eta(\mathbb{O}_{L_\eta}) = \mathbb{Z}_{\geq 0}$, then for $x \in \mathbb{O}_{L_\eta}$, $\mathrm{val}_\pi(x) = 2\,\mathrm{val}_\eta(x) \in 2\mathbb{Z}_{\geq 0}$, and

$$\mathrm{val}_\pi\big(\sqrt{u\cdot\alpha_\eta^r}\big) = \tfrac{1}{2}\,\mathrm{val}_\pi(u\cdot\alpha_\eta^r) = \mathrm{val}_\eta(u\cdot\alpha_\eta^r) = r.$$

In other words, we have shown that discriminants of quadratic extensions of p-adic fields are square-free when $p \neq 2$. □

Lemma 2.3. *We have $\mathbb{O}_K = \mathbb{O}_L[(a'+\sqrt{d})/2]$ exactly for the $a' \in \mathbb{O}_L$ such that $a' \equiv a \bmod 2\mathbb{O}_L$. Such a' satisfy $(a')^2 \equiv d \bmod 4\mathbb{O}_L$. Conversely, given $a' \in \mathbb{O}_L$ such that $(a')^2 \equiv d \bmod 4\mathbb{O}_L$, we have $\mathbb{O}_K = \mathbb{O}_L[(a'+\sqrt{d})/2]$.*

Proof. If $a' \equiv a \bmod 2\mathbb{O}_L$, we have $\mathbb{O}_K = \mathbb{O}_L[t] = \mathbb{O}_L[(a+\sqrt{d})/2] = \mathbb{O}_L[(a'+\sqrt{d})/2]$ if $a' \equiv a \bmod 2\mathbb{O}_L$. We have $d = a^2 - 4b \equiv a^2 \bmod 4\mathbb{O}_L$. Then also $(a')^2 = (a+2y)^2 = a^2+4ay+4y^2 \equiv d \bmod 4\mathbb{O}_L$.

If $\mathbb{O}_L[(a+\sqrt{d})/2] = \mathbb{O}_L[(a'+\sqrt{d})/2]$, then

$$\frac{a+\sqrt{d}}{2} = u + v\Big(\frac{a'+\sqrt{d}}{2}\Big),$$

which implies that

$$a+\sqrt{d} = 2u + va' + v\sqrt{d},$$

and so

$$v = 1 \quad \text{and} \quad a = 2u + a' \Longrightarrow a \equiv a' \bmod 2\mathbb{O}_L.$$

Finally, suppose $a' \in \mathbb{O}_L$ satisfies $(a')^2 \equiv d \bmod 4\mathbb{O}_L$. Then $(a' + \sqrt{d})/2$ is integral. Therefore, we get successively

$$\frac{a'+\sqrt{d}}{2} = u + v \cdot \left(\frac{a+\sqrt{d}}{2}\right),$$

from which we get successively

$$a' + \sqrt{d} = 2u + va + v\sqrt{d}, \quad v = 1, \quad a \equiv a' \bmod 2\mathbb{O}_L. \qquad \square$$

2.3. ***CM points on Hilbert modular varieties.*** Assume that L is a totally real field, $[L : \mathbb{Q}] = g$, and L has strict class number 1; we write $h_L^+ = 1$. This implies that $(\mathbb{O}_L{}^\times)^+ = (\mathbb{O}_L{}^\times)^2$. In this case, the Hilbert modular variety $\mathscr{H}_L$ associated to L is geometrically irreducible and affords the following description. It is the moduli space for triples $(A, \iota : \mathbb{O}_L \to \mathrm{End}(A), \eta)$, where A is a complex abelian variety of dimension g, ι is a ring embedding, and η is a principal $\mathbb{O}_L$-polarization or, equivalently, η is a principal polarization and the associated Rosati involution fixes $\mathbb{O}_L$ elementwise. We have $\mathscr{H}_L \cong \mathrm{SL}_2(\mathbb{O}_L) \setminus \mathfrak{H}^g$; see [Goren 2002, Chapter 2, §2]. Our interest is in the parametrization of CM points on $\mathscr{H}_L$.

2.3.1. *Abelian varieties with CM.* Let K be a CM field such that $K^+ = L$. We consider triples

$$(A, \iota : \mathbb{O}_K \to \mathrm{End}(A), \eta) \tag{2-1}$$

such that A is a g-dimensional complex abelian variety, ι is a ring homomorphism, and η is a principal $\mathbb{O}_K$-polarization, by which we mean a principal polarization whose associated Rosati involution induces complex conjugation on K.

Such datum produces a point on $\mathscr{H}_L$, namely, the point parametrizing $(A, \iota|_{\mathbb{O}_L}, \eta)$. This will be examined later. First we want to classify triples (A, ι, η) as in (2-1) up to isomorphism.

To a triple (A, ι, η), we may associate a CM type Φ that records the induced action of K on $T_{A,0}$, the tangent space to A at the origin. The theory of complex multiplication then asserts the existence of a fractional ideal $\mathfrak{a}$ of K such that

$$(A, \iota) \cong (\mathbb{C}^g / \Phi(\mathfrak{a}), \iota_{\mathrm{can}}),$$

where $\Phi(\mathfrak{a})$ is the lattice $\{(\varphi_1(a), \ldots, \varphi_g(a)) : a \in \mathfrak{a}\}$ and $\Phi = \{\varphi_1, \ldots, \varphi_g\}$; ι_{can} is the canonical action of $\mathbb{O}_K$ on that abelian variety obtained by extending the natural action on $\Phi(\mathfrak{a})$. Furthermore, the principal polarization η is induced from a paring on K of the form

$$(x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(ax\bar{y})$$

for some $a \in K$. The conditions on a ensuring the associated polarization, say η_a, is principal are these:

(1) $(a) = (\mathfrak{D}_K \mathfrak{a}\bar{\mathfrak{a}})^{-1}$.

(2) $\bar{a} = -a$.

(3) $\mathrm{Im}(\varphi_i(a)) > 0$ for $i = 1, \ldots, g$.

It follows easily that for every $\lambda \in K^\times$, the principally polarized abelian variety associated to $(\Phi, \mathfrak{a}, a)$ in the manner above is isomorphic to that associated to $(\Phi, \lambda\mathfrak{a}, (\lambda\bar{\lambda})^{-1}a)$. Furthermore, any isomorphism of principally polarized abelian varieties $(A, \iota, \eta) \cong (A', \iota', \eta')$ as in (2-1) arises that way.

Now, given a fractional ideal $\mathfrak{a}$ of K, the ideal $\mathfrak{a}\bar{\mathfrak{a}}$ is of the form $\mathfrak{b}\mathbb{O}_K$ for some fractional ideal $\mathfrak{b}$ of L, and since $h_L = 1$, we can write $(\mathfrak{a}\bar{\mathfrak{a}})^{-1} = \lambda\mathbb{O}_K$ for a suitable $\lambda \in L$. The fractional ideal $\mathfrak{D}_K^{-1}$ is of the form $d^{-1/2}\mathbb{O}_K$, where d is a totally negative element of L. Thus,

$$(\mathfrak{D}_K \mathfrak{a}\bar{\mathfrak{a}})^{-1} = (\lambda d^{-1/2}),$$

and $\overline{\lambda d^{-1/2}} = -\lambda d^{-1/2}$. We are free to change λ by any unit $\epsilon \in {\mathbb{O}_L}^\times$. Since $({\mathbb{O}_L}^\times)^+ = ({\mathbb{O}_L}^\times)^2$, it follows easily that for any choice of signs $s_1, \ldots, s_g$ in $\{\pm 1\}$, there is a unit $\epsilon \in {\mathbb{O}_L}^\times$ such that the sign of $\varphi_i(\epsilon)$ is s_i. Since

$$\mathrm{Im}\big(\varphi_i\big(\epsilon\lambda\sqrt{d}^{-1}\big)\big) = \varphi_i(\epsilon)\,\mathrm{Im}\big(\varphi_i\big(\lambda\sqrt{d}^{-1}\big)\big),$$

by choosing ϵ properly we may arrange $\mathrm{Im}(\varphi_i(\epsilon\lambda\sqrt{d}^{-1})) > 0$ for all $i = 1, \ldots, g$. We have thus shown that for every fractional ideal $\mathfrak{a}$ of K, there is a suitable a such that $(\Phi, \mathfrak{a}, a)$ gives a principally polarized abelian variety with CM by K.

Our discussion so far shows that the isomorphism classes of principally polarized abelian varieties with CM by $\mathbb{O}_K$ are in bijection with equivalence classes of the set

$$\{(\Phi, \mathfrak{a}, a) : \Phi \text{ is a CM type, } a \text{ satisfies (1)–(3) above relative to } (\Phi, \mathfrak{a})\}.$$

The equivalence relation is $(\Phi, \mathfrak{a}, a) \sim (\Phi, \lambda\mathfrak{a}, \lambda\bar{\lambda}a)$ for $\lambda \in K^\times$ and, further, that every pair $(\Phi, \mathfrak{a})$, where Φ is a CM type and $\mathfrak{a}$ is a fractional ideal, appears in a suitable triple $(\Phi, \mathfrak{a}, a)$.

Given $(\Phi, \mathfrak{a}, a)$ and $(\Phi, \mathfrak{a}, b)$, there is a unit $\epsilon_1 \in {\mathbb{O}_K}^\times$ such that $b = \epsilon_1 a$ because both a and b generate the ideal $(\mathfrak{D}_K \mathfrak{a}\bar{\mathfrak{a}})^{-1}$. Since $\bar{a} = -a$ and $\bar{b} = -b$, it follows that $\epsilon_1 \in {\mathbb{O}_L}^\times$, and since $\mathrm{Im}(\varphi(a)) > 0$ and $\mathrm{Im}(\varphi(b)) > 0$, it follows that $\epsilon_1 \in {\mathbb{O}_L}^{\times,+}$. Using that ${\mathbb{O}_L}^{\times,+} = {\mathbb{O}_L}^{\times,2}$, we conclude that there is an $\epsilon \in \mathbb{O}_L$ such that $\epsilon_1 = \epsilon^2 = \epsilon\bar{\epsilon}$. That is, $(\Phi, \mathfrak{a}, a) \sim (\Phi, \mathfrak{a}, b)$. We therefore conclude that, in the strict class number 1 case, isomorphism classes of principally polarized abelian varieties with CM by K and a fixed CM type are parametrized by the ideal classes of K.

2.3.2. *CM points on $\mathscr{H}_L$.* Let $(A, \iota : \mathbb{O}_K \to \mathrm{End}(A))$ be a complex abelian variety with CM by K (so $[K : \mathbb{Q}] = 2\dim(A)$). Since $h_L^+ = 1$, it carries a unique principal polarization up to isomorphism. Consider $\mathrm{End}_{\mathbb{O}_L}(A)$. We use [Chai 1995, Lemma 6, p. 464]. In the notation of that lemma since A has CM, only cases III(a) and IV

can arise. But since we are working over the complex numbers, in fact only case IV can arise, and according to which, $A \sim B^n$, where B is of dimension g/n and has CM by a CM field K_0 whose totally real subfield L_0 is contained in L and satisfies $[L : L_0] = n$. One has $\mathrm{End}_L^0(A) = L \otimes_{L_0} K_0$, which is a CM field according to that lemma. It follows, because K is primitive, that $\mathrm{End}_L^0(A) = K$. As a consequence, once a RM structure is specified on A, there are precisely two CM structures extending it; if $\iota : \mathbb{O}_K \to \mathrm{End}(A)$ is one of them, the other is $\bar{\iota} := \iota \circ \tau$, where τ is complex conjugation on K. If ι has CM type Φ, then $\bar{\iota}$ has CM type $\bar{\Phi}$. Let $\mathscr{F}$ be the set of CM types for K.

Proposition 2.4. *Let* $(\Phi, [\mathfrak{a}]) \sim (\bar{\Phi}, [\bar{\mathfrak{a}}])$ $(= (\bar{\Phi}, [\mathfrak{a}^{-1}]))$ *define an equivalence relation* $\sim$ *on* $\mathscr{F} \times \mathrm{Cl}(K)$. *Then the set* $\mathscr{F} \times \mathrm{Cl}(K)/\sim$ *has* $2^{g-1} \times \#\mathrm{Cl}(K)$ *elements and is in a natural bijection with the* K*-CM points on* $\mathscr{H}_L$, *that is, with the points* $(A, \iota : \mathbb{O}_L \to \mathrm{End}(A), \eta)$ *for which we can extend* ι *to an embedding* $\mathbb{O}_K \to \mathrm{End}(A)$ *whose image is fixed* (*as a set*) *by the Rosati involution associated to* η.

3. Quaternion algebras over totally real fields

Let L be a totally real number field of degree g and strict class number 1. Let p be a prime number unramified in L, and let

$$B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L,$$

where $B_{p,\infty}$ is the rational quaternion algebra ramified at p and ∞ alone. Let

$$S := \{\mathfrak{p} \lhd \mathbb{O}_L : \mathfrak{p} \mid p\}$$

be the set of prime ideals of L above p, and let

$$S_0 = \{\mathfrak{p} \in S : f(\mathfrak{p}/p) \equiv 1 \bmod 2\}$$

be those with odd residue degree. The algebra $B_{p,L}$ is ramified precisely at all infinite places and at the primes $\mathfrak{p} \in S_0$.

The rest of this section and Sections 4 and 5 are devoted to giving a description of the quaternion algebra $B_{p,L}$ and a classification of some particular orders under the assumptions that all primes $\mathfrak{p} \in S \setminus S_0$ split in K and all primes $\mathfrak{p} \in S_0$ are inert in K. First we prove that this assumption is satisfied when p is an unramified prime of superspecial reduction for an abelian variety with CM by K.

3.1. *Splitting behavior in the case of superspecial reduction.*

Proposition 3.1. *Let* p *be a rational prime unramified in* K. *Let* A *be an abelian variety with CM by* $\mathbb{O}_K$ *defined over a number field* M *with good reduction at a prime ideal* $\mathfrak{p}_M$ *of* M *dividing the rational prime* p. *Assume that* A *has supersingular reduction modulo* $\mathfrak{p}_M$. *Then every prime in* S_0 *is inert in* K. *Assume further that* A *has superspecial reduction*; *then every prime in* $S \setminus S_0$ *is split in* K.

Proof. Since A has supersingular reduction, say $\bar{A}$, $\mathrm{End}_L^0(\bar{A}) \cong B_{p,L} = B_{p,\infty} \otimes_{\mathbb{Q}} L$ [Chai 1995, Lemma 6], and so

$$K \hookrightarrow B_{p,L}.$$

Thus, at every prime $\mathfrak{P}$ of K above a prime $\mathfrak{p}$ of L, the field $K_{\mathfrak{P}}$ splits the quaternion algebra $B_{p,L} \otimes_L L_{\mathfrak{p}}$. The quaternion algebra $B_{p,L}$ is ramified precisely at the primes in S_0 and at infinity, so if $\mathfrak{p} \in S_0$, we find that each $K_{\mathfrak{P}}$ is a quadratic field extension of $L_{\mathfrak{p}}$; that is, since p is unramified in K, all the primes in S_0 are inert in K.

Assume now that there is a prime $\mathfrak{p} \in S \setminus S_0$ that is inert in K, and let $\mathfrak{P}$ be the prime of K above $\mathfrak{p}$. Let us denote the embedding of $\mathbb{O}_L$ into $W(\bar{\mathbb{F}}_p)$ associated to $\mathfrak{p}$ $\{\varphi_1, \ldots, \varphi_f\}$ and $f = f(\mathfrak{p}/p)$, where we may order the embeddings so that $\sigma \circ \varphi_i = \varphi_{i+1}$ and σ denotes the Frobenius automorphism. Each embedding φ_i is the restriction of two embeddings of $\mathbb{O}_K$ into $W(\bar{\mathbb{F}}_p)$ that we denote ψ_i^1 and ψ_i^2, where one is the composition of the other with complex conjugation. Since $\mathfrak{P}$ is inert over $\mathfrak{p}$, σ still acts transitively on the set $\{\psi_i^j : i = 1, \ldots, f, j = 1, 2\}$.

The Dieudonné module of $\bar{A}$ decomposes as $D = \bigoplus_{\mathfrak{p}\,|\,p} D(\mathfrak{p})$ relative to the $\mathbb{O}_L$ structure. Let $H := D(\mathfrak{p})$. Then H decomposes further as

$$H = \bigoplus_{i=1}^{f} H(\varphi_i) = \bigoplus_{i=1}^{f} (H(\psi_i^1) \oplus H(\psi_i^2)),$$

where $H(\varphi_i)$ is a free $W(\bar{\mathbb{F}}_p)$-module of rank 2 on which $\mathbb{O}_L$ acts via φ_i, and it decomposes into a direct sum of two free $W(\bar{\mathbb{F}}_p)$-modules of rank 1, $H(\psi_i^1)$ and $H(\psi_i^2)$, on which $\mathbb{O}_K$ acts by ψ_i^1 and ψ_i^2, respectively. Now, the transitivity of the action of σ on the ψ_i^j means that we can order them so that

$$\begin{aligned}
&\sigma \circ \psi_i^1 = \psi_{i+1}^1, \quad && i = 1, 2, \ldots, f-1,\\
&\sigma \circ \psi_f^1 = \psi_1^2, &&\\
&\sigma \circ \psi_i^2 = \psi_{i+1}^2, \quad && i = 1, 2, \ldots, f-1,\\
&\sigma \circ \psi_f^2 = \psi_1^1. &&
\end{aligned}$$

Let us choose a basis $\{e_i^j : i = 1, 2, \ldots, f, j = 1, 2\}$ for H such that e_i^j spans $H(\psi_i^j)$. Note that the kernel of Frobenius on $\overline{H} := H \bmod p$ is an $\mathbb{O}_K$-module and is one-dimensional in every $H(\varphi_i)$ because $\bar{A}$ satisfies the Rapoport condition or, alternately, for each i, precisely one of $\{\psi_i^1, \psi_i^2\}$ belongs to the CM type. Suppose, without loss of generality, that e_1^1 spans the kernel of Frobenius in $\overline{H}(\varphi_1)$; then we must have that $\mathrm{Fr}(e_1^2)$, which is equal up to a unit to e_2^2, spans the kernel of Frobenius in $\overline{H}(\varphi_2)$ (this is where "superspecial" is being used), and by the same rationale, we find that the kernel of Frobenius in $\overline{H}(\varphi_i)$ is spanned by e_i^1 for i odd and by e_i^2 for i even. In particular, the kernel of Frobenius in $\overline{H}(\varphi_f)$ is spanned by e_f^2 because f is

even. Now, by the same rationale, $\mathrm{Fr}(e_f^1)$ spans the kernel of Frobenius in $\overline{H}(\varphi_1)$, and it lies in $\overline{H}(\psi_1^2)$ because $\sigma \circ \psi_f^1 = \psi_1^2$. This is a contradiction. □

3.2. ***A description of $B_{p,L}$.*** Next we give a description of the quaternion algebra $B_{p,L}$ in terms of a CM field K for a certain set of primes p, which according to Proposition 3.1 includes the superspecial primes of K. This description generalizes the approach of Gross and Zagier.

Notation. If $\mathfrak{q}$ is a prime ideal of L, let $\alpha_\mathfrak{q}$ denote a totally positive generator of $\mathfrak{q}$. It is unique up to an element of ${\mathbb{O}_L}^{\times +} = {\mathbb{O}_L}^{\times,2}$. Write $p = \prod_{\mathfrak{p}\in S} \alpha_\mathfrak{p}$.

Proposition 3.2. *Let K be a CM field and $K^+ = L$. Assume p is odd and unramified in L and that all primes $\mathfrak{p} \in S \setminus S_0$ split in K and all primes $\mathfrak{p} \in S_0$ are inert in K. These conditions imply that K embeds in $B_{p,L}$. Assume that the discriminant $\mathfrak{d}_{K/L} = (d)$ satisfies $(d, 2p) = 1$. Then there is a totally negative prime element $\alpha_0 \in \mathbb{O}_L$ such that $(\alpha_0, 2pd) = 1$, the ideal (α_0) is split in K, and*

$$B_{p,L} \cong \left(\frac{d, \alpha_0 p}{L}\right).$$

Proof. We first need a lemma.

Lemma 3.3 (Primes in arithmetic progressions). *Let L be a number field, and let $\nu_1, \ldots, \nu_t$ be some of L's embeddings into $\mathbb{R}$. Let $\mathfrak{r} \lhd \mathbb{O}_L$ be an integral ideal and $r \in \mathbb{O}_L$ an element such that $(r, \mathfrak{r}) = 1$. Then there is a prime element $\alpha \in \mathbb{O}_L$ such that $\alpha \equiv r \mod \mathfrak{r}$ and $\nu_i(\alpha) > 0$ for $i = 1, \ldots, t$.*

Proof. We may assume $\nu_i(r) > 0$ for $i = 1, \ldots, t$. Indeed, one may replace r by $r + n$ for any element $n \in \mathfrak{r}$. Since $\mathfrak{r} \otimes \mathbb{Q} = L$, for any $c \in \mathbb{R}$, $\mathfrak{r}$ contains elements n such that $\nu(n) > c$ for every real place ν of L. Taking $C = \max\{|\nu_i(r)| : \nu_i(r) < 0\}$ and a suitable element $n \in \mathfrak{r}$, we get $\nu_i(r + n) > 0$ for $i = 1, \ldots, t$.

Consider the modulus $\mathfrak{r}\nu_1\nu_2 \cdots \nu_t = \mathfrak{m}$ and the ray class group modulo $\mathfrak{m}$, $I(\mathfrak{m})/P(\mathfrak{m})$. Here $I(\mathfrak{m})$ is the multiplicative group of fractional ideals prime to $\mathfrak{m}$ and $P(\mathfrak{m})$ is the subgroup of principal ideals having a generator β such that $\beta \equiv 1 \mod \mathfrak{m}$ and $\nu_i(\beta) > 0$ for $i = 1, \ldots, t$. Let $L(\mathfrak{m})$ be the corresponding class field with $\mathrm{Gal}(L(\mathfrak{m})/L) \cong I(\mathfrak{m})/P(\mathfrak{m})$. The ideal (r) is an element of $I(\mathfrak{m})/P(\mathfrak{m})$. Let

$$\sigma := ((r), L(\mathfrak{m})/L) \in \mathrm{Gal}(L(\mathfrak{m})/L)$$

be the Artin symbol. By Chebotarev, there is a prime ideal $\mathfrak{p}$ such that $(\mathfrak{p}, \mathfrak{m}) = 1$ and

$$\sigma = \sigma_\mathfrak{p} = (\mathfrak{p}, L(\mathfrak{m})/L).$$

Also, $\mathfrak{p}$ is equivalent to (r) modulo $P(\mathfrak{m})$ and hence also principal. Indeed,

$$\sigma_\mathfrak{p}|_{H_L} = \sigma|_{H_L} = ((r), L(\mathfrak{m})/L)|_{H_L} = 1.$$

Since $\mathrm{Gal}(H_L/L) \cong I/P$, we must have that $\mathfrak{p}$ is principal. Let $(\alpha_1) = \mathfrak{p}$. By construction, $(\alpha_1) = (r)$ in $I(\mathfrak{m})/P(\mathfrak{m})$. That means that the ideal $(\alpha_1 r^{-1})$ has a generator $u\alpha_1 r^{-1}$, $u \in {\mathbb{O}_L}^\times$, such that

$$u\alpha_1 r^{-1} \equiv 1 \bmod \mathfrak{m}.$$

Let $\alpha = u\alpha_1$. Then $\alpha \equiv r \bmod \mathfrak{m}$, meaning $\alpha \equiv r \bmod \mathfrak{r}$, and for every $i = 1, \ldots, t$, $v_i(\alpha)$ has the same sign as $v_i(r)$, i.e., is positive. □

According to Lemma 3.3, we can choose $\alpha_0 \in \mathbb{O}_L$ satisfying these conditions:

(1) α_0 is a totally negative prime element of $\mathbb{O}_L$.

(2) $\alpha_0 \equiv p \bmod \eta^N$ for each $\eta \mid 2$ and some $N \gg 0$ (for the choice of N, see below).

(3) $\alpha_0 \equiv p \bmod \mathfrak{q}$ for each $\mathfrak{q} \mid d$.

(4) $\alpha_0 \equiv 1 \bmod p$.

Since $x^2 - dy^2 - \alpha_0 p z^2 \equiv 0 \bmod \eta^N$ has a nontrivial solution and N is large enough, by Hensel's lemma there is a p-adic solution. We therefore have

$$(d, \alpha_0 p)_\eta = 1 \quad \text{for all } \eta \mid 2, \qquad \left(\frac{\alpha_0}{\mathfrak{q}}\right) = \left(\frac{p}{\mathfrak{q}}\right) \quad \text{for all } \mathfrak{q} \mid d \tag{3-1}$$

and $(\alpha_0, 2pd) = 1$.

To show that $B_{p,L} \cong \left(\frac{d, \alpha_0 p}{L}\right)$, we need to check the following:

1. $(d, \alpha_0 p)_\eta = 1$ for all $\eta \mid 2$. This follows from (3-1).
2. $(d, \alpha_0 p)_\eta = 1$ for all finite η with $\eta \nmid d\alpha_0 p$. This is because $x^2 - dy^2 - \alpha_0 p z^2 \equiv 0 \bmod \eta$ has a nontrivial solution.
3. $(d, \alpha_0 p)_\eta = 1$ for all finite η such that $\eta \mid d$. This is so because $x^2 - \alpha_0 p z^2 \equiv 0 \bmod \eta$ has a nontrivial solution if and only if $\left(\frac{\alpha_0 p}{\eta}\right) = 1$, which is true by (3).
4. $(d, \alpha_0 p)_\eta = 1$ for all $\eta \in S \setminus S_0$. Indeed, $x^2 - dy^2 \equiv 0 \bmod \eta$ has a nontrivial solution if and only if $d = \square \bmod \eta$, which holds if and only if η splits in K.
5. $(d, \alpha_0 p)_\eta = 1$ if $\eta = \alpha_0$. This is so because the congruence $x^2 - dy^2 \equiv 0 \bmod \alpha_0$ has a nontrivial solution if and only if $\left(\frac{d}{\alpha_0}\right) = 1$. We will examine this below.
6. $(d, \alpha_0 p)_\eta = -1$ for all $\eta \in S_0$. Indeed, $x^2 - dy^2 \equiv 0 \bmod \eta$ has only the trivial solution if and only if $d \neq \square \bmod \eta$, which holds if and only if η is inert in K.
7. $(d, \alpha_0 p)_\eta = -1$ for all η real. This is so because $x^2 - dy^2 - \alpha_0 p z^2 = 0$ in $\mathbb{R}$ has only the trivial solution (since $-d$ and $-\alpha_0 p$ are both positive).

So it remains to prove only that $\left(\frac{d}{\alpha_0}\right) = 1$.

Write $d = (-1) \cdot \prod_{\mathfrak{q}|d} \alpha_{\mathfrak{q}}$ and $p = \prod_{\mathfrak{p}|p} \alpha_{\mathfrak{p}}$. Then

$$\begin{aligned}
\left(\frac{d}{\alpha_0}\right) &= \left(\frac{-1}{\alpha_0}\right) \prod_{\mathfrak{q}|d} \left(\frac{\alpha_{\mathfrak{q}}}{\alpha_0}\right) \\
&= \left(\frac{-1}{\alpha_0}\right) \prod_{\mathfrak{q}|d} \left(\left(\frac{\alpha_0}{\alpha_{\mathfrak{q}}}\right)(\alpha_0, \alpha_{\mathfrak{q}})_2\right) && \text{(by quadratic reciprocity)} \\
&= \left(\frac{-1}{\alpha_0}\right) \prod_{\mathfrak{q}|d} \left(\prod_{\mathfrak{p}|p} \left(\frac{\alpha_{\mathfrak{p}}}{\alpha_{\mathfrak{q}}}\right)\right)(\alpha_0, \alpha_{\mathfrak{q}})_2 && \left(\text{since } \left(\tfrac{\alpha_0}{\mathfrak{q}}\right) = \left(\tfrac{p}{\mathfrak{q}}\right)\right) \\
&= \left(\frac{-1}{\alpha_0}\right)(\alpha_0, -d)_2 \prod_{\mathfrak{q}|d,\, \mathfrak{p}|p} \left(\frac{\alpha_{\mathfrak{p}}}{\alpha_{\mathfrak{q}}}\right) \\
&= \left(\frac{-1}{\alpha_0}\right)(\alpha_0, -d)_2 \prod_{\mathfrak{q}|d,\, \mathfrak{p}|p} \left(\frac{\alpha_{\mathfrak{q}}}{\alpha_{\mathfrak{p}}}\right)(\alpha_{\mathfrak{p}}, \alpha_{\mathfrak{q}})_2 && \text{(by quadratic reciprocity)} \\
&= \left(\frac{-1}{\alpha_0}\right)(\alpha_0, -d)_2 \prod_{\mathfrak{p}|p} \left(\frac{-d}{\alpha_{\mathfrak{p}}}\right)(-d, \alpha_{\mathfrak{p}})_2 \\
&= \left(\frac{-1}{\alpha_0}\right)(\alpha_0, -1)_2(\alpha_0, d)_2 \prod_{\mathfrak{p}|p} \left(\frac{-1}{\alpha_{\mathfrak{p}}}\right)(\alpha_{\mathfrak{p}}, -1)_2(\alpha_{\mathfrak{p}}, d)_2 \left(\frac{d}{\alpha_{\mathfrak{p}}}\right) \\
&= (-1)^g (\alpha_0, d)_2 \prod_{\mathfrak{p}|p} (\alpha_{\mathfrak{p}}, d)_2 \left(\frac{d}{\alpha_{\mathfrak{p}}}\right) && \text{(by Proposition 2.1(5))} \\
&= (-1)^g (\alpha_0 p, d)_2 (-1)^{\#S_0} && \text{(by our assumptions on } K\text{).}
\end{aligned}$$

This equals $(-1)^{g+\#S_0}$ since $(\alpha_0 p, d)_\eta = 1$ for all $\eta | 2$; but the exponent, being the number of ramified primes of $B_{p,L}$, is necessarily even. This concludes the proof. □

3.3. *Another description of the quaternion algebra $B_{p,L}$.*

Definition 3.4. For $\alpha, \beta \in K$, define

$$[\alpha, \beta] := \begin{pmatrix} \alpha & \beta \\ \alpha_0 p \bar{\beta} & \bar{\alpha} \end{pmatrix} \in M_2(K).$$

Lemma 3.5. *With assumptions as in Proposition 3.2, $B_{p,L} \cong \{[\alpha, \beta] : \alpha, \beta \in K\}$.*

Proof. Proposition 3.2 implies that $B_{p,L} = L \oplus Li \oplus Lj \oplus Lij$ with $i^2 = d$, $j^2 = \alpha_0 p$, and $ij = -ji$. We can write this as $K \oplus Kj$ with the multiplicative structure such that, for $x, y \in K$, we have $x(yj) = (xy)j$, $j^2 = \alpha_0 p$, and

$$xj = (x_1 + x_2 i)j = x_1 j + x_2 ij = jx_1 - jix_2 = j(x_1 - ix_2) = j\bar{x}.$$

So for the isomorphism $x + yj \to [x, y]$ to respect the multiplicative structure, it is enough to check the following:

(1) $[\alpha, 0][0, \beta] = [0, \alpha\beta]$, so

$$\begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} \begin{pmatrix} 0 & \beta \\ \alpha_0 p\bar{\beta} & 0 \end{pmatrix} = \begin{pmatrix} 0 & \alpha\beta \\ \alpha_0 p\overline{\alpha\beta} & 0 \end{pmatrix},$$

(2) $[0, 1]^2 = [\alpha_0 p, 0]$, so

$$\begin{pmatrix} 0 & 1 \\ \alpha_0 p & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \alpha_0 p & 0 \end{pmatrix} = \begin{pmatrix} \alpha_0 p & 0 \\ 0 & \alpha_0 p \end{pmatrix},$$

(3) $[\alpha, 0][0, 1] = [0, 1][\bar{\alpha}, 0]$, so

$$\begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ \alpha_0 p & 0 \end{pmatrix} = \begin{pmatrix} 0 & \alpha \\ \alpha_0 p\bar{\alpha} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ \alpha_0 p & 0 \end{pmatrix} \begin{pmatrix} \bar{\alpha} & 0 \\ 0 & \alpha \end{pmatrix}.$$ □

4. Orders in the quaternion algebra $B_{p,L}$

By Proposition 3.2, the ideal $\alpha_0\mathbb{O}_L$ splits in K. Write

$$\alpha_0\mathbb{O}_K = \mathscr{A} \cdot \bar{\mathscr{A}},$$

and let $\mathscr{D} = \mathscr{D}_{K/L} = (\sqrt{d})$ be the different ideal of K/L.

Definition 4.1. Let $\mathfrak{a}$ be an integral ideal of $\mathbb{O}_K$. For each $\mathfrak{q}|d$, fix a solution $\lambda_\mathfrak{q}$ to

$$x^2 \equiv \alpha_0 p \bmod \mathfrak{q}.$$

Let $\varepsilon(\mathfrak{a}, \mathfrak{q}) \in \{\pm 1\}$ be a choice of sign for each $\mathfrak{q}|d$ and $\lambda \in L$, $(\lambda, d) = 1$, such that

(1) $\lambda \equiv \varepsilon(\mathfrak{a}, \mathfrak{q})\lambda_\mathfrak{q} \bmod \mathfrak{q}$, $\forall \mathfrak{q}|d$ and

(2) $\lambda\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$ is an integral ideal of $\mathbb{O}_K$.

This is possible by the Chinese remainder theorem and using $(\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}, d) = 1$.

We shall denote $\epsilon(\mathfrak{a})$ the vector of signs $\{\epsilon(\mathfrak{a}, \mathfrak{q}) : \mathfrak{q}|d\}$. When we need to emphasize the dependence of λ on the choice of signs, we shall write $\lambda_{\epsilon(\mathfrak{a})}$ instead of λ. For example, one particular choice of signs that we will often make is $\varepsilon(\mathfrak{a}, \mathfrak{q}) = (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a})}$, where $\tilde{\mathfrak{q}} \lhd \mathbb{O}_K$ is an ideal such that $\mathfrak{q}\mathbb{O}_K = \tilde{\mathfrak{q}}^2$, and we denote $\lambda_\mathfrak{a}$ the corresponding λ.

Let $l \in \mathbb{O}_L$ be any nonzero element such that $(l, \alpha_0 d\mathfrak{a}^{-1}\bar{\mathfrak{a}}) = 1$ and l is split in K/L. In particular, l could be a power of p. Now define

$$R := R(\mathfrak{a}, \lambda, l) = \left\{[\alpha, \beta] : \alpha \in \mathscr{D}^{-1}, \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}l\mathfrak{a}^{-1}\bar{\mathfrak{a}}, \alpha \equiv \lambda\beta \bmod \mathbb{O}_K\right\}.$$

Proposition 4.2. *Apply assumptions as in Proposition 3.2. In particular, K is a CM field such that $K^+ = L$ has strict class number 1, the discriminant of K/L is prime to 2 and thus square-free, and p is odd and unramified in K. All primes $\mathfrak{p} \in S \setminus S_0$ split in K, and all primes $\mathfrak{p} \in S_0$ are inert in K. Then*:

(1) *R is an order of $B_{p,L}$ containing $\mathbb{O}_K$.*

(2) *R has discriminant $p \cdot l$.*

(3) *R does not depend on the choice of λ as long as λ satisfies the same local sign conditions.*

Proof. (1) It should be clear that R is a finitely generated $\mathbb{O}_L$-module containing $\mathbb{O}_K = \{[\alpha, 0] : \alpha \in \mathbb{O}_K\}$. We need to show that R is closed under multiplication. The multiplication formula is

$$[x, y][z, w] = [xz + \alpha_0 py\overline{w}, xw + y\overline{z}],$$

and we need to show that, for $[x, y], [z, w] \in R$, also $[x, y][z, w] \in R$.

Step 1: *Show that $xz + \alpha_0 py\overline{w} \in \mathcal{D}^{-1}$.*

A priori, $xz \in \mathcal{D}^{-2}$, and

$$\alpha_0 py\overline{w} \in \alpha_0 p\mathcal{D}^{-1}\mathcal{A}^{-1} l\mathfrak{a}^{-1}\bar{\mathfrak{a}}\overline{\mathcal{D}^{-1}\mathcal{A}^{-1} l\mathfrak{a}^{-1}\bar{\mathfrak{a}}}$$
$$= \alpha_0 p\mathcal{D}^{-2}(\mathcal{A}\overline{\mathcal{A}})^{-1} l^2 = p\mathcal{D}^{-2} l^2 \subseteq \mathcal{D}^{-2} m,$$

so it is enough to show that $\mathrm{val}_{\tilde{\mathfrak{q}}}(xz + \alpha_0 py\overline{w}) \geq -1$ for all $\tilde{\mathfrak{q}} | \mathcal{D}$. Let $\mathfrak{q} = \tilde{\mathfrak{q}} \cap \mathbb{O}_L$. Then $\mathfrak{q}\mathbb{O}_K = \tilde{\mathfrak{q}}^2$. We will work $\mathfrak{q}$-adically. Let $\pi \in \mathbb{O}_{K_{\tilde{\mathfrak{q}}}}$ be a uniformizer such that $\overline{\pi} = -\pi$ (the extension of complex conjugation from K to $K_{\tilde{\mathfrak{q}}}$).

Lemma 4.3. *Such a π exists.*

Proof. Choose a uniformizer π_0 of $\mathbb{O}_{L_\mathfrak{q}}$, and let $K_1 = L_\mathfrak{q}(\sqrt{\pi_0})$. Then for K_1 there exists such a uniformizer. So it is enough to show that if $\mathfrak{q} | q$ and $q \neq 2$ then any q-adic field L_1 has a unique quadratic ramified extension. By local class field theory, ramified quadratic extensions are in bijection with subgroups of index 2 of $\mathbb{O}_{L_1}^\times$. There is a unique subgroup of index 2 of $\mathbb{O}_{L_1}^\times$ since it contains $\mathbb{O}_{L_1}^{\times 2}$ and $\mathbb{O}_{L_1}^\times / \mathbb{O}_{L_1}^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$. □

Note that $\mathcal{D}^{-1}\mathcal{A}^{-1} l\mathfrak{a}^{-1}\bar{\mathfrak{a}}\mathbb{O}_{K_{\tilde{\mathfrak{q}}}} = (1/\pi)\mathbb{O}_{K_{\tilde{\mathfrak{q}}}}$ since $(\mathcal{A}, \tilde{\mathfrak{q}}) = 1$, $(l, \tilde{\mathfrak{q}}) = 1$, and $(\mathfrak{a}^{-1}\bar{\mathfrak{a}}, \tilde{\mathfrak{q}}) = 1$ because $\mathfrak{a}^{-1}\bar{\mathfrak{a}}$ has no ramified or inert primes. Write then $x = x_0/\pi$, $y = y_0/\pi$, $z = z_0/\pi$, and $w = w_0/\pi$ with $x_0, y_0, z_0, w_0 \in \mathbb{O}_{K_{\tilde{\mathfrak{q}}}}$. So

$$x \equiv \lambda y \bmod \mathbb{O}_K \Longrightarrow x_0 - \lambda y_0 \in (\pi) \quad \text{and} \quad z \equiv \lambda w \bmod \mathbb{O}_K \Longrightarrow z_0 - \lambda w_0 \in (\pi).$$

Now

$$xz + \alpha_0 py\overline{w} = \frac{1}{\pi^2}(x_0 z_0 - \alpha_0 p y_0 \overline{w_0}),$$

so it is enough to show $\mathrm{val}_{\tilde{\mathfrak{q}}}(x_0z_0 - \alpha_0 p y_0 \overline{w_0}) \geq 1$. But

$$\begin{aligned} x_0z_0 - \alpha_0 p y_0 \overline{w_0} &\equiv \lambda y_0 \lambda w_0 - \alpha_0 p y_0 \overline{w_0} \bmod (\pi) \\ &\equiv \lambda^2 y_0 w_0 - \alpha_0 p y_0 w_0 \bmod (\pi) \end{aligned}$$

because conjugation is trivial mod (π)

$$\begin{aligned} &\equiv (\lambda^2 - \alpha_0 p) y_0 w_0 \\ &\equiv (\lambda_{\mathfrak{q}}^2 - \alpha_0 p) y_0 w_0 \\ &\equiv 0 \bmod (\pi). \end{aligned}$$

Step 2: *Show that* $xw + y\bar{z} \in \mathscr{D}^{-1}\mathscr{A}^{-1} l \mathfrak{a}^{-1} \bar{\mathfrak{a}}$.

A priori, xw, $y\bar{z} \in \mathscr{D}^{-2}\mathscr{A}^{-1} l \mathfrak{a}^{-1} \bar{\mathfrak{a}}$, so we just need to show $\mathrm{val}_{\tilde{\mathfrak{q}}}(xw + y\bar{z}) \geq -1$ at all primes $\tilde{\mathfrak{q}} | \mathscr{D}$. We need to show $\mathrm{val}_{\tilde{\mathfrak{q}}}(x_0w_0 - y_0\overline{z_0}) \geq 1$, using the same notation as in 1. We have, modulo (π), $x_0w_0 - y_0\overline{z_0} = x_0w_0 - y_0z_0 = \lambda y_0 w_0 - \lambda y_0 w_0 = 0$.

Step 3: *Show that* $xz + \alpha_0 p y \bar{w} - \lambda(xw + y\bar{z}) \in \mathbb{O}_K$.

A priori, by steps 1 and 2, $xz + \alpha_0 p y \bar{w} \in \mathscr{D}^{-1}$ and

$$\lambda(xw + y\bar{z}) \in \mathscr{D}^{-1} l \lambda \mathscr{A}^{-1} \mathfrak{a}^{-1} \bar{\mathfrak{a}} \subset \mathscr{D}^{-1} l \subset \mathscr{D}^{-1}$$

since $\lambda \mathscr{A}^{-1} \mathfrak{a}^{-1} \bar{\mathfrak{a}} \subseteq \mathbb{O}_K$. Therefore, we just need to show that for all $\tilde{\mathfrak{q}} | \mathscr{D}$,

$$\mathrm{val}_{\tilde{\mathfrak{q}}}(xz + \alpha_0 p y \bar{w} - \lambda(xw + y\bar{z})) \geq 0.$$

Using the same notation as above, this is equivalent to

$$\mathrm{val}_{\tilde{\mathfrak{q}}}(x_0z_0 - \alpha_0 p y_0 \overline{w_0} - \lambda(x_0w_0 - y_0\overline{z_0})) \geq 2.$$

Write $x_0 = \lambda y_0 + \pi x_1$ and $z_0 = \lambda w_0 + \pi z_1$. Then

$$\begin{aligned} &(\lambda y_0 + \pi x_1)(\lambda w_0 + \pi z_1) - \alpha_0 p y_0 \overline{w_0} - \lambda(\lambda y_0 + \pi x_1) w_0 + \lambda y_0(\lambda \overline{w_0} - \pi \overline{z_1}) \\ &\qquad = (\lambda^2 - \alpha_0 p) y_0 \overline{w_0} + \lambda \pi y_0 (z_1 - \overline{z_1}) \equiv 0 \bmod \pi^2 \end{aligned}$$

since $(z_1 - \overline{z_1}) \in (\pi)$ and $(\lambda^2 - \alpha_0 p) \in \mathfrak{q}\mathbb{O}_{L_{\mathfrak{q}}} \subset (\pi^2)$. This proves conclusion (1) of the proposition.

(2) We need to compute the discriminant of

$$R = R(\mathfrak{a}, \lambda, l) = \left\{ [\alpha, \beta] : \alpha \in \mathscr{D}^{-1}, \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1} l \mathfrak{a}^{-1} \bar{\mathfrak{a}}, \alpha \equiv \lambda\beta \bmod \mathbb{O}_K \right\}.$$

Let

$$R' := \{ [\alpha, \beta] : \alpha \in \mathbb{O}_K, \beta \in l \mathfrak{a}^{-1} \bar{\mathfrak{a}} \}.$$

Then R' is an $\mathbb{O}_L$-module of rank 4.

Lemma 4.4. *We have* $\mathrm{disc}(R') = (l \alpha_0 p d)^2$.

Proof. The quadratic form on R' is $\det[\alpha,\beta]=\alpha\bar{\alpha}-\alpha_0 p\beta\bar{\beta}=:q([\alpha,\beta])$. Note this quadratic form coincides with the norm form on the quaternion algebra $B_{p,L}$; writing

$$[\alpha,\beta]=[\alpha,0]+[0,\beta][0,1]=(\alpha_1+\alpha_2 i)+(\beta_1+\beta_2 i)j,$$

where $i^2=d$ and $j^2=\alpha_0 p$, we have

$$\begin{aligned}\mathrm{Norm}(\alpha_1+\alpha_2 i+\beta_1 j+\beta_2 ij)&=\alpha_1^2-\alpha_2^2 d-\beta_1^2\alpha_0 p+\beta_2^2 d\alpha_0 p\\&=(\alpha_1+\alpha_2 i)(\alpha_1-\alpha_2 i)-\alpha_0 p(\beta_1+\beta_2 i)(\beta_1-\beta_2 i)\\&=\alpha\bar{\alpha}-\alpha_0 p\beta\bar{\beta}.\end{aligned}$$

The associated bilinear form is

$$\langle[\alpha,\beta],[\gamma,\delta]\rangle=\alpha\bar{\gamma}+\bar{\alpha}\gamma-\alpha_0 p(\beta\bar{\delta}+\bar{\beta}\delta),$$

where $\frac{1}{2}\langle x,x\rangle=q(x)$. Note that $\langle[\alpha,0],[0,\delta]\rangle=0$,

$$\langle[\alpha_1,0],[\alpha_2,0]\rangle=\alpha_1\bar{\alpha}_2+\bar{\alpha}_1\alpha_2=\mathrm{Tr}_{K/L}\,\alpha_1\bar{\alpha}_2,$$

$$\langle[0,\beta_1],[0,\beta_2]\rangle=-\alpha_0 p(\beta_1\bar{\beta}_2+\bar{\beta}_1\beta_2)=-\alpha_0 p\,\mathrm{Tr}_{K/L}\,\beta_1\bar{\beta}_2.$$

To compute the discriminant of R' with respect to the bilinear form, we need to compute the determinant of the matrix $(\langle x_i,x_j\rangle)$ for $\{x_i\}$ a basis for R'. Choose a basis $\{w_1,w_2\}$ for $\mathbb{O}_K$ as an $\mathbb{O}_L$-module (for example, $\{1,t\}$). Choose a basis $\{w_3,w_4\}$ for $l\mathfrak{a}^{-1}\bar{\mathfrak{a}}$ as an $\mathbb{O}_L$-module. By the above calculations, we see that

$$\det(\langle w_i,w_j\rangle)=\det(M_1)\det(M_2),$$

where

$$M_1=\begin{pmatrix}2w_1\overline{w_1} & w_1\overline{w_2}+w_2\overline{w_1}\\ w_1\overline{w_2}+w_2\overline{w_1} & 2w_2\overline{w_2}\end{pmatrix}=(\mathrm{Tr}(w_i\overline{w_j})),\quad i,j=1,2,$$

$$M_2=-\alpha_0 p\begin{pmatrix}2w_3\overline{w_3} & w_3\overline{w_4}+w_4\overline{w_3}\\ w_3\overline{w_4}+w_4\overline{w_3} & 2w_4\overline{w_2}\end{pmatrix}=-\alpha_0 p(\mathrm{Tr}(w_i\overline{w_j})),\quad i,j=3,4.$$

We have

$$\det(M_1)=-\operatorname{disc}_{K/L}(\mathbb{O}_K)\quad\text{and}\quad\det(M_2)=-(\alpha_0 p)\operatorname{disc}_{K/L}(l\mathfrak{a}^{-1}\bar{\mathfrak{a}}).$$

For any $\mathbb{O}_K$-ideal $\mathfrak{b}$, $\operatorname{disc}_{K/L}(\mathfrak{b})=\operatorname{disc}_{K/L}(\mathbb{O}_K)\,\mathrm{Norm}_{K/L}(\mathfrak{b})^2$ [Lang 1986, Proposition 13, p. 66], so

$$\operatorname{disc}(R')=\operatorname{disc}_{K/L}(\mathbb{O}_K)^2\,\mathrm{Norm}_{K/L}(l\mathfrak{a}^{-1}\bar{\mathfrak{a}})^2(\alpha_0 p)^2=(l\alpha_0 pd)^2.$$

We remark that this uses that l is split in K/L. In a typical application, l will be a prime lying above p. If p is inert in L, then it will automatically be split in K/L according to the hypotheses of Proposition 3.2. If l is not split in K/L, we get a higher power of l in the final answer. □

In order to show that R has discriminant $p \cdot l$, the following lemma is needed:

Lemma 4.5. *The following sequence is exact*:

$$0 \to R' \hookrightarrow R \xrightarrow{\psi} \mathcal{D}^{-1}\mathcal{A}^{-1}/\mathcal{O}_K \to 0,$$

where

$$[\alpha, \beta] \mapsto \beta \in \frac{\mathcal{D}^{-1}\mathcal{A}^{-1} l \mathfrak{a}^{-1}\bar{\mathfrak{a}}}{l\mathfrak{a}^{-1}\bar{\mathfrak{a}}} \cong \mathcal{D}^{-1}\mathcal{A}^{-1}/\mathcal{O}_K.$$

Proof. First, $R' \subseteq R$ because $\alpha \in \mathcal{O}_K$ and $\lambda\beta \in \lambda l \mathfrak{a}^{-1}\bar{\mathfrak{a}} = (\lambda\mathfrak{a}^{-1}\bar{\mathfrak{a}})l \subseteq \mathcal{O}_K l \subseteq \mathcal{O}_K$. Since $\lambda\beta \in \mathcal{O}_K$, clearly $\alpha \equiv \lambda\beta \bmod \mathcal{O}_K$. Now:

- Exactness at R: Clearly $R' \subseteq \mathrm{Ker}(\psi)$. Now suppose $[\alpha, \beta] \in \mathrm{Ker}(\psi)$. Then $\beta \in l\mathfrak{a}^{-1}\bar{\mathfrak{a}}$, and so $\alpha \in \mathcal{O}_K$ because $\lambda\beta \in \mathcal{O}_K$ by the definition of λ and $\alpha \equiv \lambda\beta \bmod \mathcal{O}_K$. So $[\alpha, \beta] \in R'$.
- Surjectivity of ψ: Let $\beta \in \mathcal{D}^{-1}\mathcal{A}^{-1} l \mathfrak{a}^{-1}\bar{\mathfrak{a}}$. Then we have $[\lambda\beta, \beta] \in R$ because $\lambda\beta \in \mathcal{D}^{-1} l(\lambda\mathcal{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}) \subseteq \mathcal{D}^{-1} l \mathcal{O}_K \subseteq \mathcal{D}^{-1}$. □

Thus, $\mathrm{disc}_{K/L}(R) = \mathrm{disc}_{K/L}(R')/\mathrm{Norm}_{K/L}(\mathcal{D}\mathcal{A})^2 = (l\alpha_0 pd)^2/(\alpha_0 d)^2 = l^2p^2$, so the discriminant of R as an order of $B_{p,L}$ is lp. This proves conclusion (2).

(3) Finally, R is independent of the choice of λ assuming λ satisfies the same local sign conditions. Suppose both λ and λ' satisfy the conditions of Definition 4.1. Let $[\alpha, \beta] \in R(\mathfrak{a}, \lambda, l)$, so $\alpha \in \mathcal{D}^{-1}$, $\beta \in \mathcal{D}^{-1}\mathcal{A}^{-1} l \mathfrak{a}^{-1}\bar{\mathfrak{a}}$, and $\alpha \equiv \lambda\beta \bmod \mathcal{O}_K$. Then

$$\alpha - \lambda\beta \in \mathcal{O}_K \Longrightarrow (\sqrt{d}\alpha) - \lambda(\sqrt{d}\beta) \in (\sqrt{d}),$$

and

$$(\sqrt{d}\alpha) - \lambda'(\sqrt{d}\beta) - (\lambda - \lambda')(\sqrt{d}\beta) \in (\sqrt{d}).$$

Now, because d is square-free and for all $\mathfrak{q} | d$ we have $\lambda' = e(\mathfrak{a}, \mathfrak{q})\lambda_{\mathfrak{q}} \equiv \lambda \bmod \mathfrak{q}$, it follows that $\lambda - \lambda' \in (d)$. But

$$\lambda - \lambda' \in (d) \Longrightarrow (\lambda - \lambda')\sqrt{d}\beta \in dl\mathcal{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$$

and

$$\lambda\sqrt{d}\beta - \lambda'\sqrt{d}\beta \in \mathcal{O}_K$$

by the definitions of λ and λ', so

$$(\lambda - \lambda')\sqrt{d}\beta \in \mathcal{O}_K \cap dl\mathcal{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}} \subseteq (d).$$

It follows that $(\sqrt{d}\alpha) - \lambda'(\sqrt{d}\beta) \in (\sqrt{d})$, so $\alpha \equiv \lambda'\beta \bmod \mathcal{O}_K$. □

5. Classification of superspecial orders of $B_{p,L}$ in which $\mathbb{O}_K$ embeds, having chosen an embedding $K \hookrightarrow B_{p,L}$

By a superspecial order in $B_{p,L}$, we mean an order of discriminant $p\mathbb{O}_L$. An example is $R \otimes_{\mathbb{Z}} \mathbb{O}_L$ for a maximal order R of $B_{p,\infty}$. Let K be a primitive CM field such that $K^+ = L$. As before, d will denote a totally negative generator of the relative different ideal $\mathscr{D}_{K/L}$. In this section, we classify the superspecial orders in which $\mathbb{O}_K$ embeds, relying on the results in Section 4 and making the particular choice of local signs $\varepsilon(\mathfrak{a}, \mathfrak{q}) = (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a})}$, where $\tilde{\mathfrak{q}} \lhd \mathbb{O}_K$ is an ideal such that $\mathfrak{q}\mathbb{O}_K = \tilde{\mathfrak{q}}^2$, and we denote $\lambda_{\mathfrak{a}}$ the corresponding λ. We shall prove that, once the embedding $K \hookrightarrow B_{p,L}$ has been fixed, the isomorphism classes of the superspecial orders in which $\mathbb{O}_K$ embeds are in bijection with the ideal class group of K (Theorem 5.7). Our classification of these orders will be achieved through a series of lemmas:

Lemma 5.1. *Let R_1 and R_2 be two superspecial orders in $B_{p,L}$. Then $R_1 \cong R_2$ over K if and only if there exists $\mu \in K$ such that $R_1 = \mu R_2 \mu^{-1}$.*

Proof. By Skolem–Noether, $R_1 \cong R_2$ if and only if there exists $\mu \in B_{p,L}^{\times}$ such that $R_1 = \mu R_2 \mu^{-1}$. This is a K-automorphism if and only if $\mu \in \mathrm{Cent}_{B_{p,L}}(K) = K$. □

Lemma 5.2. *Given $\mathfrak{a}$ and λ as in Definition 4.1, there exists $\mathfrak{c} \mid d$ such that we have $R(\mathfrak{a}, \lambda) = R(\mathfrak{ac}, \lambda_{\mathfrak{ac}})$.*

Proof. We have $R(\mathfrak{ac}, \lambda_{\mathfrak{ac}}, l) = R(\mathfrak{a}, \lambda_{\mathfrak{a}} \cdot \lambda_{(-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{c})}}, l)$ because

$$\lambda_{\mathfrak{ac}} \equiv (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{ac})} \lambda_{\mathfrak{q}} \bmod \mathfrak{q} \quad \text{for all } \mathfrak{q} \mid d,$$

so

$$\lambda_{\mathfrak{ac}} \equiv \lambda_{\mathfrak{a}} (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{c})} \bmod \mathfrak{q} \quad \text{for all } \mathfrak{q} \mid d.$$

So as $\mathfrak{c}$ ranges over the ideals dividing d, we get all sign vectors $\varepsilon(\mathfrak{a})$ that appear in the left-hand side and each one once. □

Lemma 5.3. *Fix $\{\mathfrak{b}_1, \ldots, \mathfrak{b}_h\}$ representatives for the class group of K and the choice of local signs as above. Then every $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$ is isomorphic to $R(\mathfrak{b}, \lambda_{\mathfrak{b}})$ for some $\mathfrak{b} \in \{\mathfrak{b}_1, \ldots, \mathfrak{b}_h\}$.*

Proof. Let $\mu \in K^{\times}$ be such that $\mathfrak{b} = \mu\mathfrak{a}$ for some (unique) $\mathfrak{b} \in \{\mathfrak{b}_1, \ldots, \mathfrak{b}_h\}$. Then

$$\begin{aligned}
&\mu^{-1} R(\mathfrak{a}, \lambda_{\mathfrak{a}}) \mu \\
&= \left\{ \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \bar{\mu}^{-1} \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \alpha_0 p \bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \mu & 0 \\ 0 & \bar{\mu} \end{pmatrix} \right. \\
&\qquad \left. : \alpha \in \mathscr{D}^{-1},\ \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}},\ \alpha \equiv \lambda_{\mathfrak{a}}\beta \bmod \mathbb{O}_K \right\} \\
&= \left\{ \begin{pmatrix} \alpha & (\bar{\mu}/\mu)\beta \\ \alpha_0 p \overline{((\bar{\mu}/\mu)\beta)} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathscr{D}^{-1},\ \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}},\ \alpha \equiv \lambda_{\mathfrak{a}}\beta \bmod \mathbb{O}_K \right\}.
\end{aligned}$$

By setting $b = \frac{\overline{\mu}}{\mu}\beta$, this is equal to

$$\left\{ \begin{pmatrix} \alpha & b \\ \alpha_0 p\bar{b} & \bar{\alpha} \end{pmatrix} : \alpha \in \mathscr{D}^{-1},\ b \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}},\ \alpha \equiv \lambda_{\mathfrak{a}}\frac{\mu}{\overline{\mu}}b \bmod \mathbb{O}_K \right\}$$

because $\mathfrak{b} = \mu\mathfrak{a}$,

$$\frac{\overline{\mu}}{\mu}\beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}\frac{\overline{\mu}}{\mu} = \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}},$$

and $\alpha \equiv \lambda_{\mathfrak{a}}(\mu/\overline{\mu})(\overline{\mu}/\mu)\beta = \lambda_{\mathfrak{a}}(\mu/\overline{\mu})b \bmod \mathbb{O}_K$.

Now it remains to show $\alpha \equiv \lambda_{\mathfrak{a}}(\mu/\overline{\mu})b \bmod \mathbb{O}_K$ if and only if $\alpha \equiv \lambda_{\mathfrak{b}}b \bmod \mathbb{O}_K$. In other words, we must show that the following two conditions are equivalent:

$$(\sqrt{d}\alpha) \equiv \lambda_{\mathfrak{a}}\frac{\mu}{\overline{\mu}}(\sqrt{d}b) \bmod \tilde{\mathfrak{q}} \quad \text{for all } \tilde{\mathfrak{q}} \mid \sqrt{d}\mathbb{O}_K,$$

$$(\sqrt{d}\alpha) \equiv \lambda_{\mathfrak{b}}(\sqrt{d}b) \bmod \tilde{\mathfrak{q}} \quad \text{for all } \tilde{\mathfrak{q}} \mid \sqrt{d}\mathbb{O}_K.$$

This can be checked in $\mathbb{O}_{K_{\tilde{\mathfrak{q}}}}$ for every $\tilde{\mathfrak{q}}$. The point is that $(-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{b})} = (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a})} \cdot (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mu)}$, and so it is enough to show that $\mu/\overline{\mu} \equiv (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mu)} \bmod \tilde{\mathfrak{q}}$. This follows from the fact that $\mathbb{O}_{K_{\tilde{\mathfrak{q}}}} = \mathbb{O}_{L_{\mathfrak{q}}}[\pi]$ with $\overline{\pi} = -\pi$, so writing $\mu = \pi^r \cdot u$ with $u \in \mathbb{O}_{K_{\tilde{\mathfrak{q}}}}^{\times}$, we have $\bar{u} = u \bmod \tilde{\mathfrak{q}}$ and

$$\frac{\mu}{\overline{\mu}} = (-1)^r\frac{u}{\bar{u}} \equiv (-1)^r \bmod \tilde{\mathfrak{q}}.$$

Thus, we have proved that $\mu^{-1}R(\mathfrak{a}, \lambda_{\mathfrak{a}})\mu = R(\mu\mathfrak{a}, \lambda_{\mu\mathfrak{a}})$. □

Lemma 5.4. *We have* $R(\mathfrak{a}, \lambda_{\mathfrak{a}}) = R(\mathfrak{b}, \lambda_{\mathfrak{b}})$ *if and only if* $\mathfrak{a}^{-1}\bar{\mathfrak{a}} = \mathfrak{b}^{-1}\bar{\mathfrak{b}}$ *and* $\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a}) \equiv \mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{b}) \bmod 2$ *for all* $\tilde{\mathfrak{q}} \mid d$.

Proof. ($\Leftarrow$) This is obvious.

($\Rightarrow$) Let $\beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$ and $\alpha := \lambda_{\mathfrak{a}}\beta$. Since $\lambda_{\mathfrak{a}}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}} \subseteq \mathbb{O}_K$, it follows that $\alpha \in \mathscr{D}^{-1}$. Therefore, $[\alpha, \beta] \in R(\mathfrak{a}, \lambda_{\mathfrak{a}}) = R(\mathfrak{b}, \lambda_{\mathfrak{b}})$, so $\beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}}$. Therefore, $\mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}} \subseteq \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{b}^{-1}\bar{\mathfrak{b}}$. By symmetry, we have equality.

Furthermore, since $[\lambda_{\mathfrak{a}}\beta, \beta] \in R(\mathfrak{b}, \lambda_{\mathfrak{b}})$, we have

$$\lambda_{\mathfrak{a}}\beta \equiv \lambda_{\mathfrak{b}}\beta \bmod \mathbb{O}_K \quad \text{for all } \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}.$$

Otherwise said,

$$\beta(\lambda_{\mathfrak{a}} - \lambda_{\mathfrak{b}}) \equiv 0 \bmod \mathbb{O}_K \quad \text{for all } \beta \in \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}},$$

and this implies

$$\lambda_{\mathfrak{a}} \equiv \lambda_{\mathfrak{b}} \bmod \mathscr{D}^{-1}\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}.$$

We conclude that

$$\lambda_{\mathfrak{a}} \equiv \lambda_{\mathfrak{b}} \bmod \tilde{\mathfrak{q}} \quad \text{for all } \tilde{\mathfrak{q}} \mid d \quad (\text{because } (\mathscr{D}, \mathscr{A}\mathfrak{a}\bar{\mathfrak{a}}^{-1}) = 1).$$

It follows that

$$(-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a})} = (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{b})} \quad \text{for all } \tilde{\mathfrak{q}} \mid d. \qquad \square$$

Lemma 5.5. *For* $\mathfrak{b}, \mathfrak{b}' \in \{\mathfrak{b}_1, \ldots, \mathfrak{b}_h\}$, $R(\mathfrak{b}, \lambda_{\mathfrak{b}}) \sim R(\mathfrak{b}', \lambda_{\mathfrak{b}'})$ *if and only if* $\mathfrak{b} = \mathfrak{b}'$.

Proof. ($\Leftarrow$) This is obvious.

($\Rightarrow$) Suppose $R(\mathfrak{b}, \lambda_{\mathfrak{b}}) = \mu^{-1} R(\mathfrak{b}', \lambda_{\mathfrak{b}'})\mu = R(\mu\mathfrak{b}', \lambda_{\mu\mathfrak{b}'})$ (this second equality was proved in Lemma 5.3 above). By Lemma 5.4, this implies

$$\mathfrak{b}^{-1}\bar{\mathfrak{b}} = \mathfrak{b}'^{-1}\bar{\mathfrak{b}}'\frac{\bar{\mu}}{\mu} \quad \text{or} \quad \mathfrak{b}'\mathfrak{b}^{-1}\mu = \overline{\mathfrak{b}'\mathfrak{b}^{-1}\mu}.$$

An ideal $\mathfrak{f} \lhd \mathbb{O}_K$ satisfies $\mathfrak{f} = \bar{\mathfrak{f}}$ if and only if $\mathfrak{f} = j \cdot \prod_{\tilde{\mathfrak{q}} \mid d} \tilde{\mathfrak{q}}^{s(\tilde{\mathfrak{q}})}$ for $j \in L$. Indeed, write $\mathfrak{f}$ as a product of inert, split, and ramified prime ideals. Inert prime ideals are generated by elements of L. Split prime ideals must appear in the factorization to the same power as their complex conjugate because of the condition $\mathfrak{f} = \bar{\mathfrak{f}}$. Thus, it is actually some power of their norm that appears, and that is also generated by an element of L. What remains is a product of some ramified primes.

Applying this to the ideal $\mathfrak{f} = \mathfrak{b}'\mathfrak{b}^{-1}\mu$, we find that

$$\mu\mathfrak{b}' = j \cdot \prod_{\tilde{\mathfrak{q}} \mid d} \tilde{\mathfrak{q}}^{s(\tilde{\mathfrak{q}})} \cdot \mathfrak{b}.$$

Note that $R(\mu\mathfrak{b}', \lambda_{\mu\mathfrak{b}'}) = R((\mu/j)\mathfrak{b}', \lambda_{(\mu/j)\mathfrak{b}'})$, so we can replace μ by μ/j to obtain $R(\mathfrak{b}, \lambda_{\mathfrak{b}}) = R(\mu\mathfrak{b}', \lambda_{\mu\mathfrak{b}'})$ with $\mu\mathfrak{b}'$ of the form

$$\mu\mathfrak{b}' = \prod_{\tilde{\mathfrak{q}} \mid d} \tilde{\mathfrak{q}}^{s(\tilde{\mathfrak{q}})} \cdot \mathfrak{b}.$$

Now $\lambda_{\mathfrak{b}} = \lambda_{\mu\mathfrak{b}'}$ implies that each $s(\tilde{\mathfrak{q}})$ is even, so $\mu\mathfrak{b}' = k\mathfrak{b}$ for some $k \in K$. Thus, $\mathfrak{b}' = \mathfrak{b}$ because they are already representatives for the class group. $\square$

Lemma 5.6. *Any superspecial order* $R \supseteq \mathbb{O}_K$ *is isomorphic to some* $R(\mathfrak{a}, \lambda)$.

Proof. Let $\mathfrak{c}$ be a prime ideal of L. For any ideal $\mathfrak{a}$ of $K_{\mathfrak{c}}$, define orders $R^{\mathfrak{c}}(\mathfrak{a}, \lambda_{\mathfrak{a}})$ of $(B_{p,L})_{\mathfrak{c}}$ exactly the same way as for $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$. The orders have the same properties that were proved for the $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$ in Proposition 4.2: independent of the choice of λ and conductor $p\mathbb{O}_{L_{\mathfrak{c}}}$.

Then for an ideal $\mathfrak{a}$ of K, we have $R(\mathfrak{a}, \lambda_{\mathfrak{a}})_{\mathfrak{c}} = R^{\mathfrak{c}}(\mathfrak{a}_{\mathfrak{c}}, \lambda_{\mathfrak{a}_{\mathfrak{c}}})$. Let R be an order of $B_{p,L}$ that contains $\mathbb{O}_K$ of discriminant $p\mathbb{O}_L$. For every $\mathfrak{c}$, the order $R_{\mathfrak{c}}$ is an Eichler order of discriminant $p\mathbb{O}_{L_{\mathfrak{c}}}$ as is the order $R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}}$, where $\mathbb{O}$ represents the trivial ideal class. For every $\mathfrak{c}$, there is a $\mu_{\mathfrak{c}} \in (B_{p,L})_{\mathfrak{c}}^{\times}$ such that

$$R_{\mathfrak{c}} = \mu_{\mathfrak{c}}^{-1} R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}} \mu_{\mathfrak{c}}$$

because Eichler orders of the same discriminant are locally conjugate. Furthermore,

$$R_{\mathfrak{c}} = \mathrm{M}_2(\mathbb{O}_{L_{\mathfrak{c}}}) \subseteq (B_{p,L})_{\mathfrak{c}} = \mathrm{M}_2(L_{\mathfrak{c}})$$

for almost all $\mathfrak{c}$, and the same holds for $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$. Now it is enough to show that we can choose $\mu_{\mathfrak{c}} \in K_{\mathfrak{c}}^{\times}$ for all $\mathfrak{c}$ because in that case

$$R_{\mathfrak{c}} = \mu_{\mathfrak{c}}^{-1} R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}} \mu_{\mathfrak{c}} = R^{\mathfrak{c}}((\mu_{\mathfrak{c}}), \lambda_{(\mu_{\mathfrak{c}})})$$

for a collection of elements

$$\{\mu_{\mathfrak{c}} : \mathfrak{c} \lhd \mathbb{O}_L \text{ prime}, \mu_{\mathfrak{c}} = 1 \text{ for almost all } \mathfrak{c}, \mu_{\mathfrak{c}} \in K_{\mathfrak{c}}^{\times}\}.$$

Therefore, there is an ideal $\mathfrak{a}$ of K such that, for all $\mathfrak{c}$, $\mathfrak{a}_{\mathfrak{c}} = (\mu_{\mathfrak{c}})$. The two orders R and $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$ are equal because they are equal locally everywhere, and we are done.

To show that we may choose $\mu_{\mathfrak{c}} \in K_{\mathfrak{c}}^{\times}$ for all $\mathfrak{c}$, we use [Vignéras 1980, Theorems 3.1 and 3.2, pages 43–44] to produce an element $\nu_{\mathfrak{c}}$ such that

(1) $\nu_{\mathfrak{c}}^{-1}(\mu_{\mathfrak{c}}^{-1} R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}} \mu_{\mathfrak{c}})\nu_{\mathfrak{c}} = \mu_{\mathfrak{c}}^{-1} R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}} \mu_{\mathfrak{c}} = R_{\mathfrak{c}}$ and

(2) the embedding of $\mathbb{O}_{K_{\mathfrak{c}}}$ into $R_{\mathfrak{c}}$ is the embedding of $\mathbb{O}_{K_{\mathfrak{c}}}$ into $R(\mathbb{O}, \lambda_{\mathbb{O}})_{\mathfrak{c}}$ conjugated by $\nu_{\mathfrak{c}}\mu_{\mathfrak{c}}$.

Since conjugation by $\nu_{\mathfrak{c}}\mu_{\mathfrak{c}}$ fixes $K_{\mathfrak{c}}$ pointwise, this implies $\nu_{\mathfrak{c}}\mu_{\mathfrak{c}}$ commutes with $K_{\mathfrak{c}}$, and so $\nu_{\mathfrak{c}}\mu_{\mathfrak{c}} \in K_{\mathfrak{c}}^{\times}$. □

Our conclusion is that isomorphism classes of superspecial orders of $B_{p,L}$ in which $\mathbb{O}_K$ embeds are the isomorphism classes of $R(\mathfrak{a}, \lambda_{\mathfrak{a}})$. Thus, we have proved the following theorem:

Theorem 5.7. *Fix an embedding of $K \hookrightarrow B_{p,L}$. The isomorphism classes of the superspecial orders in which $\mathbb{O}_K$ embeds are in bijection with the ideal class group of K via the map*

$$[\mathfrak{a}] \mapsto R(\mathfrak{a}, \lambda_{\mathfrak{a}}).$$

Remark 5.8. In the case $L = \mathbb{Q}$, Theorem 5.7 provides a different proof for the main theorems of Dorman's paper [1989a] on global orders in definite quaternion algebras and corrects several minor errors and gaps in the proofs there. For example, we correct the missing condition on the integrality for $\lambda\mathfrak{D}^{-1}\mathfrak{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$ and the resulting mistake in the proof of Proposition 2, and we give a different proof of the one-to-one correspondence.

6. Main theorems on counting formulas

6.1. ***Assumptions and notation.*** Let L be a totally real field of degree g of strict class number 1, p a rational prime that is unramified in L, and K a primitive CM field with $K^+ = L$. Using the same notation as in Lemma 2.2, write the ring of

integers of K, $\mathbb{O}_K = \mathbb{O}_L[t]$, where $t^2 + at + b = 0$ for some $a, b \in \mathbb{O}_L$, and the different $\mathfrak{D} = \mathfrak{D}_{K/L} = (\sqrt{d})$ with $d = a^2 - 4b$ a totally negative element of $\mathbb{O}_L$.

Assume as in Proposition 3.2 that all primes $\mathfrak{p} \in S \setminus S_0$ split in K and all primes $\mathfrak{p} \in S_0$ are inert in K and that the discriminant $\mathfrak{d}_{K/L} = (d)$ satisfies $(d, 2) = 1$ and $(d, p) = 1$. Let $\alpha_0 \in \mathbb{O}_L$ be a totally negative prime element such that

$$B_{p,L} \cong \left(\frac{d, \alpha_0 p}{L}\right),$$

where $(\alpha_0, 2pd) = 1$, $\alpha_0 \equiv p \mod \mathfrak{q}$ for each $\mathfrak{q} \mid d$, $\alpha_0 \equiv 1 \mod p$, and $\alpha_0 \mathbb{O}_K = \mathscr{A} \cdot \bar{\mathscr{A}}$.

For $l \in \mathbb{O}_L$ such that $(l, \alpha_0 d \mathfrak{a}^{-1} \bar{\mathfrak{a}}) = 1$, let

$$R := R(\mathfrak{a}, \lambda, l) = \left\{[\alpha, \beta] : \alpha \in \mathfrak{D}^{-1}, \beta \in \mathfrak{D}^{-1} \mathscr{A}^{-1} l \mathfrak{a}^{-1} \bar{\mathfrak{a}}, \alpha \equiv \lambda\beta \mod \mathbb{O}_K\right\}.$$

6.2. ***Counting simultaneous embeddings.*** Let K' be another CM field that has $\mathbb{O}_{K'} = \mathbb{O}_L[w]$ and

$$\operatorname{disc}_{K'/L} = (\operatorname{Tr}(w)^2 - 4 \operatorname{Norm}(w)) = (d')$$

generated by a totally negative element d' of L.

Now we are assuming we are in the situation where an abelian variety A with CM by K has superspecial reduction modulo p, and we fix an isomorphism

$$\operatorname{End}_{\mathbb{O}_L}(A) \cong R(\mathfrak{a}, \lambda)$$

for some unique $\mathfrak{a} \lhd \mathbb{O}_K$ (Lemma 5.6, Theorem 5.7). Then, to count simultaneous embeddings of $\mathbb{O}_{K'} = \mathbb{O}_L[\omega]$, i.e., embeddings $\mathbb{O}_{K'} \to \operatorname{End}_{\mathbb{O}_L}(A)$, we count elements $[\alpha, \beta] \in R(\mathfrak{a}, \lambda)$ with trace equal to $\operatorname{Tr}(\omega)$ and with norm equal to $\operatorname{Norm}(\omega)$, that is, elements of the set $S(\mathfrak{a}, \lambda, 1)$, where

$$S(\mathfrak{a}, \lambda, l) = \left\{[\alpha, \beta] = \begin{pmatrix} \alpha & \beta \\ \alpha_0 p \bar{\beta} & \bar{\alpha} \end{pmatrix} \in R(\mathfrak{a}, \lambda, l) \right. \\ \left. : \operatorname{Tr}[\alpha, \beta] = \operatorname{Tr}(w), \operatorname{Norm}[\alpha, \beta] = \operatorname{Norm}(w)\right\}.$$

Let $[\alpha, \beta]$ be an element of this set. Since

$$\mathbb{O}_K = \mathbb{O}_L + \mathbb{O}_L \cdot \frac{a + \sqrt{d}}{2} = \left\{\frac{2l_1 + l_2(a + \sqrt{d})}{2} : l_1, l_2 \in \mathbb{O}_L\right\} \\ = \left\{\frac{l_3 + l_4\sqrt{d}}{2} : l_3, l_4 \in \mathbb{O}_L, l_3 - a l_4 \equiv 0 \mod 2\mathbb{O}_L\right\},$$

we can write $\alpha \in \mathfrak{D}^{-1}$ in the form $\alpha = (l_3 + l_4\sqrt{d})/2\sqrt{d}$, where $l_3, l_4 \in \mathbb{O}_L$ with $l_3 - a l_4 \equiv 0 \mod 2\mathbb{O}_L$, and in this notation, $\operatorname{Tr}(\alpha) = \operatorname{Tr}([\alpha, \beta]) = l_4$. So

$$\alpha = \frac{x + \operatorname{Tr}(w)\sqrt{d}}{2\sqrt{d}}, \quad x \in \mathbb{O}_L,\ x - a \operatorname{Tr}(w) \equiv 0 \mod 2\mathbb{O}_L,$$

where $a = -\mathrm{Tr}(t)$ and

$$\beta = \frac{l}{\sqrt{d}}\gamma, \quad \gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}.$$

Since

$$\begin{aligned}\mathrm{Norm}[\alpha,\beta] &= \det[\alpha,\beta] = \alpha\bar{\alpha} - \alpha_0 p\beta\bar{\beta} \\ &= \frac{x + \mathrm{Tr}(w)\sqrt{d}}{2\sqrt{d}} \cdot \frac{x - \mathrm{Tr}(w)\sqrt{d}}{-2\sqrt{d}} - \alpha_0 p \frac{l^2}{-d}\gamma\bar{\gamma} \\ &= \frac{1}{-4d}(x^2 - \mathrm{Tr}(w)^2 d - 4\alpha_0 p l^2 \gamma\bar{\gamma}),\end{aligned}$$

it follows that

$$-d\left(4\,\mathrm{Norm}(w) - \mathrm{Tr}(w)^2\right) = x^2 - 4\alpha_0 p l^2 \gamma\bar{\gamma}.$$

So an element $[\alpha,\beta]$ of the set $S(\mathfrak{a},\lambda,l)$ gives rise to a solution (x,γ) to

$$dd' = x^2 - 4\alpha_0 p l^2 \gamma\bar{\gamma}$$

with $\gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$, $x \in \mathbb{O}_L$, and $x \equiv a\,\mathrm{Tr}(w) \bmod 2\mathbb{O}_L$, where $x^2 - dd'$ is a totally negative element of $\mathbb{O}_L$ because α_0 is. Call this set of conditions on x conditions **C**.

Our analysis allows us to define a function $\phi : S(\mathfrak{a},\lambda,l) \to S_1(\mathfrak{a},x,l)$ that sends $[\alpha,\beta] \mapsto \gamma$ (it is used in the proof of Theorem 6.5 below), where the set $S_1(\mathfrak{a},x,l)$ is defined for an integral ideal $\mathfrak{a}$ and x satisfying conditions **C** by

$$S_1(\mathfrak{a},x,l) := \left\{\gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}} : \mathrm{Norm}(\gamma) = \gamma\bar{\gamma} = \frac{x^2 - dd'}{4\alpha_0 p l^2}\right\}.$$

For $\gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$, the ideal generated by γ can be written as $(\gamma) = \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}} \cdot \mathfrak{b}$ for $\mathfrak{b}$ an ideal of $\mathbb{O}_K$, and $\mathrm{Norm}(\mathfrak{b}) = \alpha_0\,\mathrm{Norm}(\gamma)$. We let $S_2(\mathfrak{a},x,l)$ be the set

$$S_2(\mathfrak{a},x,l) := \left\{\mathfrak{b} \lhd \mathbb{O}_K : \mathrm{Norm}(\mathfrak{b}) = \frac{x^2 - dd'}{4pl^2},\ \mathfrak{b} \sim \mathfrak{a}^2\mathscr{A}\right\}.$$

Proposition 6.1. *The map $S_1(\mathfrak{a},x,l) \to S_2(\mathfrak{a},x,l)$ that sends $\gamma \mapsto \mathfrak{b}_\gamma = (\gamma)\mathscr{A}\mathfrak{a}\bar{\mathfrak{a}}^{-1}$ is a surjective $[w_K : 1]$-map, where w_K equals the number of roots of unity in K.*

Proof. To show that the map is $[w_K : 1]$, we first show $\mathfrak{b}_\gamma = \mathfrak{b}_\delta$ if and only if $\gamma = \mu\delta$, where μ is a root of unity in K. Since $\mathfrak{b}_\gamma$ depends only on (γ), the "only if" part is clear. Now if $\mathfrak{b}_\gamma = \mathfrak{b}_\delta$, then $(\gamma) = (\delta)$, so $\gamma = \mu\delta$ for some $\mu \in \mathbb{O}_K{}^\times$, but also $\mathrm{Norm}(\gamma) = \mathrm{Norm}(\delta) = \mathrm{Norm}(\mu)\cdot\mathrm{Norm}(\gamma)$ implies $\mathrm{Norm}(\mu) = 1$ implies $\mu \in \mu_K$.

Next we show that the map is surjective. Given $\mathfrak{b} \in S_2(\mathfrak{a},x,l)$, let γ be a generator of $\mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}\mathfrak{b}$. Then $\gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$, and

$$(\mathrm{Norm}(\gamma)) = (\gamma\bar{\gamma}) = \left(\frac{x^2 - dd'}{4\alpha_0 p l^2}\right).$$

Hence, there exists a totally positive unit $\epsilon' \in {\mathbb{O}_L}^{\times +} = {\mathbb{O}_L}^{\times 2}$ with $\epsilon' = \epsilon^2$ such that

$$\epsilon' \gamma \bar{\gamma} = \frac{x^2 - dd'}{4\alpha_0 p l^2}.$$

Changing γ to $\epsilon\gamma$,

$$\gamma \bar{\gamma} = \frac{x^2 - dd'}{4\alpha_0 p l^2}.$$

So $\gamma \in S_1(\mathfrak{a}, x, l)$, and since it is still true that $(\gamma) = \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}\mathfrak{b}$, we have $\mathfrak{b}_\gamma = \mathfrak{b}$. □

Now given an element γ of $S_1(\mathfrak{a}, x, l)$, we can construct elements of $S(\mathfrak{a}, \lambda, l)$ as follows. Let

$$\alpha = \frac{x + \mathrm{Tr}(w)\sqrt{d}}{2\sqrt{d}} \quad \text{and} \quad \beta = \frac{l}{\sqrt{d}}\gamma.$$

First, we note that $\alpha \in \mathscr{D}^{-1}$ if and only if $(x + \mathrm{Tr}(w)\sqrt{d})/2 \in \mathbb{O}_K$ if and only if $x \in \mathbb{O}_L$ and $x \equiv a\,\mathrm{Tr}(w) \bmod 2\mathbb{O}_L$, which holds because x satisfies conditions **C**.

Next, note that $\beta = (l/\sqrt{d})\gamma \in \mathscr{D}^{-1}\mathscr{A}^{-1} l \mathfrak{a}^{-1}\bar{\mathfrak{a}}$ if and only if $\gamma \in \mathscr{A}^{-1}\mathfrak{a}^{-1}\bar{\mathfrak{a}}$, which holds by the definition of the set $S_1(\mathfrak{a}, x)$.

It remains to check that the congruence $\alpha \equiv \lambda\beta \bmod \mathbb{O}_K$ is satisfied. Since $\gamma \in S_1(\mathfrak{a}, x, l)$,

$$x^2 - 4\alpha_0 p l^2 \gamma\bar{\gamma} = dd' \equiv 0 \bmod d.$$

Next, the congruence $\lambda^2 \equiv \alpha_0 p \bmod d$ implies that

$$x^2 - 4\alpha_0 p l^2 \gamma\bar{\gamma} + 4l^2\gamma\bar{\gamma}(\alpha_0 p - \lambda^2) \equiv 0 \bmod d,$$

and so

$$x^2 - 4\lambda^2 l^2 \gamma\bar{\gamma} \equiv 0 \bmod d.$$

Therefore,

$$(x + \mathrm{Tr}(w)\sqrt{d})(x - \mathrm{Tr}(w)\sqrt{d}) - 4\lambda^2 l^2 \gamma\bar{\gamma} \equiv 0 \bmod d.$$

Using $x + \mathrm{Tr}(w)\sqrt{d} = 2\sqrt{d}\alpha$ and $l\gamma = \sqrt{d}\beta$, we get

$$-4d(\alpha\bar{\alpha} - \lambda^2\beta\bar{\beta}) \equiv 0 \bmod d.$$

Since $(d, 2) = 1$, it follows that $\alpha\bar{\alpha} \equiv \lambda^2\beta\bar{\beta} \bmod \mathbb{O}_K$. Now, α and $\lambda\beta$ belong to $\mathscr{D}^{-1} = (1/\sqrt{d})\mathbb{O}_K$, and hence,

$$\alpha_1 := \sqrt{d}\alpha \quad \text{and} \quad \beta_1 := \sqrt{d}\lambda\beta$$

are in $\mathbb{O}_K$, and we have $\alpha_1\bar{\alpha}_1 \equiv \beta_1\bar{\beta}_1 \bmod d$. Equivalently, this relation holds modulo all ideals $\mathfrak{q}$ of $\mathbb{O}_L$ dividing d:

$$\alpha_1\bar{\alpha}_1 \equiv \beta_1\bar{\beta}_1 \bmod \mathfrak{q} \quad \text{for all } \mathfrak{q} \mid d, \mathfrak{q} \lhd \mathbb{O}_L. \tag{6-1}$$

Let $\tilde{\mathfrak{q}} \lhd \mathbb{O}_K$ be a prime such that $\mathfrak{q}\mathbb{O}_K = \tilde{\mathfrak{q}}^2$. Then $\mathbb{O}_K/\tilde{\mathfrak{q}} \cong \mathbb{O}_L/\mathfrak{q}$, and complex conjugation hence acts trivially modulo $\tilde{\mathfrak{q}}$. So (6-1) is equivalent to

$$\alpha_1^2 \equiv \beta_1^2 \bmod \tilde{\mathfrak{q}} \quad \text{for all } \tilde{\mathfrak{q}} | d\mathbb{O}_K, \tilde{\mathfrak{q}} \lhd \mathbb{O}_K,$$

which is equivalent to

$$\alpha_1 \equiv \pm\beta_1 \bmod \tilde{\mathfrak{q}} \quad \text{for all } \tilde{\mathfrak{q}} | d\mathbb{O}_K, \tilde{\mathfrak{q}} \lhd \mathbb{O}_K.$$

So this shows that there exists a choice of signs $\varepsilon(\mathfrak{a}, \mathfrak{q})$ and a λ depending on this choice for which the congruence condition is satisfied, and $[\alpha, \beta] \in S(\mathfrak{a}, \lambda, l)$. However, for any ideal $\mathfrak{q}$ for which $x \equiv 0 \bmod \mathfrak{q}$, both signs will work. This motivates the following definitions and theorem:

Definition 6.2. (1) For $x \in \mathbb{O}_L$, let $\delta(x) := 2^{\#\{\mathfrak{q} | d : x \equiv 0 \bmod \mathfrak{q}\}}$.

(2) Let $\tau := \#\{\mathfrak{q} | d\}$.

For clarity, we also repeat previous definitions.

Definition 6.3 (conditions **C**). We say that $x \in \mathbb{O}_L$ *satisfies* **C** if $x \equiv a\,\mathrm{Tr}(w) \bmod 2\mathbb{O}_L$, $x^2 - dd'$ is totally negative, and $(x^2 - dd')/4pl^2 \in \mathbb{O}_L$.

Definition 6.4. We write $\lambda_{\epsilon(\mathfrak{a})}$ to emphasize the dependence of λ on the choice of signs. For example, for $\mathfrak{a} \lhd \mathbb{O}_K$, let $\lambda_{\mathfrak{a}} = \lambda_{\varepsilon(\mathfrak{a})}$, where $\varepsilon(\mathfrak{a}, \mathfrak{q}) = (-1)^{\mathrm{val}_{\tilde{\mathfrak{q}}}(\mathfrak{a})}$ and $\tilde{\mathfrak{q}} \lhd \mathbb{O}_K$ is an ideal such that $\mathfrak{q}\mathbb{O}_K = \tilde{\mathfrak{q}}^2$.

Theorem 6.5.

(1)
$$\sum_{\varepsilon(\mathfrak{a})} \#S(\mathfrak{a}, \lambda_{\varepsilon(\mathfrak{a})}, l) = \sum_{x \text{ satisfies } \mathbf{C}} \delta(x) \cdot \#S_1(\mathfrak{a}, x, l)$$
$$= w_K \sum_{x \text{ satisfies } \mathbf{C}} \delta(x) \cdot \#S_2(\mathfrak{a}, x, l).$$

(2)
$$\sum_{\varepsilon(\mathfrak{a})} \#S(\mathfrak{a}, \lambda_{\varepsilon(\mathfrak{a})}, l) = \sum_{\substack{\mathfrak{c} | d \\ \mathfrak{c} \lhd \mathbb{O}_K}} \#S(\mathfrak{a}\mathfrak{c}, \lambda_{\mathfrak{a}\mathfrak{c}}, l).$$

Proof. To avoid confusion, we remark that in (1), the first summation is a sum over 2^τ elements, one of them being $\#S(\mathfrak{a}, \lambda_{\mathfrak{a}}, l)$. The second equality of (1) follows from Proposition 6.1. To prove the first equality in (1), we refer to the construction given above of the map $\phi : S(\mathfrak{a}, \lambda, l) \to S_1(\mathfrak{a}, x, l)$. It can be extended to a map

$$\phi : \coprod_{\varepsilon(\mathfrak{a})} S(\mathfrak{a}, \lambda_{\varepsilon(\mathfrak{a})}, l) \to \coprod_{x \text{ satisfies } \mathbf{C}} S_1(\mathfrak{a}, x, l).$$

We claim that ϕ is a surjective map that is $[\delta(x) : 1]$. Given an element γ of $S_1(\mathfrak{a}, x, l)$, we constructed above, for some possible choice of signs $\epsilon(\mathfrak{a})$ determining

λ, an element of $S(\mathfrak{a}, \lambda, l)$

$$\alpha = \frac{x + \mathrm{Tr}(w)\sqrt{d}}{2\sqrt{d}} \quad \text{and} \quad \beta = \frac{l}{\sqrt{d}}\gamma.$$

For any ideal $\tilde{\mathfrak{q}} \mid d$, let $\mu(x, \gamma) \in \{\pm 1\}$ be such that $\alpha_1 \equiv \mu(x, \gamma)\beta_1 \bmod \tilde{\mathfrak{q}}$, where $\alpha_1 = \sqrt{d}\alpha$ and $\beta_1 = \sqrt{d}\lambda\beta$. Given $\varepsilon(\mathfrak{a})$, we have $\alpha \equiv \lambda_{\varepsilon(\mathfrak{a})}\beta \bmod \mathbb{O}_K$ if and only if, for all $\tilde{\mathfrak{q}} \mid d$, either $\alpha_1 \equiv \beta_1 \equiv 0 \bmod \tilde{\mathfrak{q}}$ or $\beta_1 \not\equiv 0 \bmod \tilde{\mathfrak{q}}$ and $\varepsilon(\mathfrak{a}, \mathfrak{q}) \equiv \mu(x, \gamma) \bmod \tilde{\mathfrak{q}}$. It follows that for a given (x, γ), the number of sign vectors $\varepsilon(\mathfrak{a})$ such that we have $\alpha \equiv \lambda_{\varepsilon(\mathfrak{a})}\beta \bmod \mathbb{O}_K$ is equal to

$$2^{\#\{\tilde{\mathfrak{q}} \mid d : \sqrt{d}\alpha \equiv 0 \bmod \tilde{\mathfrak{q}}\}}.$$

Now since $\mathrm{val}_{\tilde{\mathfrak{q}}}(\sqrt{d}\alpha) = \mathrm{val}_{\tilde{\mathfrak{q}}}(x + \mathrm{Tr}(w)\sqrt{d}) \geq \min\{\mathrm{val}_{\tilde{\mathfrak{q}}}(x), \mathrm{val}_{\tilde{\mathfrak{q}}}(\mathrm{Tr}(w)\sqrt{d})\}$, it follows that

$$\mathrm{val}_{\tilde{\mathfrak{q}}}(\sqrt{d}\alpha) > 0 \iff \mathrm{val}_{\tilde{\mathfrak{q}}}(x) > 0 \iff \mathrm{val}_{\tilde{\mathfrak{q}}}(x) > 0,$$

so the number of sign vectors $\varepsilon(\mathfrak{a})$ such that $\alpha \equiv \lambda_{\varepsilon(\mathfrak{a})}\beta \bmod \mathbb{O}_K$ is equal to $2^{\#\{\mathfrak{q} \mid d : x \equiv 0 \bmod \mathfrak{q}\}}$.

The second assertion in the theorem follows from the same argument given in the proof of Lemma 5.2. □

7. Endomorphism rings of abelian surfaces with complex multiplication

Let K be a primitive CM field of degree 4 over the rational numbers. Let $W = W(\bar{\mathbb{F}}_p)$ be the Witt ring, and let

$$(A, \iota : \mathbb{O}_K \to \mathrm{End}_W(A))$$

be an abelian scheme over W of relative dimension 2 such that $A \pmod p$ is superspecial. Assume also that p is unramified in K. Then $R := \mathrm{End}_{\mathbb{O}_L}(A \pmod p)$ is a superspecial order of the quaternion algebra $B_{p,L}$ [Nicole 2008, Proposition 4.1].

Theorem 7.1. *One has*

$$\mathrm{End}_{\mathbb{O}_L, W/(p^n)}(A \pmod{p^n}) = \mathbb{O}_K + p^{n-1}R.$$

This theorem is a generalization of a theorem of Gross that deals with the case of elliptic curves [1986], but our method of proof is different; it is based on crystalline deformation theory.

Proof. Consider $A \pmod{p^n}$. We have an identification

$$\mathbb{H}^1_{dR}(A \pmod{p^n}) \cong H^1_{\mathrm{Crys}}(A \pmod p / W) \otimes W/(p^n).$$

Using that $W/(p^{n+1}) \to W/(p^n)$ has canonical divided power structure, we know the deformations of $A \pmod{p^n}$ to an abelian scheme B over $W/(p^{n+1})$ are in functorial correspondence with direct summands of $H^1_{\mathrm{Crys}}(A \pmod p/W) \otimes W/(p^{n+1})$ such that the following diagram commutes:

$$\begin{array}{ccc} M & \subseteq & H^1_{\mathrm{Crys}}(A \pmod p/W) \otimes W/(p^{n+1}) \\ \downarrow{\scriptstyle \bmod p^n} & & \downarrow{\scriptstyle \bmod p^n} \\ \underline{\omega}_{A \pmod{p^n}} & \subseteq & H^1_{\mathrm{Crys}}(A \pmod p/W) \otimes W/(p^n) \end{array}$$

where $\underline{\omega}_{A \pmod{p^n}}$ are the relative differentials at the origin of $A \pmod{p^n}$.

We shall show that there exists a unique such B to which the $\mathbb{O}_K$-action extends, namely, a unique M fixed under the $\mathbb{O}_K$ action on $H^1_{\mathrm{Crys}}(A \pmod p/W)$. We may conclude then that for that M there is an isomorphism

$$\begin{aligned}\mathrm{End}_{\mathbb{O}_L}(A \pmod{p^{n+1}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{End}_{\mathbb{O}_L}\left(M \subset H^1_{\mathrm{Crys}}(A \pmod p/W) \otimes W/(p^{n+1})\right) \\ \cap \mathrm{End}_{\mathbb{O}_L}(A \pmod{p^{n+1}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p. \quad (7\text{-}1)\end{aligned}$$

We then calculate the right-hand side and find that it is equal to $(\mathbb{O}_K + p^n R) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Since we know a priori that $\mathrm{End}_{\mathbb{O}_L}(A \pmod{p^{n+1}})$ has index equal to a power of p in R [Goren and Lauter 2012, Proposition 6.1], our theorem will follow.

First, the uniqueness of M is easy to establish. We have an isomorphism of $\mathbb{O}_K \otimes_{\mathbb{Z}} W$ modules

$$H^1_{\mathrm{Crys}}(A \pmod p/W) \cong \bigoplus_{\varphi \in \mathrm{Emb}(\mathbb{O}_K, W)} W(\varphi),$$

where $W(\varphi)$ is just W with the $\mathbb{O}_K$ action given by φ. Since p is unramified, for all $n \geq 1$, $W(\varphi) \ncong W(\varphi') \pmod{p^n}$ as $\mathbb{O}_K$-modules for any distinct $\varphi, \varphi' \in \mathrm{Emb}(\mathbb{O}_K, W)$. If Φ is the CM-type of A, it follows that if M is a direct summand of rank g, which is an $\mathbb{O}_K$-submodule, then M must be $\bigoplus_{\varphi \in \Phi} W(\varphi) \pmod{p^{n+1}}$.

Let $R_n := \mathrm{End}_{\mathbb{O}_L, W/(p^n)}(A \pmod{p^n})$. We prove by induction on n that

$$R_n = \mathbb{O}_K + p^{n-1} R.$$

As remarked, it is enough to prove that after p-adic completion, and in fact, we actually calculate the right-hand side of (7-1). The case $n = 1$ is tautological.

Since we assumed that $A \pmod p$ is superspecial and p is unramified in K, there are, according to [Goren and Lauter 2012, Tables 3.3.1(ii), 3.4.1(iii) and (iv), and 3.5.1(iii) and (vi)] and the results of Yu [2004], precisely two possibilities for $H^1_{\mathrm{Crys}}(A \pmod p/W)$, equivalently for the Dieudonné module of $A \pmod p$, as an $\mathbb{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$-module. Our calculations are done separately according to these cases.

Case 1: In this case, the completions at p of the rings are

$$\mathcal{O}_{L,p} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \quad \text{and} \quad \mathcal{O}_{K,p} \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2},$$

where we write $\mathbb{Z}_{p^2}$ for $W(\mathbb{F}_{p^2})$. The Dieudonné module $\mathbb{D}$ is a direct sum of Dieudonné modules

$$\mathbb{D} = \mathbb{D}_1 \oplus \mathbb{D}_2,$$

where for $i = 1, 2$, $\mathbb{D}_i$ has a basis relative to which Frobenius is given by the matrix

$$\begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix},$$

and the ith copy of $\mathbb{Z}_{p^2}$ in $\mathcal{O}_{K,p}$ acts on $\mathbb{D}_i$ by

$$a \mapsto \begin{pmatrix} a & \\ & a^\sigma \end{pmatrix}$$

and $\mathbb{D}_{i+1 \pmod 2}$ by zero. (Here σ is the Frobenius automorphism of $\mathbb{Z}_{p^2}$.) Clearly,

$$\mathrm{End}_{\mathcal{O}_L}(\mathbb{D}) = \mathrm{End}(\mathbb{D}_1) \times \mathrm{End}(\mathbb{D}_2),$$

and, as one can easily check,

$$\mathrm{End}(\mathbb{D}_i) = \left\{ \begin{pmatrix} \alpha & p\beta \\ \beta^\sigma & \alpha^\sigma \end{pmatrix} : \alpha, \beta \in W(\mathbb{F}_{p^2}) \right\}.$$

(The restriction on the entries $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ comes from the identity

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a^\sigma & b^\sigma \\ c^\sigma & d^\sigma \end{pmatrix}$$

that an endomorphism of the Dieudonné module must satisfy.)

Now, for every n, $\underline{\omega}_{A \pmod{p^n}} = \mathrm{Span}_{W/(p^n)}\{(0\ \ 1)^{\mathrm{T}}\} \oplus \mathrm{Span}_{W/(p^n)}\{(0\ \ 1)^{\mathrm{T}}\}$ in the decomposition $\mathbb{D} = \mathbb{D}_1 \oplus \mathbb{D}_2$. By induction, the endomorphisms in $\mathrm{End}_{\mathcal{O}_L}(\mathbb{D})$ preserving $\underline{\omega}_{A \pmod{p^n}}$ are

$$(\mathcal{O}_K + p^{n-1}R) \otimes_{\mathbb{Z}} \mathbb{Z}_p = \left\{ \left(\begin{pmatrix} \alpha & p^n\beta \\ p^{n-1}\beta^\sigma & \alpha^\sigma \end{pmatrix}, \begin{pmatrix} \gamma & p^n\delta \\ p^{n-1}\delta^\sigma & \gamma^\sigma \end{pmatrix} \right) : \alpha, \beta, \gamma, \delta \in W(\mathbb{F}_{p^2}) \right\}.$$

The condition for such an endomorphism to preserve $\underline{\omega}_{A \pmod{p^{n+1}}}$ is that the vectors

$$\begin{pmatrix} \alpha & p^n\beta \\ p^{n-1}\beta^\sigma & \alpha^\sigma \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \gamma & p^n\delta \\ p^{n-1}\delta^\sigma & \gamma^\sigma \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

are multiples of $(0\ \ 1)^{\mathrm{T}}$ modulo p^{n+1}. This is the case precisely when β and δ, respectively, are in pW. Thus, $\mathrm{End}(A \pmod{p^{n+1}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p = (\mathbb{O}_K + p^n R) \otimes_{\mathbb{Z}} \mathbb{Z}_p$, and the proof is complete in Case 1.

Case 2: In this case, the completions at p of the rings are

$$\mathbb{O}_{L,p} \cong \mathbb{Z}_{p^2} \quad \text{and} \quad \mathbb{O}_{K,p} \cong \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2},$$

where $\mathbb{Z}_{p^2}$ is embedded diagonally in $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$. The Dieudonné module has a basis $\{e_1, e_2, e_3, e_4\}$ relative to which

$$\mathrm{Fr} = \begin{pmatrix} 0 & 0 & p & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \end{pmatrix}.$$

The element $(a, b) \in \mathbb{O}_{K,p}$ acts by the diagonal matrix $\mathrm{diag}(a, b, a^\sigma, b^\sigma)$, and so $a \in \mathbb{O}_{L,p}$ acts by $\mathrm{diag}(a, a, a^\sigma, a^\sigma)$. Change the order of the basis elements to get a new basis $\{e_1, e_4, e_3, e_2\}$. Then Frobenius is given by

$$\begin{pmatrix} 0 & pI_2 \\ I_2 & 0 \end{pmatrix},$$

and $(a, b) \in \mathbb{O}_{K,p}$ acts by the diagonal matrix $\mathrm{diag}(a, b^\sigma, a^\sigma, b)$, and so $a \in \mathbb{O}_{L,p}$ acts by $\mathrm{diag}(a, a^\sigma, a^\sigma, a)$.

The condition for a matrix

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_4(W)$$

to be in $\mathrm{End}(\mathbb{D})$ is

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} 0 & pI_2 \\ I_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & pI_2 \\ I_2 & 0 \end{pmatrix} \begin{pmatrix} A^\sigma & B^\sigma \\ C^\sigma & D^\sigma \end{pmatrix},$$

and so we find

$$\mathrm{End}(\mathbb{D}) = \left\{ \begin{pmatrix} A & pC^\sigma \\ C & A^\sigma \end{pmatrix} : A, C \in M_2(W(\mathbb{F}_{p^2})) \right\}.$$

For such a matrix to be in $\mathrm{End}_{\mathbb{O}_L}(\mathbb{D})$, it must commute with all matrices of the form $\mathrm{diag}(a, a^\sigma, a^\sigma, a)$, where a runs over $W(\mathbb{F}_{p^2})$. An easy computation gives

$$\mathrm{End}_{\mathbb{O}_L}(\mathbb{D}) = \left\{ \begin{pmatrix} A & pC^\sigma \\ C & A^\sigma \end{pmatrix} : \text{diagonal matrices } A, C \in M_2(W(\mathbb{F}_{p^2})) \right\}.$$

We have $\underline{\omega}_{A \pmod{p^n}} = \mathrm{Span}\{e_3, e_2\}$, where e_3 and e_2 are the last two vectors in the current basis. One argues by induction, as before, to prove that the endomorphisms

in $\mathrm{End}_{\mathcal{O}_L}(\mathbb{D})$ preserving $\underline{\omega}_{A\ (\mathrm{mod}\ p^n)}$ are precisely those of the form

$$\left\{\begin{pmatrix} A & p^n C^\sigma \\ p^{n-1}C & A^\sigma \end{pmatrix} : \text{diagonal matrices } A, C \in M_2(W(\mathbb{F}_{p^2}))\right\} \cong (\mathcal{O}_K + p^{n-1}R) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

That completes the proof of Case 2 and hence of the theorem. □

8. Geometric interpretation

Let $W := W(\bar{\mathbb{F}}_p)$ and $Q := W \otimes_{\mathbb{Z}} \mathbb{Q}$; Q is the completion of the maximal unramified extension of $\mathbb{Q}_p$. Assume that p is unramified in K, and consider the functor on W-schemes associating to a W-scheme S the isomorphism classes of triples

$$\underline{A} = (A, \iota, \eta), \tag{8-1}$$

where $A \to S$ is an abelian scheme of relative dimension g, $\iota : \mathcal{O}_K \to \mathrm{End}_S(A)$ is a ring homomorphism, and η is a principal polarization of A inducing complex conjugation on K. Arguments as in [Goren and Lauter 2007] show that this functor is represented by an étale scheme over W whose complex points are in natural bijection with $\mathcal{F} \times \mathrm{Cl}(K)$ as described in Proposition 2.4. In particular, isomorphism classes of $\underline{A}$ over $\bar{\mathbb{F}}_p$ as in (8-1), or more generally of $\underline{A}$ over $W/(p^n)$, are also in bijection with $(\mathcal{F} \times \mathrm{Cl}(K))/\sim$ once we have fixed an identification of $\mathrm{Hom}(K, \mathbb{C})$ with $\mathrm{Hom}(K, \bar{\mathbb{Q}}_p)$. This allows us to speak about the CM type of A over $W/(p^n)$. Of course, this is nothing but the isomorphism class of the representation of $\mathcal{O}_K$ on the Lie algebra of A and is determined by its reduction modulo p.

Consider pairs (A, ι) over $\bar{\mathbb{F}}_p$ such that A is a g-dimensional abelian variety and $\iota : \mathcal{O}_K \to \mathrm{End}(A)$ is a ring homomorphism such that $(A, \iota|_{\mathcal{O}_L})$ satisfies the Rapoport condition. One knows that there exists a principal $\mathcal{O}_L$-polarization η on A, unique up to isomorphism. We claim that η automatically induces complex conjugation on K. This can be verified by case-by-case analysis using [Chai 1995, Lemma 6].

8.1. ***Isomorphisms of CM abelian varieties.*** Now fix a CM field K' whose totally real subfield is L. Consider $(A, \iota_A : \mathcal{O}_K \to \mathrm{End}(A))$ and $(A', \iota_{A'} : \mathcal{O}_{K'} \to \mathrm{End}(A'))$ over $\bar{\mathbb{F}}_p$, and assume that we are given an isomorphism

$$\alpha : (A, \iota_A|_{\mathcal{O}_L}) \xrightarrow{\sim} (A', \iota_{A'}|_{\mathcal{O}_L}).$$

We then get an embedding

$$j_\alpha : \mathcal{O}_{K'} \to \mathrm{End}(A), \quad j_\alpha(r) = \alpha^{-1} \circ \iota_{A'}(r) \circ \alpha.$$

If $\beta : (A, \iota_A|_{\mathcal{O}_L}) \xrightarrow{\sim} (A', \iota_{A'}|_{\mathcal{O}_L})$ is another isomorphism, then

$$\beta = \gamma \circ \alpha,$$

where

$$\gamma \in \mathrm{Aut}(A', \iota_{A'}|_{\mathcal{O}_L}) \quad \text{and} \quad j_\beta(r) = \alpha^{-1} \circ \gamma^{-1} \circ \iota_{A'}(r) \circ \gamma \circ \alpha.$$

This gives another embedding of $\mathcal{O}_{K'}$ into $\mathrm{End}(A)$. The embeddings are equal if and only if $\gamma^{-1} \circ \iota_{A'}(r) \circ \gamma = \iota_{A'}(r)$ for all $r \in \mathcal{O}_{K'}$. This, in turn is equivalent to $\gamma \in \mathrm{Cent}_{\mathrm{End}^0(A')}(K') \cap \mathrm{Aut}((A', \iota_{A'}|_{\mathcal{O}_L})) = \mathcal{O}_{K'}^\times$. (Here $\mathrm{Cent}_{\mathrm{End}^0(A')}(K')$ denotes the centralizer of K' in $\mathrm{End}^0(A')$.) Thus, each isomorphism class of $(A', \iota_{A'})$ such that $(A, \iota_A|_{\mathcal{O}_L}) \cong (A', \iota_{A'}|_{\mathcal{O}_L})$ gives us

$$\#(\mathrm{Aut}((A', \iota_{A'}|_{\mathcal{O}_L}))/\mathcal{O}_{K'}^\times) = \#(\mathrm{Aut}((A, \iota_A|_{\mathcal{O}_L}))/\mathcal{O}_{K'}^\times)$$

distinct embeddings of $\mathcal{O}_{K'}$ into $\mathrm{End}(A)$.

8.2. ***Counting isomorphisms in the superspecial case.*** Now assume we are in the superspecial reduction situation, and fix an isomorphism

$$\mathrm{End}_{\mathcal{O}_L}(A) \cong R(\mathfrak{a}, \lambda_\mathfrak{a})$$

for some unique $\mathfrak{a} \lhd \mathcal{O}_K$ (Lemma 5.6 and Theorem 5.7). With $\mathcal{O}_{K'} = \mathcal{O}_L[\omega]$ as before, to give an embedding $\mathcal{O}_{K'} \to \mathrm{End}_{\mathcal{O}_L}(A)$ is to choose an element $[\alpha, \beta] \in R(\mathfrak{a}, \lambda_\mathfrak{a})$ with trace equal to $\mathrm{Tr}(\omega)$ and norm equal to $\mathrm{Norm}(\omega)$, that is, an element of the set $S(\mathfrak{a}, \lambda_\mathfrak{a}, 1)$. Such an embedding makes $(A, \iota_A|_{\mathcal{O}_L})$ into an abelian variety with CM by $\mathcal{O}_{K'}$, and so the embedding $\mathcal{O}_{K'} \to \mathrm{End}_{\mathcal{O}_L}(A)$ arises via a particular isomorphism

$$(A, \iota_A : \mathcal{O}_K \to \mathrm{End}(A)) \xrightarrow{\sim} (A', \iota' : \mathcal{O}_{K'} \to \mathrm{End}(A'))$$

(where, in fact, we may take $A = A'$ and ι' restricts to ι_A on $\mathcal{O}_L$). We conclude that

$$\frac{\#S(\mathfrak{a}, \lambda_\mathfrak{a}, 1)}{\#(R(\mathfrak{a}, \lambda_\mathfrak{a})^\times/\mathcal{O}_{K'}^\times)} = \#\left\{(A', \iota_{A'} : \mathcal{O}_{K'} \to \mathrm{End}_{\mathcal{O}_L}(A'))/\overline{\mathbb{F}}_p : (A', \iota_{A'}|_{\mathcal{O}_L}) \xrightarrow{\sim} (A, \iota_A|_{\mathcal{O}_L})\right\}$$

(where on the left-hand side we consider $(A', \iota_{A'} : \mathcal{O}_{K'} \to \mathrm{End}_{\mathcal{O}_L}(A'))$ up to isomorphism with CM by $\mathcal{O}_{K'}$, of course). Exactly the same analysis is valid over $W/(p^n)$, and using $\mathrm{End}_{W/(p^n)}(A, \iota|_{\mathcal{O}_L}) \cong R(\mathfrak{a}, \lambda_\mathfrak{a}, p^{n-1})$ as follows from Theorem 7.1, we get

$$\frac{\#S(\mathfrak{a}, \lambda_\mathfrak{a}, p^{n-1})}{\#(R(\mathfrak{a}, \lambda_\mathfrak{a}, p^{n-1})^\times/\mathcal{O}_{K'}^\times)}$$
$$= \#\left\{(A', \iota_{A'} : \mathcal{O}_{K'} \to \mathrm{End}_{\mathcal{O}_L}(A'))/W/(p^n) : (A', \iota_{A'}|_{\mathcal{O}_L}) \xrightarrow{\sim} (A, \iota_A|_{\mathcal{O}_L})\right\}. \quad (8\text{-}2)$$

8.3. ***Counting formulas for the number of isomorphisms for superspecial CM types.*** Now fix a superspecial CM type Φ of K, namely, a CM type arising for some superspecial abelian variety. By [Goren and Lauter 2012], then any abelian variety with CM by $\mathcal{O}_K$ of CM type Φ is superspecial.

We consider representatives $\underline{A} = (A, \iota_A : \mathbb{O}_K \to \mathrm{End}(A))$ for the isomorphism classes with CM type Φ. For each such $\underline{A}$, we may choose an isomorphism

$$f_{\underline{A}} : \mathrm{End}_L^0(\underline{A}) \xrightarrow{\sim} B_{p,L}$$

and hence get an embedding

$$f_{\underline{A}} \circ \iota_A : K \to B_{p,L}.$$

By Skolem–Noether, we may conjugate the identifications $f_{\underline{A}}$ so that the embeddings $f_{\underline{A}} \circ \iota_A$ are *the same*, and in fact, this will be the case if $f_{\underline{A}_1}$ and $f_{\underline{A}_2}$ are related by a CM isogeny to begin with. Then for every $\underline{A}$, $f_{\underline{A}}(\mathrm{End}_{\mathbb{O}_L}(\underline{A}))$ is a superspecial order containing $\mathbb{O}_K$. This order is uniquely determined by $\underline{A}$ up to conjugation by $K^\times$.

By our results, the representatives for these orders modulo conjugation by $K^\times$ are precisely the orders $R(\mathfrak{a}, \lambda_\mathfrak{a})$ as $\mathfrak{a}$ ranges over representatives for $\mathrm{Cl}(\mathbb{O}_K)$. We therefore conclude:

Theorem 8.1. *We have* (*where, of course, the* $\underline{A}'$ *are taken up to isomorphism*)

$$\sum_{\mathfrak{a}} \#S(\mathfrak{a}, \lambda_\mathfrak{a}, p^{n-1}) = \sum_{\substack{\underline{A}/(W/(p^n)) \\ \text{with CM type } \Phi}} \#\left(\frac{\mathrm{End}_{\mathbb{O}_L, W/(p^n)}(\underline{A})^\times}{\mathbb{O}_{K'}^\times}\right) \cdot \#\left\{\begin{array}{c}\underline{A}' \text{ with CM by } \mathbb{O}_{K'} \text{ such that} \\ (A', \iota_{A'}|_{\mathbb{O}_L}) \cong (A, \iota_A|_{\mathbb{O}_L})\end{array}\right\}. \quad (8\text{-}3)$$

If we wish not to fix a CM type on K, we get the following:

Theorem 8.2. *We have*

$$\#\{\text{superspecial CM types}\} \times \sum_{\mathfrak{a}} \#S(\mathfrak{a}, \lambda_\mathfrak{a}, p^{n-1}) = \sum_{\substack{\underline{A}/(W/(p^n)) \\ \text{with CM by } \mathbb{O}_K}} \#\left(\frac{\mathrm{End}_{\mathbb{O}_L, W/(p^n)}(\underline{A})^\times}{\mathbb{O}_{K'}^\times}\right) \cdot \#\left\{\begin{array}{c}\underline{A}' \text{ with CM by } \mathbb{O}_{K'} \text{ such that} \\ (A', \iota_{A'}|_{\mathbb{O}_L}) \cong (A, \iota_A|_{\mathbb{O}_L})\end{array}\right\}. \quad (8\text{-}4)$$

8.4. ***Counting formulas for pairs of embeddings into superspecial orders.*** The left-hand side of (8-3), for $n = 1$, has another interpretation. Consider a pair of embeddings $\iota : \mathbb{O}_K \to R$ and $\iota' : \mathbb{O}_{K'} \to R$ into a superspecial order R such that both restrict to a fixed, given embedding of $\mathbb{O}_L$ into R. We call it an optimal triple (ι, ι', R). We say that (ι, ι', R) is conjugate to $(j, j', \tilde{R})$ if there exists $t \in B_{p,L}^\times$ such that $t^{-1}Rt = \tilde{R}$ and $t^{-1}\iota(x)t = j(x)$ for all $x \in {\mathbb{O}_K}^\times$ and $t^{-1}\iota'(x)t = j'(x)$ for all $x \in \mathbb{O}_{K'}^\times$.

To count the number of conjugacy classes of optimal triples, let us fix an embedding $I : K \to B_{p,L}$. Then any optimal triple is conjugate to $(I|_{\mathbb{O}_K}, \iota', R)$, where R is a superspecial order containing $I(\mathbb{O}_K)$. We may still conjugate by $K^\times$ and so assume that $R = R(\mathfrak{a}, \lambda_\mathfrak{a})$ for some $\mathfrak{a}$. We may still conjugate by ${\mathbb{O}_K}^\times$, and if $K \neq K'$, that

induces a faithful action of $\mathcal{O}_K{}^\times/\mathcal{O}_L{}^\times$ on the embeddings $\iota' : \mathcal{O}_{K'} \to R(\mathfrak{a}, \lambda_\mathfrak{a})$ if they exist at all. We conclude that

$$\#(\mathcal{O}_K{}^\times/\mathcal{O}_L{}^\times)^{-1} \sum_{\mathfrak{a}} \#S(\mathfrak{a}, \lambda_\mathfrak{a}, 1) = \#\{\text{optimal triples up to conjugation}\}.$$

Corollary 8.3. *The number of optimal triples up to conjugation equals*

$$\begin{aligned}
&\#(\mathcal{O}_K{}^\times/\mathcal{O}_L{}^\times)^{-1} \sum_{\mathfrak{a}} \#S(\mathfrak{a}, \lambda_\mathfrak{a}, 1) \\
&= \sum_{\substack{\underline{A}/(W/(p^n)) \\ \text{with CM type } \Phi}} \#(\mathcal{O}_K{}^\times/\mathcal{O}_L{}^\times)^{-1} \#(\mathcal{O}_{K'}^\times/\mathcal{O}_L{}^\times)^{-1} \#\left(\frac{\mathrm{End}_{\mathcal{O}_L, W/(p^n)}(\underline{A})^\times}{\mathcal{O}_L^\times}\right) \\
&\qquad \times \#\left\{ \begin{array}{c} \underline{A}' \text{ with CM by } \mathcal{O}_{K'} \text{ such that} \\ (A', \iota_{A'}|_{\mathcal{O}_L}) \cong (A, \iota_A|_{\mathcal{O}_L}) \end{array} \right\}. \qquad (8\text{-}5)
\end{aligned}$$

If we multiply the whole set of equalities (8-5) above by the number of superspecial types for K, we may be justified in calling the new right-hand side of (8-5) the "coincidence number of K and K' at p" as it counts the number of coincidences between abelian varieties with CM by K and abelian varieties with CM by K' in characteristic p once one considers them as abelian varieties with RM only.

9. The connection to moduli spaces

In their paper [1985], Gross and Zagier give a beautiful formula. Let E_1 and E_2 be two elliptic curves over $W = W(\bar{\mathbb{F}}_p)$. Let j_i be the j-invariant of E_i. Their formula is

$$\mathrm{val}_p(j_1 - j_2) = \frac{1}{2} \sum_{n \geq 1} \#\,\mathrm{Isom}_n(E_1, E_2),$$

where Isom_n denotes the isomorphisms between the reduction of E_i modulo (p^n).

The proof Gross and Zagier provided is through direct manipulations of Weierstrass equations. A more conceptual proof was given by Brian Conrad in [2004]. The proof makes essential use of moduli spaces but uses many features unique to modular curves and hence is not readily amenable to generalization. This result is the basis of interpreting their theorem on $J(d, d')$ and $\mathrm{ord}_\lambda(J(d, d'))$ (cf. Section 1) as an arithmetic intersection number. It thus remains a question of how to give an interpretation for our theorems, Theorem 8.2 for example, as an intersection number of CM points on Shimura varieties.

One possibility is to use Shimura curves associated with quaternion algebras over totally real fields split at exactly one infinite prime. This approach entails using the p-adic, not-quite-canonical models for these Shimura curves, following Morita, Carayol, and Boutot–Carayol. The other possibility is to view these CM 0-cycles as lying on a Hilbert modular variety. This approach is complicated by the

fact that there is no "robust" definition of the arithmetic intersection of 0-cycles (1-cycles on the arithmetic models) once their codimension is bigger than 1. This calls for an ad-hoc approach, and it has its own challenging problems.

For now, we will replace the notion of an intersection number with something less precise and define instead a *coincidence number*, which does not reflect the power to which various primes may appear in the differences of invariants but at least reflects whether a prime appears in the factorizations of the differences of invariants. In Section 12, we will give an example to illustrate the coincidence number in computations.

Let L be a totally real field with strict class number 1 and K_i with $i = 1, 2$ two CM fields containing L as their maximal totally real subfield. Let p be a prime unramified in both K_1 and K_2. For each CM field, we can associate a 0-cycle $\mathrm{CM}(K_i)$ on the generic fiber of the Hilbert modular variety $\mathscr{H}_L$ parametrizing principally polarized abelian varieties with RM by $\mathbb{O}_L$ (Section 2.3). Each point x_η in $\mathrm{CM}(K_i)$ can be extended to a $W(\bar{\mathbb{F}}_p)$-point x on $\mathscr{H}_L$ [Goren and Lauter 2012, Lemma 2.3]. This implicitly depends on a choice of a prime $\mathfrak{p}$ in a common field of definition for all the CM abelian varieties under consideration. We write $\mathrm{CM}(K_1) = \sum_i x_i$ and $\mathrm{CM}(K_2) = \sum_j y_j$. We then define the arithmetic *coincidence number* (for lack of better terminology) of $\mathrm{CM}(K_1)$ and $\mathrm{CM}(K_2)$ as

$$\mathrm{CM}(K_1) \wedge \mathrm{CM}(K_2) = \sum_{ij} x_i \wedge y_j,$$

where $x_i \wedge y_j$ is defined as 1 if x_i and y_j have isomorphic reduction modulo p and as 0 otherwise. In this notation, Theorem 8.2 implies the following:

Corollary 9.1. *The contribution from a prime p of superspecial reduction to $\mathrm{CM}(K_1) \wedge \mathrm{CM}(K_2)$ is equal to $\#\{\text{superspecial CM types}\} \times \sum_{\mathfrak{a}} \#S(\mathfrak{a}, \lambda_{\mathfrak{a}}, 1)$.*[1] *This number, and in particular whether it is zero, can be effectively calculated.*

10. Supersingular orders

Theorem 10.1. *Let p be a rational prime and k an algebraically closed field of characteristic p. Let K be a quartic CM field, and let $L = K^+$ be its real subfield. Let A/k be an abelian surface that is supersingular, but not superspecial, with complex multiplication by $\mathbb{O}_K$. Let $\mathbb{O} := \mathrm{End}_{\mathbb{O}_L}(A)$, where the endomorphisms are over k. Let $B_{p,\infty}$ be the quaternion algebra over $\mathbb{Q}$ ramified at only p and ∞, and let $B_{p,L} := B_{p,\infty} \otimes_{\mathbb{Q}} L$. Then $\mathbb{O}$ is an Eichler order of $B_{p,L}$ of discriminant p^2.*

Proof. Let H be a quaternion algebra over a number field F, and let R be an order of H containing $\mathbb{O}_F$. Recall that R is called an Eichler order if it is the intersection of two maximal orders. This is a local property [Vignéras 1980, p. 84]. If F denotes

[1] Likewise, the notion of superspecial CM types depends on the implicit choice of $\mathfrak{p}$.

now a nonarchimedean local field with uniformizer π, then an order of H containing $\mathcal{O}_F$ is Eichler (namely, is the intersection of two maximal orders of H) if and only if it is conjugate to the order

$$M = \begin{pmatrix} \mathcal{O}_F & \mathcal{O}_F \\ \pi^n \mathcal{O}_F & \mathcal{O}_F \end{pmatrix}$$

for some positive integer n [Vignéras 1980, p. 39].

We wish to find the completion of $\mathcal{O}$ at every rational prime ideal $\mathfrak{l}$ of $\mathcal{O}_L$.

First, since there exists an isogeny of degree a power of p between any two supersingular abelian surfaces A and A' with real multiplication respecting the real multiplication structure [Bachmat and Goren 1999], for $\mathfrak{l} \nmid p$, we have that $\mathcal{O}_\mathfrak{l} := \mathcal{O} \otimes_{\mathcal{O}_L} \mathcal{O}_{L,\mathfrak{l}} \cong \mathcal{O}'_\mathfrak{l}$, where $\mathcal{O}' = \mathrm{End}_{\mathcal{O}_L}(A')$. We may choose for A' the surface $E \otimes_\mathbb{Z} \mathcal{O}_L$, where E is a supersingular elliptic curve with $R = \mathrm{End}(E)$ a maximal order in $B_{p,\infty}$. Then $\mathcal{O}' = \mathrm{End}(A') = R \otimes_\mathbb{Z} \mathcal{O}_L$, so $\mathcal{O}'$ and $\mathcal{O}$ are maximal orders at $\mathfrak{l}$.

We remark that according to the classification of the reduction of abelian surfaces with CM, the situation we consider occurs if and only if p is inert in K, that is, in the following cases:

(a) $K/\mathbb{Q}$ is cyclic Galois and p inert in K [Goren and Lauter 2012, Table 3, case (iii)], and

(b) $K/\mathbb{Q}$ is non-Galois and p inert in K [Goren and Lauter 2012, Table 5, case (vii)].

Following the conventions of [Goren and Lauter 2012], the Dieudonné module of the p-divisible group of the reduction of A modulo $\mathfrak{p}_L$ is

$$\mathbb{D} \cong \mathbb{W}(1) \oplus \mathbb{W}(y^2) \oplus \mathbb{W}(y) \oplus \mathbb{W}(y^3),$$

where $\mathbb{W}(\alpha)$ denotes the Witt vectors of $\bar{\mathbb{F}}_p$, where $\mathcal{O}_K$ acts through the embedding $\alpha : K \to \bar{\mathbb{Q}}_p$. Let σ denote the Frobenius automorphism of $\mathbb{W}$. Then

(a) $\mathcal{O}_L$ acts on $\mathbb{D}$ by $l \mapsto \mathrm{diag}(l, l, \sigma(l), \sigma(l))$, and

(b) $\mathcal{O}_K$ acts on $\mathbb{D}$ by $k \mapsto \mathrm{diag}(k, \sigma^2(k), \sigma(k), \sigma^3(k))$.

The p-adic CM type is $\{1, y^3\}$ according to our conventions, but since the situation is symmetric, we may assume that the p-adic CM type is $\{1, y\}$, and so Frobenius is given in the standard basis by the matrix

$$\mathrm{Fr} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & p & 0 \\ p & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

By a theorem of Tate, $\mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Z}_p \cong \mathrm{End}(\mathbb{D})$, where on the right the endomorphisms are as Dieudonné modules (cf. [Waterhouse and Milne 1971, Theorem 5]),

namely, in this case, $\mathbb{W}$-linear maps $\mathbb{D} \to \mathbb{D}$ that commute with Frobenius. In the same way,

$$\mathcal{O}_p = \mathrm{End}_{\mathcal{O}_L}(A) \otimes_{\mathcal{O}_L} \mathcal{O}_{L\,p} = \mathrm{End}_{\mathcal{O}_L}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathrm{End}_{\mathcal{O}_L}(\mathbb{D}).$$

Since $\mathcal{O}_p$ commutes with $\mathcal{O}_L$, one finds that $\mathcal{O}_p$ is given by block diagonal matrix with blocks of size 2. Writing the general such matrix as

$$M = \begin{pmatrix} m_{11} & m_{12} & & \\ m_{21} & m_{22} & & \\ & & n_{11} & n_{12} \\ & & n_{21} & n_{22} \end{pmatrix},$$

the condition $M \cdot \mathrm{Fr} = \mathrm{Fr} \cdot \sigma(M)$ gives, after a short computation,

$$\mathcal{O}_p = \left\{ \begin{pmatrix} m_{11} & m_{12} & & \\ p^2 m_{12}^{\sigma^2} & m_{11}^{\sigma^2} & & \\ & & m_{11}^{\sigma} & p m_{12}^{\sigma} \\ & & p m_{12}^{\sigma^3} & m_{11}^{\sigma^3} \end{pmatrix} : m_{ij} \in \mathbb{W}(\mathbb{F}_{p^4}) \right\}.$$

Since p is inert in L, the quaternion algebra $B_{p,L}$ is ramified only at the two places at infinity. In particular, $B_{p,L} \otimes_L L_p \cong M_2(\mathbb{Q}_{p^2})$, where $\mathbb{Q}_{p^2} = \mathbb{W}(\mathbb{F}_{p^2}) \otimes_{\mathbb{Z}} \mathbb{Q}$. To determine the nature of $\mathcal{O}_p$, we want to recognize it as a suborder of $M_2(\mathbb{W}(\mathbb{F}_{p^2}))$.

The case $p \neq 2$. Put

$$i := \begin{pmatrix} & 1 \\ p^2 & \end{pmatrix} \quad \text{and} \quad j := \begin{pmatrix} \alpha & \\ & \alpha^{\sigma^2} \end{pmatrix},$$

where α is chosen such that $\mathbb{W}(\mathbb{F}_{p^4}) = \mathbb{W}(\mathbb{F}_{p^2})[\alpha]$ and $\alpha^{\sigma^2} = -\alpha$. We have then

$$i^2 = p^2, \qquad j^2 = \alpha^2, \quad \text{and} \quad k := ij = -ji = \begin{pmatrix} & -\alpha \\ p^2\alpha & \end{pmatrix}.$$

Writing $m_1 = x_1 + y_1\alpha$ and $m_2 = x_2 + y_2\alpha$ with $x_i, y_i \in \mathbb{W}(\mathbb{F}_{p^2})$, we can write

$$\begin{aligned} \begin{pmatrix} m_{11} & m_{12} \\ p^2 m_{12}^{\sigma^2} & m_{11}^{\sigma^2} \end{pmatrix} &= x_1 \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + y_1 \begin{pmatrix} \alpha & \\ & \alpha^{\sigma^2} \end{pmatrix} + x_2 \begin{pmatrix} & 1 \\ p^2 & \end{pmatrix} - y_2 \begin{pmatrix} & -\alpha \\ p^2\alpha & \end{pmatrix} \\ &= x_1 \cdot 1 + y_1 \cdot j + x_2 \cdot i - y_2 \cdot k. \end{aligned}$$

Conversely, for any $x_i, y_i \in \mathbb{W}(\mathbb{F}_{p^2})$, we get an element of $\mathcal{O}_p$. Thus,

$$\mathcal{O}_p = \mathbb{W}(\mathbb{F}_{p^2}) \cdot 1 \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot i \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot j \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot k.$$

Let $I = p^{-1}i$, $J = j$, and $K = IJ = -JI$. Then $I^2 = 1$, $J^2 = \alpha^2$, and $K^2 = -\alpha^2$. The module

$$R = \mathbb{W}(\mathbb{F}_{p^2})[1, I, J, K]$$

is in fact an order of $M_2(\mathbb{Q}_{p^2})$, and it has discriminant 1. It must then be isomorphic to $M_2(\mathbb{W}_{p^2})$, and, indeed, if we send

$$1 \mapsto \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \qquad I \mapsto \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}, \qquad J \mapsto \begin{pmatrix} & \alpha^2 \\ 1 & \end{pmatrix}, \quad \text{and} \quad K \mapsto \begin{pmatrix} & \alpha^2 \\ -1 & \end{pmatrix},$$

we get the isomorphism $R \cong M_2(\mathbb{W}(\mathbb{F}_{p^2}))$. Under this isomorphism, $\mathbb{O}_p$ is mapped isomorphically to the order spanned over $\mathbb{W}(\mathbb{F}_{p^2})$ by the matrices

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \qquad \begin{pmatrix} p & \\ & -p \end{pmatrix}, \qquad \begin{pmatrix} & \alpha^2 \\ 1 & \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} & p\alpha^2 \\ -p & \end{pmatrix},$$

which can be described as

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{W}(\mathbb{F}_{p^2}),\ p \mid (a-d),\ p \mid (b - \alpha^2 c) \right\}.$$

Now conjugate $\mathbb{O}_p$ by the matrix

$$A = \begin{pmatrix} 1 & \alpha \\ \alpha^{-1} & -1 \end{pmatrix}.$$

Using

$$2A^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} A = \begin{pmatrix} a + \alpha^{-1} b + \alpha c + d & \alpha(a-d) + (\alpha^2 c - b) \\ \alpha^{-1}(a-d) + \alpha^{-2}(b - \alpha^2 c) & a - \alpha^{-1} b - \alpha c + d \end{pmatrix},$$

we find that $\mathbb{O}_p$ is conjugate to a suborder of

$$R' = \begin{pmatrix} \mathbb{W}(\mathbb{F}_{p^2}) & p\mathbb{W}(\mathbb{F}_{p^2}) \\ p\mathbb{W}(\mathbb{F}_{p^2}) & \mathbb{W}(\mathbb{F}_{p^2}) \end{pmatrix}.$$

However, comparing the discriminant of $\mathbb{O}_p$, which is p^2, and of R', which is p^2 as well, we conclude that $\mathbb{O}_p$ is isomorphic to R'. Further conjugation by the matrix

$$\begin{pmatrix} & 1/p \\ 1 & \end{pmatrix}$$

shows that $\mathbb{O}_p$ is isomorphic to the order

$$R'' = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{W}(\mathbb{F}_{p^2}),\ p^2 \mid c \right\},$$

which is an Eichler order of discriminant p^2.

The case $p = 2$. We may find $\alpha \in \mathbb{W}(\mathbb{F}_{p^2})$ such that $\mathbb{W}(\mathbb{F}_{p^4}) = \mathbb{W}(\mathbb{F}_{p^2})[(1+\alpha)/2]$ and $\alpha^{\sigma^2} = -\alpha$. Indeed, for a suitable $\epsilon \in \mathbb{W}(\mathbb{F}_{p^2})^\times$, we have $\mathbb{W}(\mathbb{F}_{p^4}) = \mathbb{W}(\mathbb{F}_{p^2})[\beta]$, where $\beta^2 + \beta + \epsilon = 0$. Note that β is a unit. Take $\alpha = -(2\beta + 1)$.

To make the analogy with the previous case more visible, we keep using p instead of 2 in most places. As before, we let

$$i = \begin{pmatrix} & 1 \\ p^2 & \end{pmatrix}, \qquad j = \begin{pmatrix} \alpha & \\ & -\alpha \end{pmatrix}, \quad \text{and} \quad k = ij = -ji = \begin{pmatrix} & -\alpha \\ \alpha p^2 & \end{pmatrix}.$$

Writing $m_1 = x_1 + y_1(1+\alpha)/2$ and $m_2 = x_2 + y_2(1+\alpha)/2$ with $x_i, y_i \in \mathbb{W}(\mathbb{F}_{p^2})$, we can write,

$$\begin{pmatrix} m_{11} & m_{12} \\ p^2 m_{12}^{\sigma^2} & m_{11}^{\sigma^2} \end{pmatrix} = x_1 \cdot 1 + y_1 \cdot \frac{1+j}{2} + x_2 \cdot i + y_2 \cdot \frac{i-k}{2},$$

and one concludes that

$$\mathbb{O}_p = \mathbb{W}(\mathbb{F}_{p^2}) \cdot 1 \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot i \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot \frac{1+j}{2} \oplus \mathbb{W}(\mathbb{F}_{p^2}) \cdot \frac{i-k}{2}.$$

One can verify directly that the right side is indeed an order and its discriminant is p^2.

The order $\mathbb{O}_p$ contains the order $\mathbb{W}(\mathbb{F}_{p^2})[1, i, j, k] = \mathbb{W}(\mathbb{F}_{p^2})[1, I, J, K]$, where $I = i$, $J = j/\alpha$, and $K = k/\alpha$. Note that $I^2 = p^2$, $J^2 = 1$, $K^2 = -p^2$, and $IJ = -JI = K$. Consider the linear map

$$\mathbb{W}(\mathbb{F}_{p^2})[1, I, J, K] \to M_2(\mathbb{W}(\mathbb{F}_{p^2}))$$

determined by

$$1 \mapsto \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \qquad I \mapsto \begin{pmatrix} & 2 \\ 2 & \end{pmatrix}, \qquad J \mapsto \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}, \quad \text{and} \quad K \mapsto \begin{pmatrix} & -2 \\ 2 & \end{pmatrix}.$$

One checks that this map is a ring homomorphism and verifies that

$$\mathbb{O}_p \cong \mathbb{W}(\mathbb{F}_{p^2})\left[\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} \frac{1+\alpha}{2} & \\ & \frac{1-\alpha}{2} \end{pmatrix}, 2\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}, 2\begin{pmatrix} & \frac{1+\alpha}{2} \\ \frac{1-\alpha}{2} & \end{pmatrix}\right].$$

Let $u := (1+\alpha)/(1-\alpha) = \beta^2/\epsilon$. Then u and $1-u = 2+u/\beta$ are units. It follows that

$$\mathbb{O}_p \cong \mathbb{W}(\mathbb{F}_{p^2})\left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, 2\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, 2\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right]$$
$$= \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{W}(\mathbb{F}_{p^2}),\ p \mid b,\ p \mid c\right\}.$$

An additional conjugation as in the case $p \neq 2$ shows that this is an Eichler order of discriminant p^2. □

11. A crude version of Gross–Zagier's result on singular moduli

Let A be a g-dimensional abelian variety over a field k. Let L be a totally real field of degree g over $\mathbb{Q}$ of strict class number 1, and let K_i with $i = 1, 2$ be two CM fields contained in some algebraic closure of L such that $K_1^+ = K_2^+ = L$. We allow $K_1 = K_2$. Assume we are given two embeddings

$$\varphi_i : K_i \to \mathrm{End}_k^0(A) := \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$$

such that

$$\varphi_1|_L = \varphi_2|_L \quad \text{and} \quad \varphi_1(K) \neq \varphi_2(K).$$

Lemma 11.1. *The field k has positive characteristic p. The abelian variety is supersingular, and $\mathrm{End}^0(A) \cong B_{p,L}$, where $B_{p,L} = B_{p,\infty} \otimes_{\mathbb{Q}} L$ and $B_{p,\infty}$ is "the" quaternion algebra over $\mathbb{Q}$ ramified at p and ∞.*

Proof. This follows easily from the classification of the endomorphism algebras of abelian varieties with real multiplication as in [Chai 1995, Lemma 6]; one observes that under our assumptions, the centralizer of L in $\mathrm{End}_k^0(A)$ is an L-vector space of dimension greater than 2. □

Let $\mathcal{O}_i \subseteq K_i$ be orders containing $\mathcal{O}_L$. The order $\mathcal{O}_i$ is determined by its conductor $\mathfrak{c}_i$, which is an integral ideal of $\mathcal{O}_L$ for which we choose a generator c_i [Goren and Lauter 2009, Lemma 4.1]. In fact, one can write

$$\mathcal{O}_{K_i} = \mathcal{O}_L[\kappa_i],$$

where $-m_i = B_i^2 - 4C_i$ is a totally negative element of $\mathcal{O}_L$ and κ_i satisfies a quadratic equation $x^2 + B_i x + C_i$ for $B_i, C_i \in \mathcal{O}_L$. The relative different ideal $\mathcal{D}_{K_i/L}$ is equal to $\mathcal{O}_{K_i}[1/\sqrt{-m_i}]$ [Goren and Lauter 2006, Lemma 3.1]. We have $\mathcal{O}_{K_i} = \mathcal{O}_L[\kappa_i] \supseteq \mathcal{O}_L[\sqrt{-m_i}] \supseteq \mathcal{O}_L[2\kappa_i]$, and so

$$\mathcal{O}_i = \mathcal{O}_L[c_i\kappa_i] \supseteq \mathcal{O}_L[c_i\sqrt{-m_i}] \supseteq \mathcal{O}_L[2c_i\kappa_i].$$

The discriminant of $\mathcal{O}_i$ relative to $\mathcal{O}_L$, $\mathrm{disc}_{K_i/L}(\mathcal{O}_i)$, is equal to the $\mathcal{O}_L$-ideal generated by $c_i^2 m_i$, and the discriminant of $\mathcal{O}_i$ relative to $\mathbb{Z}$, $\mathrm{disc}(\mathcal{O}_i) = \mathrm{disc}_{K/\mathbb{Q}}(\mathcal{O}_i)$, is equal to $\mathrm{Norm}_{L/\mathbb{Q}}(c_i^2 m_i) \cdot \mathrm{disc}(\mathcal{O}_L)^2$. (In general, we use "disc" to denote absolute discriminant, that is, relative to $\mathbb{Z}$.)

Let B be any totally definite quaternion algebra over L; that is, $B \otimes_{L,\sigma} \mathbb{R}$ is a division algebra for any embedding $\sigma : L \to \mathbb{R}$, and let $\mathfrak{d}$ be its discriminant. Let

$$\varphi_i : K_i \to B$$

be two embeddings such that $\varphi_1|_L = \varphi_2|_L$ and $\varphi_1(K_1) \neq \varphi_2(K_2)$. Let

$$k_i = \varphi_i(c_i\sqrt{-m_i}).$$

Let $\mathbb{O}$ be an order of B, which we assume to contain $\varphi_i(\mathbb{O}_i)$ for $i = 1, 2$ and hence also $\mathbb{O}_L$ (we view φ_i as the identity maps on L). Let $\mathfrak{d}^+$ be the discriminant of $\mathbb{O}$. As in [Goren and Lauter 2007], subject to the assumption $\varphi_1(K_1) \neq \varphi_2(K_2)$, one proves the following lemma:

Lemma 11.2. *The $\mathbb{O}_L$ module $\Lambda = \mathbb{O}_L + \mathbb{O}_L k_1 + \mathbb{O}_L k_2 + \mathbb{O}_L k_1 k_2$ has finite index in $\mathbb{O}$ and is in fact a direct sum $\Lambda = \mathbb{O}_L \oplus \mathbb{O}_L k_1 \oplus \mathbb{O}_L k_2 \oplus \mathbb{O}_L k_1 k_2$.*

Theorem 11.3. *Let $\alpha = \mathrm{Trd}(k_1 k_2)$. We have a divisibility of integral ideals in L:*

$$\mathfrak{d}^+ \mid (4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) - \alpha^2) \quad \text{in } \mathbb{O}_L.$$

Furthermore,

$$N_{L/\mathbb{Q}}(\mathfrak{d}^+) \leq 4^g \frac{\mathrm{disc}(\mathbb{O}_1)\cdot\mathrm{disc}(\mathbb{O}_2)}{\mathrm{disc}(\mathbb{O}_L)^4}.$$

Proof. The discriminant of the order Λ relative to L, $\mathrm{disc}_{B/L}(\Lambda)$, is divisible by the discriminant of $\mathbb{O}$; namely, it is an integral ideal of L divisible by $\mathfrak{d}^+$. Using the basis $\{1, k_1, k_2, k_1 k_2\}$ for Λ and putting $\alpha = \mathrm{Trd}(k_1 k_2)$, we find that the discriminant of Λ is the $\mathbb{O}_L$-ideal generated by

$$\det \begin{pmatrix} 2 & 0 & 0 & \alpha \\ 0 & 2\,\mathrm{Nrd}(k_1) & -\alpha & 0 \\ 0 & -\alpha & 2\,\mathrm{Nrd}(k_2) & 0 \\ \alpha & 0 & 0 & 2\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) \end{pmatrix} = (4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) - \alpha^2)^2,$$

and so $\mathfrak{d}^+ \mid (4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) - \alpha^2)$ in $\mathbb{O}_L$. Thus,

$$N_{L/\mathbb{Q}}(\mathfrak{d}^+) \mid N_{L/\mathbb{Q}}(4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) - \alpha^2) \quad \text{in } \mathbb{Z}.$$

Now, $4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2) - \alpha^2$ is a totally positive element of $\mathbb{O}_L$. Indeed, this is just the Cauchy–Schwartz inequality applied to the bilinear form $\mathrm{Trd}(x\bar{y})$ under every embedding $L \to \mathbb{R}$. We can therefore conclude that

$$N_{L/\mathbb{Q}}(\mathfrak{d}^+) \leq N_{L/\mathbb{Q}}(4\,\mathrm{Nrd}(k_1)\,\mathrm{Nrd}(k_2)).$$

We conclude that

$$\begin{aligned} N_{L/\mathbb{Q}}(\mathfrak{d}^+) &\leq \mathrm{disc}(\mathbb{O}_L)^{-4} 4^{-g} \prod_{i=1}^{2} 4^g\,\mathrm{disc}(\mathbb{O}_L)^2 N_{L/\mathbb{Q}}\,\mathrm{Nrd}(k_i) \\ &\leq \mathrm{disc}(\mathbb{O}_L)^{-4} 4^{-g} \prod_{i=1}^{2} \mathrm{disc}(\mathbb{O}_L[2c_i\kappa_i]) \\ &= \mathrm{disc}(\mathbb{O}_L)^{-4} 4^g \prod_{i=1}^{2} \mathrm{disc}(\mathbb{O}_L[c_i\kappa_i]) = 4^g \frac{\mathrm{disc}(\mathbb{O}_1)\cdot\mathrm{disc}(\mathbb{O}_2)}{\mathrm{disc}(\mathbb{O}_L)^4}. \end{aligned}$$

□

p	Unramified (inert/split)	Inert	Ramified	Ramified
Reduction	ssp	s.sing, not ssp	ssp	ssp
Rapoport?	Yes	Yes	Yes	No
r'	2	4	2	1
Table 3 (K cyclic)	ii, iv, v	iii		vi
Table 4 (K biquadratic)	iii, iv, vii, viii		vi	ix, x, xi
Table 5 (K non-Galois)	iii, vi, viii, ix, x, xi, xiii, xv, xxii, xxiii	vii		xvi, xvii, xviii, xix, xx, xxi, xxiv, xxv, xxvi

Table 1. The case $[L:\mathbb{Q}]=2$. Table numbers refer to [Goren and Lauter 2012]. The column headings refer to the decomposition of p in L. "Reduction" refers to the reduction of the abelian variety modulo $\mathfrak{p}$. The abbreviations "s.sing." and "ssp" mean "supersingular" and "superspecial".

Corollary 11.4. (1) *Let A_i be an abelian variety with CM by $\mathbb{O}_{K_i}$. Choose a common field of definition M for A_1 and A_2 such that M contains the normal closure of both K_1 and K_2 and both A_i have good reduction over M. Let $\mathfrak{p}$ be a prime ideal of M, $(p)=\mathfrak{p}\cap\mathbb{Z}$, and suppose that*

$$A_1 \pmod{\mathfrak{p}} \cong A_2 \pmod{\mathfrak{p}}.$$

Let r be the number of prime ideals $\mathfrak{q}$ in $\mathbb{O}_L$ for which $e(\mathfrak{q}/p)f(\mathfrak{q}/p)$ is odd. If $r>0$, then

$$p \le \left(4^g \frac{\operatorname{disc}_{K_1}\cdot\operatorname{disc}_{K_2}}{\operatorname{disc}(\mathbb{O}_L)^4}\right)^{1/r}.$$

(2) *Suppose that $[L:\mathbb{Q}]=2$ and that A_i are principally polarized abelian surfaces. Then we have the bound*

$$p \le \left(16 \frac{\operatorname{disc}_{K_1}\cdot\operatorname{disc}_{K_2}}{\operatorname{disc}(\mathbb{O}_L)^4}\right)^{1/r'}$$

according to the cases listed in Table 1 (and no other case is possible).

Proof. Since the A_i are principally polarized abelian surfaces, they satisfy the Deligne–Pappas condition and, when p is unramified, even the Rapoport condition. We can therefore use the results of [Bachmat and Goren 1999; Nicole 2005].

If p is split in L, then every supersingular abelian variety is superspecial. In that case, $\operatorname{End}_{\mathbb{O}_L}(A)$ is an order of discriminant $p\mathbb{O}_L$ in $B_{p,L}$, and we apply (1) with $r=2$.

If p is inert, then the reduction is necessarily supersingular by Lemma 11.1 and may or may not be superspecial. If it is superspecial, then, again, $\mathrm{End}_{\mathcal{O}_L}(A)$ is an order of discriminant $p\mathcal{O}_L$ in $B_{p,L}$, and the bound holds with $r' = 2$.

If the reduction is supersingular and not superspecial, then in fact $\mathrm{End}_{\mathcal{O}_L}(A)$ has discriminant $p^2\mathcal{O}_L$, and so we may take $r' = 4$.

Next we consider the case when p is ramified. There are three cases. The first is when we have superspecial reduction and the Rapoport condition holds. In that case, $\mathrm{End}_{\mathcal{O}_L}(A)$ has discriminant $p\mathcal{O}_L$, and we may take $r' = 2$. The second case is when we have superspecial reduction and the Rapoport condition does not hold (but the Deligne–Pappas condition holds). In this case, $\mathrm{End}_{\mathcal{O}_L}(A)$ has discriminant $\mathfrak{p}$, where $\mathfrak{p}$ is the prime of $\mathcal{O}_L$ above p, and we can take $r' = 1$. The last possibility is, ostensibly, that we have supersingular reduction, which is not superspecial. This in fact never happens in the presence of CM by the full ring of integers. It is interesting to note, though, that for supersingular and not superspecial reduction, the abelian variety A has a unique copy of the group scheme α_p contained in it, which is therefore preserved under all endomorphisms. Thus, $\mathrm{End}(A) \hookrightarrow \mathrm{End}(A/\alpha_p)$, and A/α_p is superspecial but doesn't satisfy the Rapoport condition [Andreatta and Goren 2003]. And so, were this case to occur, we could have taken $r' = 1$. □

Remark 11.5. Suppose that $r = 0$. Then g is even, and a maximal order $R \subset B_{p,L}$ has discriminant 1 since $B_{p,L}$ can only be ramified at primes dividing p, and if $F/\mathbb{Q}_p$ is a field extension and $[F : \mathbb{Q}_p] = \alpha$, then $B_{p,\infty} \otimes_{\mathbb{Q}_p} F$ is split if and only if α is even. Taking $F = L_{\mathfrak{q}}$, we have that $\alpha = e(\mathfrak{q}/p)f(\mathfrak{q}/p)$. For every prime p (and for any decomposition behavior of p), there certainly exist supersingular abelian varieties A with RM such that $\mathrm{End}_{\mathcal{O}_L}(A) = R$. This is easily achieved by choosing an R-stable lattice of the Dieudonné module of A. Experience shows, however, that such abelian varieties tend to be badly behaved; for example, the Deligne–Pappas condition tends to fail when p is unramified (it fails in the cases we have checked, and we did not find an example where it holds), or in other cases, such as when p is totally ramified, the Deligne–Pappas condition holds, but the endomorphism ring is not the maximal order. Thus, one would expect that under the Deligne–Pappas condition the discriminant of $\mathrm{End}_{\mathcal{O}_L}(A)$ is never 1 and, if so, one obtains a version of Corollary 11.4(1) in all cases.

In fact, one can be more optimistic and guess that the largest order $\mathcal{O}$ arising for a supersingular characteristic p abelian variety with RM A satisfying the Deligne–Rapoport condition also arises for some superspecial such abelian variety. Superspecial abelian varieties with RM were studied by Nicole [2005; 2008]. When p is unramified in L and A is superspecial, $\mathrm{End}_{\mathcal{O}_L}(A)$ has discriminant $p\mathcal{O}_L$. When p is ramified in L, larger orders arise [Nicole 2005, Theorem 2.8.5], but at least when p is totally ramified, $p\mathcal{O}_L = \mathfrak{p}^{[L:\mathbb{Q}]}$, still the largest order arising (for a superspecial abelian variety) has discriminant $\mathfrak{p}$.

12. Computations: $g = 2$

Consider the two primitive Galois quartic CM fields $K' = \mathbb{Q}(\sqrt{-85+34\sqrt{5}})$ and $K = \mathbb{Q}(\zeta_5)$. The common real quadratic subfield $L = K^+ = K'^+ = \mathbb{Q}(\sqrt{5})$ has strict class number 1 as it has class number 1 and a unit $(1+\sqrt{5})/2$ of negative norm. The field K has class number 1, and the triple of absolute Igusa invariants of the principally polarized abelian surface with CM by K is $i_1 = i_2 = i_3 = 0$. The field K' has class number 2, and the triple of absolute Igusa invariants for one of the CM points associated to K' is

$$i_1 = \frac{2^{33}\cdot 3^{10}\cdot 5^5\cdot 19^5\cdot 521^5}{71^{12}}, \qquad i_2 = \frac{2^{23}\cdot 3^{10}\cdot 5^5\cdot 19^5\cdot 521^3}{71^8},$$
$$i_3 = \frac{2^{16}\cdot 3^7\cdot 5^4\cdot 19^3\cdot 521^2\cdot 755777339}{71^8}.$$

Genus-2 curves over $\mathbb{Q}$ with these invariants are given by the affine models

$$y^2 = x^5 - 1,$$
$$y^2 = -584x^6 - 4020x^5 + 28860x^4 + 130240x^3 - 514920x^2 - 190244x - 289455$$

for $\mathbb{Q}(\zeta_5)$ and K', respectively. In this case, the triple of absolute invariants is insufficient to determine whether the two curves are isomorphic modulo a prime p since the first invariant is zero. To understand for which primes the curves are isomorphic, it is necessary to compute all ten Igusa invariants for the CM point associated to K' to determine which primes divide all ten invariants (see [Goren and Lauter 2012, Section 2.2] for an explanation, especially Consequence 3 at the end of the subsection). In particular, primes that divide the differences of all ten Igusa invariants associated to two CM points of K and K' are primes for which the *coincidence number* of K and K' defined in Section 9 is nonzero.

The prime 19 appears in all three invariants, and checking all ten invariants, we find that they too are all zero modulo 19. There is also a positive contribution at the prime $p = 19$ in our formula in (8-3), which implies a nonzero coincidence number. Since K has class number 1, there is only one superspecial order $R(\mathbb{O}, \lambda)$. We find an element $x \in \mathbb{O}_L$ satisfying conditions **C** and count the elements in $S_2(\mathbb{O}, x)$. Let d and d' be as in Section 6. We find that for $x = 3\sqrt{5} - 3$, the ideal in $\mathbb{O}_L$ generated by $(x^2 - dd')/4$ factors as

$$\mathfrak{p}_2^2\mathfrak{p}_{19,1}\mathfrak{p}_{19,2}.$$

We see that there is a positive contribution for $p = 19$ in our formula because this factorization has both split factors for 19, and 2 is totally inert in K/L but appears to the power 2, so $(x^2 - dd')/(4\cdot 19)$ is a norm of an ideal from K/L, and the set $S_2(\mathbb{O}, x)$ is nonempty.

Consider the other primes that are common to all three numerators in this example. The prime 5 is ramified in L, so our results do not cover it; neither do our formulas pertain to the prime 2, which also appears in all three numerators. The prime 3 divides all ten invariants but is supersingular, not superspecial, and it certainly satisfies the crude bound Theorem 11.3 from Section 11. The prime 521 does not divide all ten invariants.

References

[Andreatta and Goren 2003] F. Andreatta and E. Z. Goren, "Geometry of Hilbert modular varieties over totally ramified primes", *Int. Math. Res. Not.* **2003**:33 (2003), 1786–1835. MR 2005a:14060 Zbl 1045.14012

[Bachmat and Goren 1999] E. Bachmat and E. Z. Goren, "On the non-ordinary locus in Hilbert–Blumenthal surfaces", *Math. Ann.* **313**:3 (1999), 475–506. MR 2000b:14058 Zbl 0919.14014

[Chai 1995] C.-L. Chai, "Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli", *Invent. Math.* **121**:3 (1995), 439–479. MR 96f:11082 Zbl 0990.11039

[Charles et al. 2009a] D. X. Charles, E. Z. Goren, and K. E. Lauter, "Families of Ramanujan graphs and quaternion algebras", pp. 53–80 in *Groups and symmetries* (Montréal, 2007), edited by J. Harnad and P. Winternitz, CRM Proc. Lecture Notes **47**, Amer. Math. Soc., Providence, RI, 2009. MR 2010m:14056 Zbl 1250.05057

[Charles et al. 2009b] D. X. Charles, K. E. Lauter, and E. Z. Goren, "Cryptographic hash functions from expander graphs", *J. Cryptology* **22**:1 (2009), 93–113. MR 2010d:94074 Zbl 1166.94006

[Conrad 2004] B. Conrad, "Gross–Zagier revisited", pp. 67–163 in *Heegner points and Rankin L-series*, edited by H. Darmon and S.-W. Zhang, Math. Sci. Res. Inst. Publ. **49**, Cambridge Univ. Press, 2004. MR 2005h:11121 Zbl 1072.11040

[Dorman 1988] D. R. Dorman, "Special values of the elliptic modular function and factorization formulae", *J. Reine Angew. Math.* **383** (1988), 207–220. MR 89k:11026 Zbl 0626.10022

[Dorman 1989a] D. R. Dorman, "Global orders in definite quaternion algebras as endomorphism rings for reduced CM elliptic curves", pp. 108–116 in *Théorie des nombres* (Québec, 1987), edited by J.-M. De Koninck and C. Levesque, de Gruyter, Berlin, 1989. MR 90j:11043 Zbl 0697.12011

[Dorman 1989b] D. R. Dorman, "Singular moduli, modular polynomials, and the index of the closure of $\mathbf{Z}[j(\tau)]$ in $\mathbf{Q}(j(\tau))$", *Math. Ann.* **283**:2 (1989), 177–191. MR 90k:11149 Zbl 0642.12014

[Goren 2002] E. Z. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Series **14**, Amer. Math. Soc., Providence, RI, 2002. MR 2003c:11038 Zbl 0986.11037

[Goren and Lauter 2006] E. Z. Goren and K. E. Lauter, "Evil primes and superspecial moduli", *Int. Math. Res. Not.* **2006** (2006), Art. ID 53864, 19. MR 2007f:11061 Zbl 1124.14042

[Goren and Lauter 2007] E. Z. Goren and K. E. Lauter, "Class invariants for quartic CM fields", *Ann. Inst. Fourier* (*Grenoble*) **57**:2 (2007), 457–480. MR 2008i:11075 Zbl 1172.11018

[Goren and Lauter 2009] E. Z. Goren and K. E. Lauter, "The distance between superspecial abelian varieties with real multiplication", *J. Number Theory* **129**:6 (2009), 1562–1578. MR 2010k:14085 Zbl 1203.14047

[Goren and Lauter 2012] E. Z. Goren and K. E. Lauter, "Genus 2 curves with complex multiplication", *Int. Math. Res. Not.* **2012**:5 (2012), 1068–1142. MR 2899960 Zbl 1236.14033

[Gross 1986] B. H. Gross, "On canonical and quasicanonical liftings", *Invent. Math.* **84**:2 (1986), 321–326. MR 87g:14051 Zbl 0597.14044

[Gross and Zagier 1985] B. H. Gross and D. B. Zagier, "On singular moduli", *J. Reine Angew. Math.* **355** (1985), 191–220. MR 86j:11041 Zbl 0545.10015

[Lang 1986] S. Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics **110**, Springer, New York, 1986. MR 95f:11085 Zbl 0601.12001

[Nicole 2005] M.-H. Nicole, *Superspecial abelian varieties, theta series and the Jacquet–Langlands correspondence*, Ph.D. thesis, McGill University, 2005, Available at http://search.proquest.com/docview/305374771?accountid=14496. MR 2709763

[Nicole 2008] M.-H. Nicole, "Superspecial abelian varieties and the Eichler basis problem for Hilbert modular forms", *J. Number Theory* **128**:11 (2008), 2874–2889. MR 2009m:11084 Zbl 1214.11076

[Vignéras 1980] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics **800**, Springer, Berlin, 1980. In French. MR 82i:12016 Zbl 0422.12008

[van Wamelen 1999] P. van Wamelen, "Examples of genus two CM curves defined over the rationals", *Math. Comp.* **68**:225 (1999), 307–320. MR 99c:11079 Zbl 0906.14025

[Waterhouse and Milne 1971] W. C. Waterhouse and J. S. Milne, "Abelian varieties over finite fields", pp. 53–64 in *1969 Number Theory Institute* (Stony Brook, NY, 1969), Proc. Sympos. Pure Math. **20**, Amer. Math. Soc., Providence, R.I., 1971. MR 47 #3397 Zbl 0216.33102

[Yu 2004] C.-F. Yu, "The isomorphism classes of abelian varieties of CM-type", *J. Pure Appl. Algebra* **187**:1-3 (2004), 305–319. MR 2004k:14077 Zbl 1087.14030

Communicated by Brian Conrad
Received 2012-02-23 Revised 2012-10-05 Accepted 2012-11-03

goren@math.mcgill.ca *Department of Mathematics and Statistics, McGill University, 805 Sherbrooke Street West, Montreal QC H3A 2K6, Canada*

klauter@microsoft.com *Cryptography Research Group, Microsoft Research, 1 Microsoft Way, Redmond, WA 98052, United States*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2013 is US $200/year for the electronic version, and $350/year (+$40, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 7 No. 6 2013