E. Z. Goren and K. E. Lauter (2012) "Genus 2 Curves with Complex Multiplication,"
International Mathematics Research Notices, Vol. 2012, No. 5, pp. 1068–1142
Advance Access Publication April 12, 2011
doi:10.1093/imrn/rnr052



# Genus 2 Curves with Complex Multiplication

**Eyal Z. Goren[1] and Kristin E. Lauter[2]**

[1]Department of Mathematics and Statistics, McGill University, 805 Sherbrooke St. W., Montreal, Québec, Canada H3A 2K6 and [2]Microsoft Research, One Microsoft Way, Redmond, WA 98052, USA

*Correspondence to be sent to: eyal.goren@mcgill.ca*
*Dedicated to Benedict H. Gross, on the occasion of his 60th birthday.*

The main goal of this paper is to give a bound on the denominators of Igusa class polynomials for genus 2 curves. Our motivation is from cryptography via the use of genus 2 curves with a prescribed number of points, and from class invariants with a view towards class field theory and Stark's conjectures. All known methods for constructing such curves rely on complex multiplication and the calculation of Igusa class polynomials. These polynomials have rational coefficients and their determination requires extensive computation and precision. The results of this paper make it possible now to perform complexity analysis of these algorithms. The analysis for bounding the denominators also informs the prime factorization for certain class invariants. Both problems are translated into questions about isomorphisms between principally polarized abelian surfaces with complex multiplication and products of elliptic curves with the product polarization, over local artinian rings. We give an overview of Igusa's results on the moduli space of genus 2 curves and the method to construct genus 2 curves via their Igusa invariants. We also give a complete characterization of the reduction type of a CM abelian surface, for any type of prime decomposition of the prime, including ramified primes. The methods used in the proofs of the main results involve studying the embedding problem of the quartic CM field into certain matrix algebras over quaternions and invoking techniques from crystalline deformation theory.

Received April 14, 2010; Revised February 17, 2011; Accepted March 14, 2011

## 1 Introduction

While the main goal of this paper is to give a bound on the denominators of Igusa class polynomials for genus 2 curves, our motivation is two-fold: on the one hand, we are interested in applications to cryptography via the use of genus 2 curves with a prescribed number of points, and on the other hand, we are interested in constructions of class invariants with a view towards explicit class field theory and Stark's conjectures. In the following, we give an overview of these motivating problems and explain the contents of the paper.

Some basic protocols in public key cryptography, such as key exchange and digital signatures, rely on the assumption that the discrete logarithm problem in an underlying group is hard. Current available alternatives favor the use of the group of points on an elliptic curve or the Jacobian of a hyperelliptic genus 2 curve over a finite field as the underlying group. The security of the system depends on the largest prime factor of the group order, so it is crucial to be able to construct curves such that the resulting group order is prime, or a small multiple of a prime. Also, for applications in pairing-based cryptography, it may be necessary to impose additional divisibility conditions on the group order. Parameterized families of curves satisfying this type of conditions are called pairing-friendly curves. Thus, algorithms to construct curves with prescribed group orders are required. Currently, typical minimum security requirements require a group size of at least $2^{256}$ when the best-known attacks are square-root algorithms, giving roughly 128 bits of security. Compared with elliptic curves, Jacobians of genus 2 curves are an attractive alternative because they offer comparable security levels over a field of half the bit size, since the group size of the Jacobian of a genus 2 curve over a finite field $\mathbb{F}_p$ is roughly $p^2$, whereas elliptic curves have group size roughly $p$.

In the case of elliptic curves, the polynomial-time point-counting algorithm proposed by Schoof and improved by Elkies and Atkin (or the newer Arithmetic-Geometric Mean algorithm, see Harley, Mestre and Gaudry [24, 38]) allows the following approach: one can pick elliptic curves over a finite field of cryptographic size and count points until a prime group order is found. This solution will not work for generating pairing-friendly curves, however. Also, over prime fields of cryptographic size, point-counting methods for hyperelliptic curves of genus greater than 1 are currently too slow to be practical. Starting with the work of Atkin and Morain on generating elliptic curves with a prescribed group order for primality proving, the standard approach to constructing such curves has been to use the theory of Complex Multiplication in the so-called CM method.

Given a prime number $p$, and a group order $N$ lying in the Hasse–Weil interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$, the goal is to produce an elliptic curve $E$ over $\mathbb{F}_p$ with $N$ points: $\#E(\mathbb{F}_p) = N = p+1-t$, where $t$ is the trace of the Frobenius endomorphism of $E$ over $\mathbb{F}_p$. Set $D = t^2 - 4p$. The Frobenius endomorphism of $E$ has a characteristic polynomial $x^2 - tx + p$, so it follows from the quadratic formula that the roots of this polynomial lie in $\mathbb{Q}(\sqrt{D})$. It is standard to identify the Frobenius endomorphism with a root of this polynomial. If $E$ is not supersingular, as we shall henceforth assume, then $R$, the endomorphism ring of $E$, is an order in the ring of integers of $K = \mathbb{Q}(\sqrt{D})$. Now the problem is transformed into one of generating elliptic curves with endomorphism ring equal to an order $R$ in $K$. Assume for simplicity that $D$ is a fundamental discriminant and so that $R$ is the maximal order $\mathcal{O}_K$ of $K$. It is well known that each such curve can be obtained as the reduction of a unique up-to-isomorphism elliptic curve over $\bar{\mathbb{Q}}$ with CM by $\mathcal{O}_K$. The correspondence between isomorphism classes of elliptic curves over $\bar{\mathbb{Q}}$ with endomorphism ring equal to $\mathcal{O}_K$ and primitive, reduced, positive definite binary quadratic forms of discriminant $D$ gives an easy way to run through all such elliptic curves.

Define the Hilbert class polynomial $H_D(X)$ associated to the field $K$ as follows:

$$H_D(X) = \prod \left( X - j\left( \frac{-b+\sqrt{D}}{2a} \right) \right),$$

where the product ranges over the set of $(a,b) \in \mathbb{Z}^2$ such that $ax^2 + bxy + cy^2$ is a primitive, reduced, positive definite binary quadratic form of discriminant $D$ for some $c \in \mathbb{Z}$, and $j$ denotes the modular $j$-function. The degree of $H_D(X)$ is equal to $h_K$, the class number of $K$, and it is known that $H_D(X)$ has integer coefficients. To find an elliptic curve modulo $p$ with $N$ points over $\mathbb{F}_p$, it suffices to find a root $j$ of $H_D(X)$ modulo $p$. One can then reconstruct the elliptic curve from its $j$-invariant $j$. Assuming $j \neq 0, 1728$ and $p \neq 2, 3$, the required elliptic curve is given by the Weierstrass equation $y^2 = x^3 + 3kx + 2k$, where $k = \frac{j}{1728-j}$. The number of points on the elliptic curve is either $p+1-t$ or $p+1+t$, and one can easily check which one it is by randomly picking points and checking whether they are killed by the group order.

There are at least three approaches to computing the Hilbert class polynomial. The complex analytic approach computes $H_D(X)$ as an integral polynomial by listing all the relevant binary quadratic forms, evaluating the $j$-function as a floating point integer with sufficient precision, and then taking the product and rounding the coefficients to nearest integers. Another approach computes $H_D(X) \bmod \ell$ for sufficiently many small primes $\ell$ and then uses the Chinese remainder theorem (CRT) to compute $H_D(X)$ as a

polynomial with integer coefficients; we shall refer to this approach as the CRT method. The $p$-adic approach uses $p$-adic lifting to approximate the roots and recognize the polynomial. See Belding [1] and the references therein, for a discussion and comparison of these methods. These algorithms are all satisfactory in practice for small $D$. The current world record for the largest $D$ for which $H_D(X)$ has been computed (modulo enough primes to uniquely determine it) is held by Sutherland, using the Explicit CRT method, for some $|D| \approx 10^{16}$; see [51] for a description. (The explicit CRT method calculates $H_D(X)$ modulo sufficiently many primes and then calculates from this data the reduction of $H_D(X)$ modulo any other prime without calculating it as a polynomial with integer coefficients; it was expounded by Bernstein [2], building on ideas of Montgomery, Silverman and Couveignes.)

The situation for generating genus 2 curves is more difficult. The moduli space of genus 2 curves is three dimensional and so at least three invariants are needed to specify a curve up to isomorphism, and, in fact, Igusa's results show that most genus 2 curves are determined by three invariants. The CM algorithm for genus 2 is analogous to the Atkin–Morain CM algorithm for elliptic curves just described. But whereas the Atkin–Morain algorithm computes the Hilbert class polynomial of an imaginary quadratic field $K$ by evaluating the modular $j$-invariants of all elliptic curves with CM by $K$, the genus 2 algorithm computes *Igusa class polynomials* of a quartic CM field $K$ by evaluating the modular invariants of all principally polarized abelian varieties of dimension 2 with CM by $K$.

For a primitive quartic CM field $K$, we can define Igusa class polynomials

$$h_i(X) = \prod_{\tau} (X - i_j(\tau)), \quad j = 1, 2, 3,$$

in analogy with the Hilbert class polynomial for a quadratic imaginary field; the class polynomials depend on the quartic CM field $K$, but we suppress it in the notation. The product is over period matrices in the Siegel upper half space $\mathfrak{H}_2$ of genus 2 modulo $\mathrm{Sp}_4(\mathbb{Z})$, such that the corresponding abelian surfaces have CM by $\mathcal{O}_K$. The functions $i_j$ appearing in the definition are called in this paper absolute Igusa invariants and are Siegel modular functions; they are defined in Section 2.3. The roots of the class polynomials are thus CM values of Siegel modular functions, and it is known that these roots generate abelian extensions of the reflex field of $K$. Again, in analogy with the elliptic curve case (where, using the complex uniformization, $E$ is isomorphic to $y^2 = f(x) = 4x^3 - g_2(\tau)x - g_3(\tau)$, where $g_2(\tau)$ and $g_3(\tau)$ are Eisentein series and also

invariants of the cubic $f(x)$, and $\tau$ is some element of the upper half plane $\mathfrak{H}$), CM values of modular functions on the Siegel upper half space can be directly related to the invariants of a binary sextic defining the genus 2 curve associated to the CM point. Note that the $j$-invariant of an elliptic curve can be calculated in two ways, either as the value of a modular function on a lattice defining the elliptic curve as a complex torus over $\mathbb{C}$, or directly from the coefficients of the equation defining the elliptic curve (the $j$-invariant of $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$ is $1728 \cdot g_2(\tau)^3/(g_2(\tau)^3 - 27g_3(\tau)^2)$). Similarly, for genus 2 curves the triple of Igusa invariants can also be calculated in these two different ways. Using classical invariant theory over a field of characteristic zero, Clebsch [7] defined the triple of invariants of a binary sextic $f$ defining a genus 2 curve $y^2 = f(x)$. Bolza [3] showed how those invariants could also be expressed in terms of theta constants on the period matrix associated to the Jacobian variety and its canonical polarization over $\mathbb{C}$. Igusa [28] showed how these invariants could be extended to work in arbitrary characteristic, and so the invariants are often referred to as Igusa or Bolza–Clebsch–Igusa invariants. These invariants will be discussed in more detail in Section 2. To recover the equation of a genus 2 curve given its invariants, Mestre [37] gave an algorithm which works in most cases, and involves possibly passing to an extension of the field of definition of the invariants.

The CM algorithm for genus 2 curves takes as input a quartic CM field $K$ and outputs the Igusa class polynomials with coefficients in $\mathbb{Q}$ and, if desired, a suitable prime $p$ and a genus 2 curve over $\mathbb{F}_p$ whose Jacobian has CM by $K$. Alternative algorithms for computing Igusa class polynomials have also been proposed and studied, such as the genus 2 Explicit CRT algorithm [12] and a $p$-adic approach [16].

The basis of the CM method in genus 2 was developed in Spallek's thesis [49], where some of the procedures assume that the totally real subfield has class number 1. Later improvements and extensions were given by van Wamelen [54] and Weng [57]. In these algorithms one determines a collection of period matrices that form a set of representatives for isomorphism classes of polarized abelian surfaces with CM by a given field. These are used to compute the Igusa polynomials by evaluating Siegel modular forms to very high precision in order to recognize the coefficients of the minimal polynomials as rational numbers. Unfortunately, the polynomials $h_i(X)$ have rational coefficients, typically not integral coefficients, which makes them harder to recognize from floating-point approximations. The running time of the CM method for generating genus 2 curves over finite fields with a given number of points had not been analyzed until recently, due to the fact that no bound on the denominators of the coefficients of the Igusa class polynomials was known. This paper provides such a bound for the

first time and in his Leiden thesis, M. Streng has used our results to perform a detailed complexity analysis of the CM method; see [50].

Since the polynomials $h_i(X)$ have rational coefficients, we can ask about the prime factorization of the coefficients. In particular, the primes appearing in the denominators are of special interest. In [35], it was conjectured that primes in the denominator are bounded by the discriminant of the CM field and satisfy some additional arithmetic conditions. In fact, the primes in the denominator are primes of bad reduction for one of the associated curves and they imply superspecial reduction of the Jacobian, and so the additional arithmetic conditions are essentially covered by Goren [19], and in more generality by Section 3 of this paper. Furthermore, it was shown in [21] that bad reduction of a CM curve at a prime is equivalent to the existence of a solution to a certain embedding problem: embedding the ring of integers of the primitive quartic CM field into the endomorphism ring of a product of supersingular elliptic curves in a way that is compatible with the Rosati involution induced by the product polarization. In [21], we provided bounds on the primes that can appear in the prime factorization of the denominators. In this paper, we extend that work to provide bounds on the powers to which those primes appear, thereby proving an absolute upper bound on the size of the denominators. In a related work of Bruinier–Yang [4], the factorization of the denominators, when averaged over the corresponding CM cycle, was studied and a precise conjecture was formulated. In the subsequent work of Yang [59], the conjecture was proved for certain classes of quartic CM fields, thereby giving tight bounds on the size of the denominators in those cases. But a general bound needed for the complexity analysis has not been known until the work of this paper.

The investigations carried out in this paper also have a completely different motivation, which comes from class field theory and Stark's conjecture. Consider the modular form that we call $\Theta$ in this paper (Section 2.4); it is the unique Siegel cusp form of weight 10 and full level, up to a scalar, and is equal, up to a scalar, to the product of the squares of the 10 even Riemann theta constants of integer characteristics. (Some call these "half-integral characteristics"; our terminology follows Farkas and Kra [14].) In many ways $\Theta$ is the analog the elliptic cusp form $\Delta$ of weight 12. Because of this analogy, Deshalit and Goren have studied [10] certain algebraic numbers constructed from values of $\Theta$ at CM points associated to a primitive quartic CM field $K$, whose definition parallels the definition of the Siegel units. Certain expressions in such values gave quantities $u(\mathfrak{a}, \mathfrak{b})$ associated to certain ideals in $K$, that depend also on the choice of CM type. These quantities lie in the Hilbert class field of the reflex field of $K$ and have many appealing properties, such as a nice transformation law under Galois automorphism,

and their dependence only on the ideal classes of $\mathfrak{a}$ and $\mathfrak{b}$. Thus, one is justified in calling them class invariants.

A natural question that arose is whether the invariants $u(\mathfrak{a}, \mathfrak{b})$ are actually units, or close to being units, in the sense that one knows their exact prime factorization, and these primes are small relative to, say, the discriminant of the field $K$. While we do not have a complete solution, several results concerning these invariants have been obtained by the authors in recent years [20, 21]. See also the thesis of Vallieres [53] for numerical data. One of the main reasons to study such quantities is Stark's conjectures.

A particular case of Stark's conjecture is the following. Let $L/k$ be an abelian extension of number fields with a Galois group $G$. Let $S$ be a set of primes of $k$ such that $|S| \geq 2$, and such that $S$ contains all the archimedean primes and all the primes ramifying in $L$, as well as a prime splitting completely in $L$. Let $v$ be a place in $S$ that splits completely in $L$ and $w$ a place of $L$ above it. For $\sigma \in G$ define the partial zeta function:

$$\zeta_S(s, \sigma) = \sum_{(\mathfrak{a}, S)=1, \sigma_{\mathfrak{a}}=\sigma} \mathbf{N}_{\mathbf{k}/\mathbb{Q}}\mathfrak{a}^{-s}.$$

Stark's conjectures state that there is a unit $\epsilon$ in $L$ such that

$$\log |\epsilon^{\sigma}|_w = -e \cdot \zeta_S'(0, \sigma),$$

for all $\sigma \in G$, where $e$ denotes the number of roots of unity in $L$. See [52, Chapitre IV, Section 2] for details. In spite of much work in this area, including a thorough study and proof by Stark of the cases $k = \mathbb{Q}$ and $k$ an imaginary quadratic field, it is fair to say that Stark's conjectures are essentially completely open. It is believed that the main obstacle is finding a "good" construction of units, and that was precisely the motivation of [10], although the problem of relating the class invariants $u(\mathfrak{a}, \mathfrak{b})$ to $L$-functions is still outstanding. (It should be remarked that since a quartic CM field has two complex places, the particular Stark conjecture formulated here is true, and easy, and one is really interested in a higher analog, called the Rubin–Stark conjecture; see [45].)

Now, as it turns out, the denominators occurring in the coefficients of the Igusa class polynomials $h_i$ have to do with the modular form $\Theta$ as well, and essentially both questions—the nature of the denominators and the factorization of the invariants $u(\mathfrak{a}, \mathfrak{b})$—have the same underlying geometric question, which is whether an abelian surface with CM by $K$, over some artinian local ring, can be isomorphic to a product of elliptic curves (with additional conditions on polarizations).

There are two central results in this paper. The first result determines the reduction of abelian surfaces with complex multiplication, extending the results in [19].

The main invariants of an abelian surface $A$ over a field of characteristic $p>0$ are its $f$-number, that determines the size of the étale quotient of $A[p]$, and the $a$-number that, together with the $f$-number, determines, for surfaces, the size of the local-local part of that group scheme. These numbers determine, for example, in which Ekedahl–Oort strata the moduli point corresponding to $A$ lies. It turns out, and that was essentially known by Goren [19] and Yu [60], that these numbers can be read from the prime factorization of $p$ in the normal closure $N$ of $K$ over $\mathbb{Q}$ and the CM type. However, to our knowledge, a complete analysis, covering also the case of ramified primes, had not appeared in the literature, and we make this analysis explicit here, in a self-contained manner. The relevance of this issue to denominators is the following. A key observation is that for a prime $p$ to appear in the denominators of the coefficients of the polynomials $h_i$, or for $\mathfrak{p}|p$ to appear in the factorization of a $u(\mathfrak{a},\mathfrak{b})$, some abelian surface with CM by $K$ must be isomorphic over $\bar{\mathbb{F}}_p$ to the product of two supersingular elliptic curves $E\times E'$. This gives $f=0$ and $a=2$, for the reduced surface and so sieves out the "evil primes" according to their factorization in $N$. The results about reduction of abelian surfaces with complex multiplication appear in Section 3.

The second result, which is the main result of this paper, is the following theorem concerning the valuation of special values of certain Siegel modular functions of genus 2.

Let $K=\mathbb{Q}(\sqrt{d})(\sqrt{r})$, where $d$ is a square-free integer and $r\in\mathbb{Z}[\sqrt{d}]$ is a totally negative element. Assume that $K$ is not biquadratic. Let $K^*$ be a reflex CM field associated to $K$ and a CM type; we denote its Hilbert class field by $H_{K^*}$. Let $L=NH_{K^*}$.

**Theorem 1.1.** Let $f=g/\Theta^k$ be a modular function of level one on $\mathfrak{H}_2$ where:

1. The modular form $\Theta$ is $-4\chi_{10}$ in Igusa's notation, and is equal to the product of the squares of the 10 Riemann theta constants with even integral characteristics, normalized to have Fourier coefficients that are integers and of g.c.d. 1.
2. The modular form $g$ is a level 1 modular form of weight 10 k with integral Fourier coefficients.

Let $\tau$ be a CM point associated to $K$ and $K^*$ the reflex field determined by the CM of $\tau$. Let $\mathfrak{p}_L$ be a prime of $L$ above a rational prime $p$ with ramification index $e=e(\mathfrak{p}_L/p)$. Then $f(\tau)\in L$. If $\mathrm{val}_{\mathfrak{p}_L}(f(\tau))<0$ then

$$\mathrm{val}_{\mathfrak{p}_L}(f(\tau))\geq\begin{cases}-2ek[\log_p(d\cdot\mathrm{Tr}(r)^2)+1], & e\leq p-1,\\ -16ek[\log_p(d\cdot\mathrm{Tr}(r)^2)-\frac{1}{2}], & \text{any other case.}\end{cases}\tag{1.1}$$

Furthermore, unless we are in the situation of superspecial reduction, namely, we have a check mark in the last column of the tables in Section 3, $\mathrm{val}_{\mathfrak{p}_L}(f(\tau)) \geq 0$. The valuation $\mathrm{val}_{\mathfrak{p}_L}$ is normalized so that a uniformizer at $\mathfrak{p}_L$ has valuation 1. In addition, if $\mathrm{val}_{\mathfrak{p}_L}(f(\tau)) < 0$, then

$$p \leq 4 \cdot d \cdot \mathrm{Tr}(r)^2. \qquad \square$$

Corollaries 7.5 and 7.6, of this theorem give the applications to denominators of Igusa class polynomials and class invariants described above.

As said, for a prime $p$ to appear in the denominators of the $h_i$, or for $\mathfrak{p}|p$ to appear in the factorization of a $u(\mathfrak{a}, \mathfrak{b})$, some abelian surface with CM by $K$ must be isomorphic over $\bar{\mathbb{F}}_p$ to the product of two supersingular elliptic curves $E \times E'$. A further, and most important condition, is imposed by the fact that the Rosati involution of $E \times E'$ must induce complex conjugation on $K$. We are able to translate the fact that a prime appears to a certain power in the denominators of the $h_i$ (similarly for the $u(\mathfrak{a}, \mathfrak{b})$) to the fact that such an isomorphism with a product of elliptic curves must hold over a certain artinian ring $(R, \mathfrak{m})$ and the index of nilpotency of $\mathfrak{m}$ is proportional to the power of the prime. This requires some results in intersection theory (Section 5) and the introduction of an auxiliary moduli space (Section 4). A certain maneuver, already used in [21], allows us at that point to reduce the problem to a question about endomorphisms of elliptic curves over $R$ whose reduction modulo $\mathfrak{m}$ are supersingular. Some special instances of this problem were studied by Gross in [22], but his results do not suffice for our purposes. We approach this problem using crystalline deformation theory in Section 6; in the course of developing the results we need, we provide more general results that are natural in that context and are likely to be useful for others. Since crystalline deformation theory is only valid under certain restrictions on ramification, we provide an alternative approach that works without any restriction (Section 6.5) and gives results that are not too much worse than crystalline deformation theory gives.

## 2 Moduli of Curves of Genus 2

### 2.1 Curves of genus two—Igusa's results

Let $y_1$, $y_2$, and $y_3$ be independent variables and let $y_4 = \frac{1}{4}(y_1 y_3 - y_2^2)$. The group of fifth roots of unity $\mu_5$ acts on the ring $\mathbb{Z}[\zeta_5][y_1, y_2, y_3, y_4]$ by $[\zeta](y_i) := \zeta^i y_i$ (and trivially on the coefficients). The ring of invariants is defined over $\mathbb{Z}$, namely it is of the form $R \otimes_{\mathbb{Z}} \mathbb{Z}[\zeta_5]$. We denote $R$, *by abuse of notation*, by

$$\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}.$$

The ring $R$ is generated over $\mathbb{Z}$ by 10 elements. One of Igusa's main results [28, p. 613] is that $\mathcal{M}_2$, the coarse moduli space of smooth projective curves of genus 2, satisfies

$$\mathcal{M}_2 \cong \mathrm{Spec}(\mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5}). \tag{2.1}$$

We remark that outside the prime 2, namely if we work over $\mathbb{Z}[1/2]$, we can dispense with $y_4$ and conclude that

$$\mathcal{M}_2 \otimes \mathbb{Z}[1/2] \cong \mathrm{Spec}(\mathbb{Z}[1/2][y_1, y_2, y_3]^{\mu_5})$$

(same abuse of notation). Note that to find generators over $\mathbb{Z}[1/2]$ for $\mathbb{Z}[1/2][y_1, y_2, y_3]^{\mu_5}$ amounts to finding vectors $(a, b, c) \in \mathbb{Z}^3_{\geq 0}$ such that $a + 2b + 3c \equiv 0 \pmod 5$ that generate the semigroup $\{(a, b, c) \in \mathbb{Z}^3_{\geq 0} : a + 2b + 3c \equiv 0 \pmod 5\}$—one associates to the vector $(a, b, c)$ the monomial $y_1^a y_2^b y_3^c$. Such generators are given by the following eight triples:

$$\{(5, 0, 0), (3, 1, 0), (1, 2, 0), (2, 0, 1), (0, 1, 1), (1, 0, 3), (0, 5, 0), (0, 0, 5)\}. \tag{2.2}$$

On the other hand, given a field $k$ of odd characteristic, to find generators for the fraction field $\mathrm{Frac}(k[y_1, y_2, y_3]^{\mu_5})$, one needs generators for the group $\{(a, b, c) \in \mathbb{Z}^3 : a + 2b + 3c \equiv 0 \pmod 5\}$, which one can choose to be the vectors $(2, -1, 0), (3, 0, -1), (5, 0, 0)$ (corresponding to the monomials $y_1^2/y_2, y_1^3/y_3, y_1^5$), for example.

Igusa's construction is based on much earlier work by Clebsch [7] and Bolza [3] on invariants of sextics. A genus 2 curve is hyperelliptic, where a hyperelliptic curve is defined to be a curve that is a double cover of the projective line. Over fields of characteristic different from 2 the situation is very much like over the complex numbers, and one can conclude that such a curve can be written as $y^2 = f(x)$, where $f(x)$ is a separable monic polynomial of degree 6, uniquely determined up to projective substitutions, thus reducing the problems of classifying genus 2 curves to studying when two sextics are equivalent under a projective transformation, or, equivalently, studying the space parameterizing unordered 6-tuples of points in $\mathbb{P}^1$.

### 2.2 Igusa's coordinates

To describe the invariants of sextics we use Igusa's notation. Let

$$y^2 = f(x) = u_0 x^6 + u_1 x^5 + \cdots + u_6,$$

be a hyperelliptic curve and let $x_1, \ldots, x_6$ be the roots of the polynomial $f(x)$. The notation $(ij)$ is a shorthand for the expression $(x_i - x_j)$. Consider then

$$A(u) = u_0^2 \sum_{\text{fifteen}} (12)^2(34)^2(56)^2, \tag{2.3}$$

$$B(u) = u_0^4 \sum_{\text{ten}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2, \tag{2.4}$$

$$C(u) = u_0^6 \sum_{\text{sixty}} (12)^2(23)^2(31)^2(45)^2(56)^2(64)^2(14)^2(25)^2(36)^2, \tag{2.5}$$

$$D(u) = u_0^{10} \prod_{i<j} (ij)^2. \tag{2.6}$$

The subscript "fifteen" in $A$ refers to the fact that there are 15 ways to partition 6 objects into three groups of two elements, the subscript "ten" in $B$ refers to the fact that there are 10 ways to partition six objects into two groups of 3 elements. The subscript "sixty" refers to partitioning six objects into two groups and then finding a matching between these two groups: there are 10 ways to partition into two groups and six matching between the two chosen groups. The invariants $A, B, C$, and $D$ are denoted $A', B', C'$, and $D'$ in [37, p. 319], but we follow Igusa's notation; these invariants are often called now the *Igusa–Clebsch invariants*. Another common notation one finds in the literature is $I_2 = A$, $I_4 = B$, $I_6 = C$, and $I_{10} = D$ (for example, in the Magma help pages on February 2010), but we shall avoid using it, especially since it conflicts with Igusa's notation as in [30, p. 848].

The invariants $A, B, C$, and $D$ are homogenous polynomials of weights $2, 4, 6$, and 10, respectively, in $u_0, \ldots, u_6$, thought of as variables. In addition, they are invariants of index $6, 12, 18$, and 30, respectively, which means the following: Let $f(x, z)$ be the homogenized form of $f$, that is,

$$f(x, z) = u_0 x^6 + u_1 x^5 z + \cdots + u_6 z^6.$$

Let $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2$ and let

$$x = \alpha x' + \beta z', \quad z = \gamma x' + \delta z'.$$

Write, by substituting these expressions for $x$ and $z$, and expanding,

$$f(x, z) = u_0' x'^6 + u_1' x'^5 z' + \cdots + u_6' z'^6.$$

Then, a polynomial $J = J(u_0, \dots, u_6)$ in the variables $u_0, \dots, u_6$ is called an *invariant of index k* if

$$J(u_0', \dots, u_6') = \det(M)^k J(u_0, \dots, u_6).$$

The terminology here is classical and follows, for example, [37]. (An *invariant*, in the terminology of [37] is a covariant of order 0, which means it is an expression in the coefficients of $f$ alone, as is the case here.) An invariant of degree $r$ of a sextic has index $3r$; cf. [37, p. 314].

Note that if we let $f'$ be the polynomial $f'(t) = u_0' t^6 + \cdots + u_6'$ then the two hyperelliptic curves

$$C : y^2 = f(x), \quad C' : y^2 = f'(x),$$

are isomorphic. Indeed, the map

$$(x', y') \mapsto (x, y) := \left( \frac{\alpha x' + \beta}{\gamma x' + \delta}, \frac{y'}{(\gamma x' + \delta)^3} \right)$$

gives an isomorphism $C' \to C$ as we have $(\frac{y'}{(\gamma x' + \delta)^3})^2 = f(\frac{\alpha x' + \beta}{\gamma x' + \delta})$.

In characteristic 0, every separable sextic gives a vector $(A, B, C, D)$ with $D \neq 0$ and, vice versa, every such vector comes from a sextic. Two curves over an algebraically closed field are isomorphic if and only if one curve has invariants $(A, B, C, D)$ and the invariants of the other curve are $(r^2 A : r^4 B : r^6 C : r^{10} D)$ for some $r \neq 0$ in the field [28, Corollary, p. 632] (it would have been more natural to write the powers of $r$ in multiples of 6, but we follow convention here). Thus, it is natural to associate to a sextic a vector $(A : B : C : D)$ in the weighted projective space $\mathbb{P}^3_{2,4,6,10}$. Similar to the case of the usual projective space $\mathbb{P}^3_{1,1,1,1}$, the complement of the hypersurface defined by $D = 0$ is affine. But, where for a usual projective space with coordinates $(x_0, x_1, x_2, x_3)$ the affine variety is $\mathrm{Spec}(\mathbb{Q}[x_0/x_3, x_1/x_3, x_2/x_3])$, for a weighted projective space we need more functions; at the case in hand one needs 10 functions, and these will be given below in terms of certain functions $J_{2i}$; every regular function on the affine variety $\mathbb{P}^3_{2,4,6,10} \setminus \{D = 0\}$ is a polynomial in these functions.

Define, as in Igusa [28, pp. 621–622],

$$J_2 = 2^{-3} A, \quad J_4 = 2^{-5} 3^{-1} (4 J_2^2 - B), \quad J_6 = 2^{-6} 3^{-2} (8 J_2^3 - 160 J_2 J_4 - C),$$
$$J_8 = 2^{-2} (J_2 J_6 - J_4^2), \quad J_{10} = 2^{-12} D.$$

A calculation [28] shows that these invariants can be extended to characteristic 2 and 3.

Let $\mathfrak{R}$ be the ring of homogenous elements of degree 0 in the graded ring generated over $\mathbb{Z}$ by $J_2, J_4, \ldots, J_{10}$ and localized at $J_{10}$. In fact, any *absolute invariant*, namely any invariant which is the quotient of two invariants of the same index, belongs to $\mathfrak{R}$ [28, Proposition 3, p. 633]. One can show that there is an isomorphism

$$\mathfrak{R} \xrightarrow{\sim} \mathbb{Z}[y_1, y_2, y_3, y_4]^{\mu_5},$$

determined by

$$J_2^{e_1} J_4^{e_2} J_6^{e_3} J_8^{e_4} J_{10}^{-e_5} \mapsto y_1^{e_1} y_2^{e_2} y_3^{e_4} y_4^{e_4},$$

where the $e_i$ are nonnegative integers satisfying the relation $e_1 + 2e_2 + 3e_3 + 4e_4 = 5e_5$ and as before $y_4 = \frac{1}{4}(y_1 y_3 - y_2^2)$ (and so $\mathfrak{R}$ can be identified with the ring we previously denoted $R$).

Over $\mathbb{Z}$, the generators of $\mathfrak{R}$ can be taken to be the following:

$$\gamma_1 = J_2^5/J_{10}, \quad \gamma_2 = J_2^3 J_4/J_{10}, \quad \gamma_3 = J_2^2 J_6/J_{10}, \quad \gamma_4 = J_2 J_8/J_{10}, \quad \gamma_5 = J_4 J_6/J_{10},$$
$$\gamma_6 = J_4 J_8^2/J_{10}^2, \quad \gamma_7 = J_6^2 J_8/J_{10}^2, \quad \gamma_8 = J_6^5/J_{10}^3, \quad \gamma_9 = J_6 J_8^3/J_{10}^3, \quad \gamma_{10} = J_8^5/J_{10}^4$$

(Over $\mathbb{Z}[1/2]$, a set of generators is

$$g_1 = J_2^5/J_{10}, \quad g_2 = J_2^3 J_4/J_{10} \quad g_3 = J_2 J_4^2/J_{10}, \quad g_4 = J_2^2 J_6/J_{10}$$
$$g_5 = J_4 J_6/J_{10}, \quad g_6 = J_2 J_6^3/J_{10}^2 \quad g_7 = J_4^5/J_{10}^2, \quad g_8 = J_6^5/J_{10}^3$$

(and the reader will recognize the exponents from (2.2).) We call the $\{\gamma_i\}$ *the Igusa coordinates of* $\mathcal{M}_2$. Here are some consequences of these results.

1. Let $C_1$ and $C_2$ be curves over an algebraically closed field $k$ of characteristic different from 2, and write $C_i : y^2 = f_i(x)$, where $f_i(x) \in k[x]$ is a sextic. Then,

$$C_1 \cong C_2 \iff (\gamma_1(f_1), \ldots, \gamma_{10}(f_1)) = (\gamma_1(f_2), \ldots, \gamma_{10}(f_2)).$$

   (See [28] for the case of $\mathrm{char}(k) = 2$.)
2. Let $C$ now be defined over a number field $L_0$, $C : y^2 = f(x)$, $f(x) \in L_0[x]$, then $C$ has potentially good reduction at a prime $\mathfrak{p}$ of $L_0$, namely there exists a finite extension field $L/L_0$ and an ideal $\mathfrak{P}|\mathfrak{p}$ of $L$ such that $C$ has good reduction modulo $\mathfrak{P}$, if and only if

$$\mathrm{val}_{\mathfrak{p}}(\gamma_i(f)) \geq 0, \quad i = 1, \ldots, 10.$$

3. Let $C_1$ and $C_2$, be curves over a number field $L$, $C_i : y^2 = f_i(x)$ as above, having good reduction at $\mathfrak{p}$. Then,

$$C_1 \pmod{\mathfrak{p}} \cong_{/\bar{\mathbb{F}}_p} C_2 \pmod{\mathfrak{p}} \iff (\gamma_1(f_1), \ldots, \gamma_{10}(f_1)) \equiv (\gamma_1(f_2), \ldots, \gamma_{10}(f_2)) \pmod{\mathfrak{p}}.$$

### 2.3 Efficacy of the absolute Igusa invariants

The so-called *absolute Igusa invariants* are the functions

$$i_1 = A^5/D, \quad i_2 = A^3B/D, \quad i_3 = A^2C/D.$$

The choice of terminology is somewhat unfortunate, as it leads one to think that these invariants determine the isomorphism class of the curve; we will discuss it further below. We remark that these functions are absolute invariants in the sense discussed previously, but this specific choice is not Igusa's. Our terminology here follows [35, 54, p. 313], for example, and agrees with [49] up to powers of 2. We also remark that there is nothing canonical about the choice we make. For many purposes other choices of invariants, each having the form $f/D^a$, where $f$ is some integral invariant and $a$ a positive integer, will be equally good and, in fact, one finds other choices in the literature [50, 57].

Since $D = 2^{12}J_{10}$, the functions $i_1, i_2$, and $i_3$, belong to $\mathfrak{R} \otimes \mathbb{Z}[1/2]$. It is a consequence of the results mentioned so far that the functions $\gamma_j$ are rational functions of the functions $i_j$ and vice versa. This calculation is presented in Tables 1 and 2.

An interesting consequence of this calculation is that the natural map

$$\mathcal{M}_2 \otimes \mathbb{Z}[1/6] = \mathrm{Spec}(\mathfrak{R} \otimes [1/6]) \longrightarrow \mathrm{Spec}(\mathbb{Z}[1/6][i_1, i_2, i_3]) = \mathbb{A}^3_{\mathbb{Z}[1/6]},$$

can be inverted whenever $i_1 \neq 0$. However, given a triple $(i_1, i_2, i_3)$ that is in the image of the map and such that $i_1 = 0$, we find that $A = 0$ and hence also that $i_2 = i_3 = 0$. Thus, there is a unique point of $\mathbb{A}^3$, which is in the image, for which we cannot invert the map and it corresponds to all the genus 2 curves for which $A = 0$. Thus, the absolute Igusa invariants fail to completely determine the isomorphism class of the curve, but only if $i_1 = 0$.

The vanishing locus of $A$ is a surface in $\mathcal{M}_2$. There is a natural immersion,

$$\rho : \mathcal{M}_2 \longrightarrow \mathcal{A}_{2,1}, \tag{2.7}$$

**Table 1.** The absolute Igusa invariants $i_1, i_2, i_3$ in terms of the generators $\gamma_j$

| | |
|---|---|
| $i_1$ | $8 \cdot \gamma_1$ |
| $i_2$ | $\frac{1}{2} \cdot (\gamma_1 - 24 \cdot \gamma_2)$ |
| $i_3$ | $\frac{1}{8} \cdot (\gamma_1 - 20 \cdot \gamma_2 - 72 \cdot \gamma_3)$ |

**Table 2.** The generators $\gamma_j$ in terms of the absolute Igusa invariants $i_1, i_2, i_3$ (the last column gives the denominator)

| | |
|---|---|
| $\gamma_1$ | $2^{-3} \cdot i_1$ |
| $\gamma_2$ | $2^{-6}3^{-1} \cdot (i_1 - 16 \cdot i_2)$ |
| $\gamma_3$ | $\frac{1}{3456} \cdot (i_1 + 80 \cdot i_2 - 384 \cdot i_3)$ |
| $\gamma_4$ | $2^{-11}3^{-3} \cdot \frac{i_1^2 + 416 \cdot i_1 i_2 - 1536 \cdot i_1 i_3 - 768 \cdot i_2^2}{i_1}$ |
| $\gamma_5$ | $2^{-10} \cdot 3^{-4} \cdot \frac{(i_1 - 16 \cdot i_2)(i_1 + 80 \cdot i_2 - 384 \cdot i_3)}{i_1}$ |
| $\gamma_6$ | $2^{-25} \cdot 3^{-7} \cdot \frac{(i_1 - 16 \cdot i_2)(i_1^2 + 416 \cdot i_1 i_2 - 1536 \cdot i_1 i_3 - 768 \cdot i_2^2)^2}{i_1^3}$ |
| $\gamma_7$ | $2^{-22} \cdot 3^{-9} \cdot \frac{(i_1 + 80 \cdot i_2 - 384 \cdot i_3)^2(i_1^2 + 416 \cdot i_1 i_2 - 1536 \cdot i_1 i_3 - 768 \cdot i_2^2)}{i_1^2}$ |
| $\gamma_8$ | $2^{-29} \cdot 3^{-15} \cdot \frac{(i_1 + 80 \cdot i_2 - 384 \cdot i_3)^5}{i_1^2}$ |
| $\gamma_9$ | $2^{-37} \cdot 3^{-12} \cdot \frac{(i_1 + 80 \cdot i_2 - 384 \cdot i_3)(i_1^2 + 416 \cdot i_1 i_2 - 1536 \cdot i_1 i_3 - 768 \cdot i_2^2)^3}{i_1^4}$ |
| $\gamma_{10}$ | $2^{-52} \cdot 3^{-15} \cdot \frac{(i_1^2 + 416 \cdot i_1 i_2 - 1536 \cdot i_1 i_3 - 768 \cdot i_2^2)^5}{i_1^6}$ |

of the moduli space of curves $\mathcal{M}_2$ to the moduli space of principally polarized abelian surfaces with no level structure $\mathcal{A}_{2,1}$, sending a curve to its canonically polarized Jacobian. The image is the complement of the Humbert surface $\mathcal{H}_1$, which is the divisor of the modular form $\Theta$, whose definition we now recall.

Let $\epsilon, \epsilon' \in \mathbb{Q}^g$, $\tau \in \mathfrak{H}_g$, and define the *Riemann theta constant* with *characteristic* $\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right]$ to be the power series

$$\Theta\begin{bmatrix}\epsilon\\ \epsilon'\end{bmatrix}(\tau) = \sum_{N \in \mathbb{Z}^g} e\left(\frac{1}{2}{}^t\left(N + \frac{\epsilon}{2}\right)\tau\left(N + \frac{\epsilon}{2}\right) + {}^t\left(N + \frac{\epsilon}{2}\right)\frac{\epsilon'}{2}\right),$$

where $e(x) = e^{2\pi i x}$. It can be shown that this series defines a holomorphic function $\mathfrak{H}_g \to \mathbb{C}$. If $[\epsilon, \epsilon'] \in \mathbb{Z}^{2g}$ it is called an *integral characteristic* (our terminology follows [14, Chapter VI, Section 1]). If ${}^t\epsilon\epsilon' \equiv 0 \pmod 2$ it is called *even*, and else *odd*. It turns out that for an odd characteristic the theta constant vanishes identically, and for even characteristic $\Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)^2$ depends only on $[\epsilon, \epsilon']$ modulo $(2\mathbb{Z})^{2g}$. For $g = 1$ this gives us three squares of even theta constants, and for $g = 2$ this gives us 10 squares of even theta constants.

One can show that each $\Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)$ to a large enough even power $2r$ is a Siegel modular form of weight $r$ of some level. For $g = 1$, it goes back probably to Jacobi that $\Delta = c\prod_{\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right] \text{ even}} \Theta\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right](\tau)^4$, where $c$ is a constant and $\Delta = E_4^3 - E_6^2$ is the classical modular form of weight 12. Recall that the divisor of $\Delta$ is the cusp of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$. Igusa proved for $g = 2$ that

$$\Theta := 2^{-12} \prod_{\left[\begin{smallmatrix}\epsilon\\ \epsilon'\end{smallmatrix}\right] \text{ even}} \Theta\begin{bmatrix}\epsilon\\ \epsilon'\end{bmatrix}(\tau)^2, \tag{2.8}$$

is a Siegel modular form of level $\mathrm{Sp}(4, \mathbb{Z})$ and weight 10. The power of 2 is introduced to ensure integral Fourier coefficients with gcd 1 (cf. [21]). The divisor of $\Theta$ is precisely the Humbert divisor $\mathcal{H}_1$ (with multiplicity 2). See Section 4.

Via the map (2.7), each of the Igusa invariants is, in a suitable sense, a pull-back via $\rho$ of a meromorphic Siegel modular form whose poles are supported on $\mathcal{H}_1$. These modular forms were calculated by Igusa [31, pp. 177–178] and the reader is referred to this reference for details. The invariant $D$ is the pullback of a scalar multiple of $\Theta$. There is a cusp form of weight 12, which Igusa denotes $\chi_{12}$, such that, in a suitable sense, $A$ is a scalar multiple of the weight 2 meromorphic form $\chi_{12}/\Theta$, [29, p. 195]. We have thus, as sets,

$$\{A = 0\} = \rho^{-1}\{\chi_{12} = 0\}.$$

However, there does not seem to be any simple interpretation for the vanishing locus of $A$.

We say that a point $x \in \mathcal{A}_{2,1}(\mathbb{C})$, with associated principally polarized abelian surface $(A_x, \lambda_x)$, is a CM point associated to a CM field $K$ if $K$ embeds in $\mathrm{End}(A_x) \otimes \mathbb{Q}$ and the Rosati involution defined by $\lambda_x$ induces complex conjugation on $K$. If $K$ is a quartic CM field, we say that $K$ is *nonbiquadratic*, or *primitive*, if $K$ is not a compositum of two quadratic imaginary fields. In this case, any CM type of $K$ is primitive, while if $K$ is biquadratic no CM type of $K$ is primitive. If $K$ is associated to a point $x$ as above, we also call $x$ primitive, or imprimitive, accordingly.

**Proposition 2.1.** Assume the André–Oort conjecture for $\mathcal{A}_{2,1}$. Let $V \subseteq \mathcal{A}_{2,1}(\mathbb{C})$ be the support of the divisor of $\chi_{12}$. There are finitely many primitive CM points on $V$. □

**Proof.** Recall Igusa's description of $\mathcal{M}_2$ as $\mathbb{P}^3_{2,4,6,10} \setminus \{D = 0\} = U//\mathbb{G}_m$, where $U$ is the open set of vectors with nonzero last coordinate. Viewed thus, $V$ is the image of $\{(0, B, C, D) : D \neq 0\}$, which is an irreducible (affine) variety, hence $V$ is irreducible itself.

Let $S$ be the collection of all primitive CM points on $V$. Let $C$ be the Zariski closure of $S$. If $S$ is infinite then $C$ is either a curve, or $V$ itself. In either case, it follows from the André–Oort conjecture, known to be true under GRH by the work of Klinger-Yafaev [58], that $C$ is either a Shimura curve, or a Shimura surface. It remains to review the possibilities: (i) if $C$ is a Shimura curve then every CM point on $C$ is coming from some biquadratic (equivalently, nonprimitive) CM field of degree 4; (ii) if $C = V$ then $V$ is a priori in the Hecke orbit of some Humbert surfaces, but that Hecke orbit is a union of Humbert surfaces (this follows easily from the moduli interpretation). Since the Humbert surfaces in $\mathcal{A}_{2,1}$ are irreducible, as is $V$, $V$ is a Humbert surface itself, which is not the case. Indeed, $V$ is the divisor of the modular form $\chi_{12}$ and the results of van der Geer [17] (see, in particular, Section 8 there) imply that the divisor of $\chi_{12}$ is *not* supported on a union of Humbert surfaces. ■

**Remark.** As the referee had suggested, the proposition can also be proved for other surfaces in $\mathcal{A}_{2,1}$, such as the divisor of the Eisenstein series $\psi_4$ or $\psi_6$ (see below). The proof is the same. This implies that for other invariants used in the literature as a system of absolute invariants one also has that the locus where the invariants do not determine the curve contains only finitely many primitive CM points. Thus, for all practical purposes, when using any such system of invariants for the purpose of generating curves whose Jacobian has CM by a given primitive CM field, one can "pretend" that the invariants determine the curve. The likelihood this will cause a problem in the computation is practically nill. □

### 2.4 Igusa class polynomials

In [21, Section 5.2], it was explained how the absolute Igusa invariants can also be expressed in terms of Siegel modular functions. We summarize this here for the reader's convenience.

The Igusa functions $i_1$, $i_2$, and $i_3$ can be defined as rational functions in Siegel Eisenstein series, $\psi_w$, of weights $w = 4, 6, 10, 12$. To begin with, the cusp forms $\Theta$ and $\chi_{12}$, of weights 10 and 12, introduced above can be expressed in terms of these Eisenstein

series as follows [29, p. 195; 30, p. 848]:

$$-2^{-2}\Theta = \chi_{10} = \frac{-43867}{2^{12}\cdot 3^5\cdot 5^2\cdot 7\cdot 53}(\psi_4\psi_6 - \psi_{10})$$

and

$$\chi_{12} = \frac{131\cdot 593}{2^{13}\cdot 3^7\cdot 5^3\cdot 7^2\cdot 337}(3^2\cdot 7^2\psi_4^3 + 2\cdot 5^3\psi_6^2 - 691\psi_{12}).$$

Then the *Igusa functions* $i_1, i_2,$ and $i_3$ can be expressed as

$$i_1 = 2\cdot 3^5\frac{\chi_{12}^5}{\chi_{10}^6}, \quad i_2 = 2^{-3}\cdot 3^3\frac{\psi_4\chi_{12}^3}{\chi_{10}^4}, \quad i_3 = 2^{-5}\cdot 3\frac{\psi_6\chi_{12}^2\chi_{10} + 2^2\cdot 3\psi_4\chi_{12}^3}{\chi_{10}^4}.$$

Let $K$ be a primitive, that is, not biquadratic, CM field of degree 4 over $\mathbb{Q}$. We define the *Igusa class polynomials* to be

$$h_1(x) = \prod_\tau (x - i_1(\tau)), \quad h_2(x) = \prod_\tau (x - i_2(\tau)), \quad h_3(x) = \prod_\tau (x - i_3(\tau)), \tag{2.9}$$

where the product is taken over all $\tau \in \mathrm{Sp}(4,\mathbb{Z})\backslash\mathfrak{H}_2$, such that the associated principally polarized abelian variety has CM by $\mathcal{O}_K$. One can define other absolute invariants, called $\mathrm{j}_1$, $\mathrm{j}_2$, and $\mathrm{j}_3$, as in [21, p. 473], where it is also remarked that $i_1 = 2^{-12}\mathrm{j}_1$ and $i_2 = 2^{-12}\mathrm{j}_2$, and then we define the corresponding class polynomials as follows:

$$\mathfrak{h}_i(x) = \prod_\tau (x - \mathrm{j}_i(\tau)), \quad i = 1, 2, 3. \tag{2.10}$$

The advantage of using these is that it is easy to see from their definition, and the fact that the Fourier coefficients of $\Theta$ are integers with gcd 1 (cf. [21]), that they satisfy the hypotheses of our Main Theorem.

### 2.5 Ramification locus of $\mathcal{A}_{2,n}(\mathbb{C}) \to \mathcal{A}_{2,1}(\mathbb{C})$

Let $n$ be a positive integer. We denote by $\mathcal{A}_{2,n}$ the moduli scheme of principally polarized abelian surfaces with symplectic level-$n$ structure over $\mathrm{Spec}(\mathbb{Z}[\zeta_n, 1/n])$. $\mathcal{A}_{2,1}\otimes\mathbb{Z}[\zeta_n, 1/n]$ is the quotient of $\mathcal{A}_{2,n}$ by the finite group $\mathrm{Sp}(4,\mathbb{Z}/n\mathbb{Z})/\{\pm I_4\}$. We denote the by $\mathcal{H}_{\Delta,n}$ the Humbert surface of invariant $\Delta$ (the discriminant of a real quadratic order) in $\mathcal{A}_{2,n}(\mathbb{C})$ [18, Chapter IX]. It is irreducible for $n = 1$, but reducible for $n > 1$.

Let $n \geq 3$, so the representation $\mathrm{Aut}(A, \lambda) \to \mathrm{Aut}(A[3])$ is faithful. The ramification locus of $\pi_n : \mathcal{A}_{2,n} \to \mathcal{A}_{2,1}$ is clearly the locus of points $x$ on $\mathcal{A}_{2,1}$ with nontrivial stabilizers, which, by the moduli interpretation, correspond to principally polarized abelian surfaces $(A, \lambda)$ such that $\mathrm{rAut}(A, \lambda) \neq \{1\}$, where rAut is the reduced automorphism group (namely the group of automorphisms $\varphi : A \to A$ such that $\varphi^* \lambda = \lambda$, modulo the subgroup $\{\pm 1\}$). Furthermore, in that case, any point in the fibre over $x$ has the same ramification index, equal to the cardinality of $\mathrm{rAut}(A, \lambda)$.

We say that a component of the Humbert divisor $\mathcal{H}_{\Delta,n}$ in $\mathcal{A}_{2,n}(\mathbb{C})$ is ramified if it is contained in the ramification locus of $\pi_n$ and otherwise we say it is unramified. If every component of $\mathcal{H}_{\Delta,n}$ is unramified then

$$\pi_n^*(\mathcal{H}_{\Delta,1}) = \mathcal{H}_{\Delta,n}.$$

**Lemma 2.2.** If $\Delta \neq 1, 4$ then every component of $\mathcal{H}_{\Delta,n}$ is unramified. If $\Delta \in \{1, 4\}$ then the ramification index along each component of $\mathcal{H}_{\Delta,n}$ is 2. □

**Proof.** Suppose first that $\Delta$ is not a square. In this case, every abelian variety $(A, \lambda)$ parameterized by $\mathcal{H}_{\Delta,n}$ has real multiplication by a real quadratic order of discriminant $\Delta$ and, generically, only by that order. Thus, generically, $\mathrm{Aut}(A, \lambda) = \{\pm 1\}$ (as the Rosati involution is the identity). That resolves this case.

Suppose now that $\Delta$ is a square, but $\Delta \neq 1$. Then, except for a codimension 1 subset, the points of $\mathcal{H}_{\Delta,n}$ correspond to curves $C$ of genus 2 affording a map $C \to E$ of degree $\sqrt{\Delta}$ to an elliptic curve $E$, that does not factor nontrivially through another elliptic curve; see Frey–Kani [15].

From the classification of $\mathrm{Aut}(C)$, cf. [28, Section 8], we deduce that there is only one two-dimensional family of curves of genus 2 with a nontrivial reduced automorphism group; the reduced automorphism group of the generic member of this family is cyclic of order 2. This family, as one observes, is comprised exactly the curves $C$ of genus 2 allowing a map $C \to E$ of degree 2 to an elliptic curve $E$, ramified at exactly two points of $E$. This family is thus the Humbert divisor $\mathcal{H}_{4,1}$, and in particular, we have proved the lemma for all cases but $\Delta = 1$.

It is easy to see that for a generic pair of elliptic curves $E_1$ and $E_2$ we have $\mathrm{Aut}(E_1 \times E_2, \lambda_1 \times \lambda_2) = \{(\pm 1, \pm 1)\}$. Thus, our proof is complete. ■

### 2.6 Existence of good models for abelian varieties with complex multiplication

Our purpose in this section is to prove a lemma concerning models of abelian varieties with complex multiplication with good reduction at a set of primes over specified

number fields. For the notion of a reflex field, see Lang [33, Chapter 1, Section 5]. For the notion of primitive CM type see [33, Chapter 1, Sections 2–3] (a *primitive* CM type is called there a *simple* CM type, but we prefer the terminology *primitive* that agrees with Shimura [48], for example).

We use here the notation $\mathcal{A}_{g,n}$ for the moduli scheme of $g$-dimensional abelian varieties with symplectic level-$n$ structure. We let $\pi_n\colon \mathcal{A}_{g,n} \to \mathcal{A}_{g,1}$ be the natural morphism. For the notion of toroidal compactifications of $\mathcal{A}_{g,n}$, in the setting we need them, a good introduction is Chai [6], and the complete theory is in Faltings–Chai [13].

We let $\underline{A} = (A, \iota, \lambda)$ be a $g$-dimensional complex abelian variety $A$ with CM by a field $K$ of degree $2g$ over $\mathbb{Q}$, $\iota : \mathcal{O}_K \to \mathrm{End}_{\mathbb{C}}(A)$, and $\lambda$ a principal polarization of $A$ whose Rosati involution induces complex conjugation on $K$. We let $\tau = \tau_1$ be the moduli point of $\underline{A}$ on $\mathcal{A}_{g,1}$ and we let $\tau_n$ be a point of $\mathcal{A}_{g,n}$ such that $\pi_n(\tau_n) = \tau$. The point $\tau_n$ is the moduli point of $\underline{A}_n = (A, \iota, \lambda, \gamma)$, where $\gamma : A[n] \to (\underline{\mathbb{Z}/n\mathbb{Z}})^{2g}$ is a symplectic isomorphism of group schemes.

We let $\Phi \subset \mathrm{Hom}(K, \mathbb{C})$ be the CM type associated to $(A, \iota)$ and $K^*$ the associated reflex field. Let $\mu$ denote the roots of unity lying in $K$ and $\mathbb{Q}(\mu)$ the corresponding cyclotomic subfield. Let $H_{K^*}$ be the Hilbert class field of $K^*$. Let $M[n]$ be the field of definition of the point $\tau_n$. We choose some embedding of $K$ into $\mathbb{C}$ and view all fields as subfields of $\mathbb{C}$.

**Lemma 2.3.** With the notation above, assume that $\Phi$ is a primitive CM type and that $\mathbb{Q}(\mu) \subseteq K^*$. (This holds at least in the following cases: (1) $\mu = \{\pm 1\}$, which is the typical case; (2) $K$ is a quartic CM field and $\Phi$ is primitive; (3) $K/\mathbb{Q}$ is Galois and $\Phi$ is primitive.) Let $n \geq 3$ be an integer.

1. Let $S$ be a finite set of primes of $H_{K^*}$. Then $\underline{A}$ has a model $\underline{A}' = (A', \iota', \lambda')$ over $H_{K^*}$ with good reduction at every prime $\mathfrak{p}$ of $S$.
2. $M[n]$ is a finite field extension of $K^*$ that is unramified at every prime $\mathfrak{p}$ of $K^*$ not dividing $n$.
3. $\underline{A}$ has a model over $M[n]$ with good reduction at every prime not dividing $n$.
4. Let $N$ be the normal closure of $K$. Let $L = NH_{K^*}$ and $L_n = LM[n]$. If $\mathfrak{p}$ is a prime of $L_n$ not dividing $n$ then the extension $L_n/N$ is unramified at $\mathfrak{p}$. There exist a model of $\underline{A}$ over $L_n$ with good reduction at $\mathfrak{p}$. □

**Proof.** By Milne [39], noting that in our case the conditions added in the errata hold automatically, $\underline{A}$ has a model over its field of moduli. This field is contained in

$H_{K^*}$ [33, Chapter 5, Theorem 4.1]. There is thus no harm in assuming, to begin with, that $\underline{A}$ is defined over $H_{K^*}$. We remark that in the case actually used in the sequel $K$ is a quartic CM field and then our assertion also follows from [47, Example 1, p. 525].

We now prove (1). Since $\underline{A}$ is defined over $H_{K^*}$ that contains $\mathbb{Q}(\mu)$, the set $S$ is ordinary in the terminology of Serre–Tate [46, p. 505]; see the remarks there (their $\mu_m$ is always contained in $\mu$). Thus, we may apply Theorem 8 of [46] to deduce that $(A, \iota)$ has a model of $H_{K^*}$ with good reduction at every prime $\mathfrak{p}$ of $S$. Furthermore, the abelian variety $A$ carries a principal polarization $\lambda$ compatible with $\iota$, by our assumption. The complex uniformization of such polarizations as "$\mathrm{Tr}_{K/\mathbb{Q}}(\xi\bar{\alpha}\beta)$" [33, Chapter 1, Section 4] shows that such a polarization is always invariant under $\mu$. Therefore, applying the first remark of [46, p. 506], we conclude that $\underline{A}$ has a model over $H_{K^*}$ with good reduction at every prime $\mathfrak{p}$ of $S$.

Next we prove (2). The field $M[n]$, being a field of definition for the isomorphism class of $\underline{A}_n$, contains the reflex field $K^*$. Let $\mathfrak{p}$ be a prime of $H_{K^*}$ not dividing $n$ and let $\underline{A}'$ be a model of $\underline{A}$ over $H_{K^*}$ with good reduction at $\mathfrak{p}$. Then $M[n] \subset H_{K^*}(A'[n])$, because $\underline{A}'$ has a symplectic level-$n$ structure defined over $H_{K^*}(A'[n])$, which is a Galois extension of $H_{K^*}$ unramified at $\mathfrak{p}$ by [46, Corollary 2]. Thus, $H_{K^*}(A'[n])$ is also an extension of $K^*$ unramified at $\mathfrak{p}$. Since $K^* \subseteq M[n] \subseteq H_{K^*}(A'[n])$, (2) follows.

For (3) we use that $\mathcal{A}_{g,n}$ is a fine moduli scheme over $\mathrm{Spec}(\mathbb{Z}[\zeta_n, 1/n])$. Let $\mathcal{A}^\dagger_{g,n}$ be a smooth toroidal compactification of $\mathcal{A}_{g,n}$ over $\mathrm{Spec}(\mathbb{Z}[\zeta_n, 1/n])$. It carries a semi-abelian variety $\mathcal{X}$ over it. Let $\beta_0 : \mathrm{Spec}(M[n]) \to \mathcal{A}_{g,n} \hookrightarrow \mathcal{A}^\dagger_{g,n}$ be the morphism corresponding to the point $\tau_n$. Then $\beta_0^*\mathcal{X}$ is a model for $\underline{A}$ over $M[n]$. Since the morphism $\mathcal{A}^\dagger_{g,n} \to \mathrm{Spec}(\mathbb{Z}[\zeta_n, 1/n])$ is proper, the morphism $\beta_0$ extends to a morphism $\beta$ over $\mathrm{Spec}(\mathbb{Z}[\zeta_n, 1/n])$, $\beta : \mathrm{Spec}(\mathcal{O}[1/n]) \to \mathcal{A}^\dagger_{g,n}$, where $\mathcal{O}$ is the ring of integers of $M[n]$. Then $\beta^*\mathcal{X}$ is a principally polarized semi-abelian variety over $\mathcal{O}$ whose generic fiber is a model for $(A, \lambda)$, hence for $(A, \iota, \lambda)$, over $M[n]$ ($\iota$ extends automatically from the generic fibre to $\beta^*\mathcal{X}$). Choose a prime $\mathfrak{P}$ of $M[n]$ not dividing $n$. As is well known, since $[K : \mathbb{Q}] = 2g > g$, the toric part of the mod $\mathfrak{P}$ reduction of $\beta^*\mathcal{X}$ must be trivial and so $\beta^*\mathcal{X}$ has good reduction modulo $\mathfrak{P}$.

Finally, (4) is a direct consequence of the previous claims. (In the sequel, we will only use (4), and, in fact, only when $K$ is a primitive quartic CM field.) ■

**Remark.** Let $\mathfrak{P}$ be a prime of $H_{K^*}$, $\mathfrak{p} = \mathfrak{P} \cap K^*$. The part of the lemma which is important for the sequel is the existence of a model for $\underline{A}$ over an extension of $H_{K^*,\mathfrak{P}}$ (the completion

of $H_{K^*}$ at $\mathfrak{P}$) for which we can bound the ramification. The lemma gives such an extension with ramification bounded by $e(\mathfrak{p}/p)$. This can also be proved by other methods. Howard [26] studied the local deformation space for abelian varieties with CM over $\bar{\mathbb{F}}_p$ in and showed that it is given by $\mathrm{Spf}(\mathbb{W}_\Phi)$, where $\mathbb{W}_\Phi$ is the completion of the maximal unramified extension of $O_{K^*,\mathfrak{p}}$. The universal object then gives a model of $\underline{A}$ that descends to a finite field extension of $K^*$ contained in the maximal unramified extension of $K^*_{\mathfrak{p}}$. The information is less precise than that given in the lemma, but suffices for the applications in the paper. □

## 3 Reduction Type of Abelian Surfaces with Complex Multiplication

Our goal in this section is to study the reduction type of an abelian surface with complex multiplication by a field $K$ modulo a prime ideal of the field of definition, lying above $p$, as a function of the decomposition of the prime $p$ in $K$. Some basic algebra relevant to this analysis is given in Section 3.1. An important tool in our analysis is the theory of Dieudonné modules, which we quickly summarize in Section 3.2, for the reader's convenience. The results of these two sections are then used in Sections 3.3–3.6 to analyze the Dieudonné modules of abelian surfaces with CM. The final sections provide examples.

### 3.1 Combinatorics of embeddings and primes

Let $K$ be a number field and $N$ its normal closure over $\mathbb{Q}$. Let $G$ be the Galois group $\mathrm{Gal}(N/\mathbb{Q})$, acting on $K$ by $k \mapsto g(k), g \in G$, and let $H = \mathrm{Gal}(N/K) < G$. Fix inclusions

$$\varphi_{\mathbb{C}} \colon N \to \mathbb{C}, \quad \varphi_p \colon N \to \bar{\mathbb{Q}}_p.$$

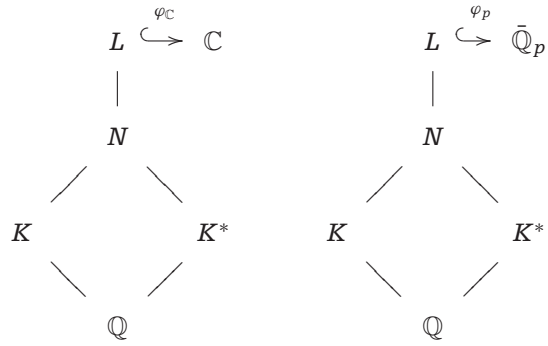
This allows us to make the following identifications:

$$\mathrm{Hom}(K, \mathbb{C}) = \varphi_{\mathbb{C}} \circ G/H, \quad \mathrm{Hom}(K, \bar{\mathbb{Q}}_p) = \varphi_p \circ G/H,$$

where a left coset $gH$ gives the embeddings $\varphi_{\mathbb{C}} \circ g$ and $\varphi_p \circ g$. We then have an identification

$$\mathrm{Hom}(K, \mathbb{C}) = \mathrm{Hom}(K, \bar{\mathbb{Q}}_p).$$

Let $L \supseteq N$ be a finite extension and choose extensions of $\varphi_{\mathbb{C}}, \varphi_p$ to $L$. We have the following diagrams:




Let $\mathfrak{P}$ be the maximal ideal of $\bar{\mathbb{Q}}_p$. The choice of $\varphi_p$ provides us with a prime ideal $\mathfrak{p}_{L,1} := \varphi_p^{-1}(\mathfrak{P})$ of $L$, and so with prime ideals $\mathfrak{p}_{N,1} = \mathfrak{p}_{L,1} \cap N$ of $N$ and $\mathfrak{p}_{K,1} = \mathfrak{p}_{L,1} \cap K$ of $K$. Let $D$ be the decomposition group of $\mathfrak{p}_{N,1}$ in $N$ and $I$ its inertia group. Let $e = \sharp I$. The prime ideals above $p$ in $N$ are in bijection with the cosets $G/D$:

$$p\mathcal{O}_N = \prod_{\alpha \in G/D} \mathfrak{p}_{N,\alpha}^e, \quad \mathfrak{p}_{N,\alpha} = \alpha(\mathfrak{p}_{N,1}).$$

The decomposition (respectively, inertia) group of $\mathfrak{p}_{N,\alpha}$ is $D^\alpha := \alpha D \alpha^{-1}$ (respectively, $I^\alpha := \alpha I \alpha^{-1}$). The primes dividing $p$ in $K$ correspond to the double cosets $H\backslash G/D$. More precisely,

$$p\mathcal{O}_K = \prod_{H\alpha D \in H\backslash G/D} \mathfrak{p}_{K,\alpha}^{e(\alpha)}, \quad \mathfrak{p}_{K,\alpha} = \alpha(\mathfrak{p}_{N,1}) \cap K,$$

where, by Lemma 3.1, $e(\alpha) = [I^\alpha : I^\alpha \cap H]$.

Let $\alpha \in G$. It induces a homomorphism $\varphi_p \circ \alpha \colon K \to \bar{\mathbb{Q}}_p$ that depends only on $\alpha H$. It therefore defines a prime $(\varphi_p \circ \alpha)^{-1}(\mathfrak{P})$ of $K$, or more precisely $(\varphi_p|_K \circ \alpha)^{-1}(\mathfrak{P})$. We have

$$(\varphi_p|_K \circ \alpha)^{-1}(\mathfrak{P}) = (\alpha^{-1}\varphi_p|_N^{-1}(\mathfrak{P})) \cap K = \alpha^{-1}(\mathfrak{p}_{N,1}) \cap K = \mathfrak{p}_{K,\alpha^{-1}}. \tag{3.1}$$

That is, *the coset $\alpha H$ corresponding to an embedding $K \to \bar{\mathbb{Q}}_p$ induces the prime corresponding to the double coset $H\alpha^{-1}D$.* (This "inversion" is a result of our definition of $\mathfrak{p}_{N,\alpha}$ as $\alpha(\mathfrak{p}_{N,1})$, as opposed to $\alpha^{-1}(\mathfrak{p}_{N,1})$, made in order to conform with [19].)

Suppose that we are given a finitely generated torsion-free $\mathcal{O}_L$-module $M$ on which $\mathcal{O}_K$ acts as $\mathcal{O}_L$-endomorphisms. Then $M_{\mathbb{C}} = M \otimes_{\mathcal{O}_L,\varphi_{\mathbb{C}}} \mathbb{C}$ is a finite-dimensional vector space over $\mathbb{C}$, which is an $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{C} = K \otimes_{\mathbb{Q}} \mathbb{C}$-module. We have then a decomposition

$$M_{\mathbb{C}} = \bigoplus_{\varphi \in \mathrm{Hom}(K,\mathbb{C})} M_{\mathbb{C}}(\varphi) = \bigoplus_{\alpha \in G/H} M_{\mathbb{C}}(\alpha), \tag{3.2}$$

where $M_{\mathbb{C}}(\varphi)$ is the eigenspace for the character $\varphi\colon K \to \mathbb{C}$, and where, using the identifications $\mathrm{Hom}(K,\mathbb{C}) = \mathrm{Hom}(K,N) = G/H$, we have let $M_{\mathbb{C}}(\alpha) := M_{\mathbb{C}}(\varphi_{\mathbb{C}} \circ \alpha)$. We assume that each eigenspace is either zero or one dimensional, and so we get a subset

$$\Phi \subset \mathrm{Hom}(K, N),$$

corresponding to the nontrivial eigenspaces. We call $\Phi$ a "CM type", although none of the fields appearing in our discussion so far needs to be a CM field.

On the other hand, we also have the finite-dimensional $\bar{\mathbb{Q}}_p$-vector space $M_p := M \otimes_{\mathcal{O}_L,\varphi_p} \bar{\mathbb{Q}}_p$, grace of the homomorphism $\varphi_p\colon L \to \bar{\mathbb{Q}}_p$, which is an $\mathcal{O}_K \otimes_{\mathbb{Z}} \bar{\mathbb{Q}}_p = K \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}_p$-module. Since all the homomorphisms $K \to \bar{\mathbb{Q}}_p$ factor as $K \to N \xrightarrow{\varphi_p} \bar{\mathbb{Q}}_p$, we have a decomposition, similar to the one in (3.2),

$$M_p = \bigoplus_{\varphi \in \mathrm{Hom}(K,\bar{\mathbb{Q}}_p)} M_p(\varphi) = \bigoplus_{\alpha \in G/H} M_p(\alpha). \tag{3.3}$$

Moreover, the decomposition $K \otimes_{\mathbb{Q}} N \cong \bigoplus_{\alpha \in G/H} N$ implies that for each $\alpha \in G/H$ there is a one dimensional $L$-subspace $M_L(\alpha)$ of $M_L := M \otimes_{\mathcal{O}_L} L$, such that

$$M_{\mathbb{C}}(\alpha) = M_L(\alpha) \otimes_{L,\varphi_{\mathbb{C}}} \mathbb{C}, \quad M_p(\alpha) = M_L(\alpha) \otimes_{L,\varphi_p} \bar{\mathbb{Q}}_p.$$

And so, in the obvious sense, $\Phi$ becomes a "$p$-adic CM type" as well.

Now, the decomposition in (3.3) can be packaged as follows: We have $\mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p = \bigoplus_{\mathfrak{p}|p} \mathcal{O}_{K_\mathfrak{p}}$ and thus $K \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}_p = \bigoplus_{\mathfrak{p}|p} (K_\mathfrak{p} \otimes_{\mathbb{Q}_p} \bar{\mathbb{Q}}_p)$, or

$$K \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}_p = \bigoplus_{\alpha \in H\backslash G/D} (K_{\mathfrak{p}_{K,\alpha}} \otimes_{\mathbb{Q}_p} \bar{\mathbb{Q}}_p).$$

This decomposition induces a decomposition

$$M_p = \bigoplus_{\alpha \in H\backslash G/D} M_{p,\alpha}. \tag{3.4}$$

Note that, due to (3.1), the relation between (3.3) and (3.4) is (sic!)

$$M_p(\alpha) \subseteq M_{p,\alpha^{-1}}. \tag{3.5}$$

### 3.2 Background on Dieudonné modules and $p$-divisible groups

General references for this section are Manin [36] and Oda [41]. Let $G$ be a commutative $p$-divisible group over a perfect field $k$ of characteristic $p$. By definition $G$ is a commutative group scheme over $k$ and, letting $G[p^a]$ be the kernel of multiplication by $p^a$, $[p^a]: G \to G$, we have $G = \varinjlim_a G[p^a]$, $[p](G[p^{a+1}]) = G[p^a]$ and $G[p]$ is a group scheme of finite rank over $k$ called the height of $G$. To a $p$-divisible group one associates its Serre dual $G^t = \varinjlim G[p^a]^t$, where $G[p^a]^t$ is the dual of the finite commutative group scheme $G[p^a]$ (representing the functor $\mathcal{H}om(G[p^a], \mathbb{G}_m)$.) Then $G$ is a direct sum $G = G_{\ell\ell} \oplus G_{\ell e} \oplus G_{e\ell}$, where "$\ell$" stands for "local" (the spectrum of a local ring) and "e" stands for "étale", and each $G_{xy}$ is a $p$-divisible group that is a direct limit of finite commutative groups schemes that have property $x$ and whose dual has property $y$.

If $A$ is a $g$-dimensional abelian variety over $k$ then $A[p^\infty] := \varinjlim A[p^a]$, where $A[p^a]$ is the $p^a$-torsion of $A$, is a self-dual $p$-divisible group of dimension $g$ and height $2g$.

Let $W(k)$ denote the Witt vectors of $k$, and $\sigma : W(k) \to W(k)$ the Frobenius automorphism, lifting the Frobenius automorphism $x \to x^p$ on $k$. A Dieudonné module $D$ over $k$ is a finitely generated $W(k)$-module, equipped with two additive functions $F, V : D \to D$ such that

$$F(\lambda \cdot x) = \sigma(\lambda) \cdot F(x), \quad V(\lambda \cdot x) = \sigma^{-1}(\lambda) \cdot V(x), \quad \forall x \in D, \lambda \in W(k),$$

and such that, denoting by $[p]$ the multiplication-by-$p$ map on $D$, we have

$$FV = VF = [p].$$

The main theorem in the theory of Dieudonné modules is that there is an anti-equivalence of categories between the category of commutative $p$-divisible groups $G$ over $k$ and $W(k)$-torsion-free Dieudonné modules over $k$, $G \mapsto D(G)$, with the

following properties:

1. The functor $D(\cdot)$ commutes with base change: if $k \to \ell$ is a homomorphism of perfect fields then $D(G \otimes_k \ell) = D(G) \otimes_{W(k)} W(\ell)$ (where equality means canonical isomorphism). In particular, $D(G^{(p)}) = D(G) \otimes_{k,\sigma} k$, where $G^{(p)}$ is the base-change of $G$ relative to Frobenius.
2. As a result, one finds that the Frobenius morphism $F : G \to G^{(p)}$ induces a $\sigma$-linear map $F : D(G) \to D(G)$ which is precisely the map $F$ in the definition of a Dieudonné module. Similarly for Verschiebung.
3. $G$ is local if and only if $F : D(G) \to D(G)$ is topologically nilpotent; $G$ is étale if and only if $F : D(G) \to D(G)$ is an isomorphism.
4. $D(G^t) = \mathrm{Hom}(D(G), W(k) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p / W(k))$ and where $F$ and $V$ are defined on the right-hand side by $(F\alpha)(x) = \alpha(Vx)^\sigma$, $(V\alpha)(x) = \alpha(Fx)^{\sigma^{-1}}$.
5. The height of $G$ is the length of $D(G)$ as a $W(k)$-module.
6. There exists canonical isomorphisms $T_G^* \cong D(G)/FD(G)$ and $T_{G^t} \cong \ker(V : D(G)/pD(G) \to D(G)/pD(G))$, where $T$ denotes the tangent space at the origin.

A closely related anti-equivalence is between the category of commutative finite group schemes $H$ over $k$ killed by $p$ and Dieudonné modules over $W(k)$, killed by $p$ (so, in effect, $k$-vector spaces), $H \mapsto D(H)$. It satisfies properties similar to the above. If $G$ is a $p$-divisible group then

$$D(G)/pD(G) = D(G[p]).$$

We define the $a$-number and $f$-number of a $p$-divisible group $G$ as the $a$-number and $f$-number of $H = G[p]$, where those are the following. Consider the group scheme $\alpha_p := \mathrm{Ker}([p] : \mathbb{G}_a \to \mathbb{G}_a) = k[x]/(x^p)$ (with co-multiplication $x \mapsto x \otimes 1 + 1 \otimes x$). Then $\mathrm{Hom}(\alpha_p, H)$ has a natural $k$-vector space structure [42, Chapter II.12] and we let $a(G) = \dim_k \mathrm{Hom}(\alpha_p, H)$ (this number is denoted $\tau(G)$ in [42], but conventions have changed); it depends only on $H_{\ell,\ell}$. The $f$-number of $H$ is that integer $f$ such that $\sharp H(k^{\mathrm{alg}}) = p^f$; it depends only on $H_{e\ell}$. One can show that $a(H)$ is the rank of $\mathrm{Ker}(F) \cap \mathrm{Ker}(V) \cap H$, and so is also the dimension over $k$ of $D(H)/(FD(H) + VD(H))$. Similarly, the $f$-number is the rank of $D(H_{e\ell})/VD(H_{e\ell})$. Thus, both the $a$-number and the $f$-number can be read from the Dieudonné module of $G$. If $G$ is the $p$-divisible group of a $g$-dimensional abelian variety, its $a$-number and $f$-number satisfy the following inequalities: $0 \le a \le g$, $0 \le f \le g$, and $a > 0 \Leftrightarrow f < g$.

We recall that a $g$-dimensional abelian variety over a field $k$ of characteristic $p$ is called *ordinary* if $\sharp\, A[p](k^{\mathrm{alg}}) = p^g$, where $k^{\mathrm{alg}}$ is an algebraic closure of $k$. This is the case if and only if $f(A) = g$. An abelian variety is called *superspecial* if $A$ is isomorphic over $k^{\mathrm{alg}}$ to a product of $g$ supersingular elliptic curves. By a theorem of Oort [43], this is the case if and only if $a(A) = g$. Note that it follows then that $f(A) = 0$.

Finally, we remark that it is often easier to do calculations with a covariant theory and, for that reason, some authors prefer to work with a covariant Dieudonné theory, $G \mapsto \mathbb{D}(G)$. Such a theory is easily deduced from the contravariant theory by duality, letting $\mathbb{D}(G) = D(G)^t$.

### 3.3 The case of quartic fields and Dieudonné modules

Let $K$ be a CM field of degree 4 over the rational numbers and let $A$ be a principally polarized abelian surface with complex multiplication by $\mathcal{O}_K$, CM type $\Phi$, defined over a field $L$ and having everywhere good reduction. Let $K^*$ be the reflex field. We assume that $L$ contains a normal closure $N$ of $K$ and let $G = \mathrm{Gal}(N/\mathbb{Q})$. The module $M$ is $\mathbb{H}^1_{\mathrm{dR}}(A/\mathcal{O}_L)$, where $A$ is an abelian variety over $\mathcal{O}_L$. Thus, our notation conforms with that in the previous section.

Let $K^+$ be the totally real subfield of $K$. Let $p$ be a prime number. Our purpose is to determine the reduction $\bar{A}$ of $A$ modulo a prime ideal $\mathfrak{p}_L$ of $L$. It follows from results of Yu [60] that the Dieudonné module of $\bar{A}$ is determined uniquely by $\Phi$ and the prime decomposition of $p$ in $K$ (and not just in the case of surfaces). A fortiori, the Ekedahl–Oort strata in which it falls is determined. In the case of surfaces, the complete information is contained in two numbers

$$a(\bar{A}) = \dim \mathrm{Hom}_{\bar{\mathbb{F}}_p}(\alpha_p, \bar{A} \otimes \bar{\mathbb{F}}_p), \qquad f(\bar{A}) = \log_p \sharp A[p](\bar{\mathbb{F}}_p),$$

the $a$-number and $f$-number.

We make the situation more explicit than in [60], and provide a self-contained proof in our case. We will have several fields to consider: $N$, $K$, $K^*$ (the reflex field determined by $K$ and $\Phi$), and the totally real subfields $K^+$ and $K^{*+}$. The basic information is the factorization of $p$ in $N$. As above, we fix a prime ideal $\mathfrak{p} = \mathfrak{p}_{N,1} = \mathfrak{p}_L \cap N$ of $N$. The decomposition of $p$ in each field is determined by the pair of subgroups $(I, D)$, where $I$ is the inertia group of $\mathfrak{p}$ in $N$ and $D$ is its decomposition group. The pair of subgroups $(I, D)$ of $\mathrm{Gal}(N/\mathbb{Q})$ satisfies the two restrictions:

- $I \lhd D$;
- $D/I$ is a cyclic group.

As explained above, having chosen $\mathfrak{p}$, we may index the primes dividing $p$ in $N$ by coset representatives for $D$ in $G$. If these coset representatives are $a, b, c, \ldots$ (so $G = aD \sqcup bD \sqcup cD \sqcup \cdots$), then we write $p\mathcal{O}_N = \mathfrak{p}_{N,a}^e \mathfrak{p}_{N,b}^e \mathfrak{p}_{N,c}^e \cdots$, where $e = \sharp I$ and $\mathfrak{p}_{N,a} := a(\mathfrak{p}_N)$ (and in particular, $\mathfrak{p}_{N,1} = \mathfrak{p}$). Since the primes appearing in the decomposition of $p$ in $N$ are determined by $G/D$, the primes appearing in the decomposition of $p$ in a subfield $N^H$ of $N$, corresponding to a subgroup $H$ of $G$, are determined by $H\backslash G/D$. As above, we shall denote such primes by $\mathfrak{p}_{N^H,x}$ where $x$ is a representative for a double coset $HxD$. (This is consistent with the previous notation for $H = \{1\}$.) The following lemma is used to determine ramification in subfields.

**Lemma 3.1.** Let $Q \subset B \subset N$ be three number fields where $N/Q$ is Galois with Galois group $G$. Let $B$ correspond to a subgroup $H$ of $G$. Let $\mathfrak{p}_N$ be a prime ideal of $N$, $\mathfrak{p}_B = \mathfrak{p}_N \cap B$ and $\mathfrak{p}_Q = \mathfrak{p}_N \cap Q$. Let $I(\mathfrak{p}_N)$ be the inertia group in $G$. Then,

$$e(\mathfrak{p}_B/\mathfrak{p}_Q) = [I(\mathfrak{p}_N) : I(\mathfrak{p}_N) \cap H]$$

and

$$e(\mathfrak{p}_N/\mathfrak{p}_B) = \sharp\, I(\mathfrak{p}_N) \cap H.$$

**Proof.** This is Lemma 3.3.29 in Cohen [9]. ■ □

The main tool for studying the reduction $\bar{A} = A \pmod{\mathfrak{p}_L}$ of the abelian surface $A$ is the covariant Dieudonné module $\mathbb{D}$ of $\bar{A}[p]$ over $\bar{\mathbb{F}}_p$. To link between the properties of $\bar{A}$ and the properties of $A$ over the complex numbers, we make use of the de Rham cohomology $\mathbb{H}^1_{\mathrm{dR}}(A/\mathcal{O}_L)$, which is a torsion-free $\mathcal{O}_L$-module of rank $2g$ with the following properties. Let $A_{\mathbb{C}} = A \otimes_{\mathcal{O}_L} \mathbb{C}$ (via $\varphi_{\mathbb{C}}$). We have $\mathbb{H}^1_{\mathrm{dR}}(A/\mathcal{O}_L) \otimes_{\mathcal{O}_L} \mathbb{C} \cong H^1_{\mathrm{Betti}}(A_{\mathbb{C}}, \mathbb{C}) \supset T^*_{A_{\mathbb{C}},0}$ and so the complex CM type is visible. Let $k = \mathcal{O}_L/\mathfrak{p}_L \subset \bar{\mathbb{F}}_p$ (via $\varphi_p$). Then, we have $\mathbb{H}^1_{\mathrm{dR}}(A/k) = \mathbb{H}^1_{\mathrm{dR}}(A/\mathcal{O}_L) \otimes_{\mathcal{O}_L} k$, while $\mathbb{D} = \mathbb{H}^1_{\mathrm{dR}}(A/k) \otimes \bar{\mathbb{F}}_p$, by [41]. This allows the transfer of information from characteristic zero to characteristic $p$. The formalism of the previous section will be applied to $M = \mathbb{H}^1_{\mathrm{dR}}(A/\mathcal{O}_L)$.

The $a$-number and $f$-number of $\bar{A}$ can of course be read from $\mathbb{D}$. The Dieudonné module has a decomposition relative to the $\mathcal{O}_{K^+}$ action and a refined decomposition relative to the $\mathcal{O}_K$ action. Using $\mathfrak{p}_{K^+}$ to denote a prime ideal of $\mathcal{O}_{K^+}$ above $p$ and similarly for $\mathfrak{p}_K$, we have, by virtue of the decompositions $\mathcal{O}_{K^+} \otimes \mathbb{Z}_p = \oplus_{\mathfrak{p}_{K^+}} \mathcal{O}_{K^+,\mathfrak{p}_{K^+}}$,

$\mathcal{O}_K \otimes \mathbb{Z}_p = \oplus_{\mathfrak{p}_K} \mathcal{O}_{K,\mathfrak{p}_K}$, induced decompositions

$$\mathbb{D} = \oplus_{\mathfrak{p}_{K^+}} \mathbb{D}(\mathfrak{p}_{K^+}), \quad \mathbb{D}(\mathfrak{p}_{K^+}) = \oplus_{\mathfrak{p}_K | \mathfrak{p}_{K^+}} \mathbb{D}(\mathfrak{p}_K).$$

Here each $\mathbb{D}(\mathfrak{p}_{K^+})$ is a self-dual Dieudonné module of dimension $2e(\mathfrak{p}_{K^+}/p) f(\mathfrak{p}_{K^+}/p)$, which is then decomposed in Dieudonné modules $\mathbb{D}(\mathfrak{p}_K)$ of dimension $e(\mathfrak{p}_K/p) f(\mathfrak{p}_K/p)$ (here $f(\mathfrak{p}_K/p)$, etc. denotes the degree $[\mathcal{O}_K/\mathfrak{p}_K : \mathbb{Z}/p\mathbb{Z}]$ and should not be confused with the $f$-number of the abelian variety). On $\mathbb{D}(\mathfrak{p}_{K^+})$, there is an action of $\mathcal{O}_{K^+,\mathfrak{p}_{K^+}} \otimes \bar{\mathbb{F}}_p \cong \oplus_\alpha \bar{\mathbb{F}}_p[t]/(t^e)$, where the summation is over embeddings $\alpha$ of the maximal unramified subring $\mathcal{O}^{\mathrm{ur}}_{K^+,\mathfrak{p}_{K^+}}$ of $\mathcal{O}_{K^+,\mathfrak{p}_{K^+}}$ into $W(\bar{\mathbb{F}}_p)$ and $e = e(\mathfrak{p}_{K^+}/p)$. There is a similar and compatible decomposition of $\mathcal{O}_{K,\mathfrak{p}_K} \otimes \bar{\mathbb{F}}_p$. These decompositions induce decompositions of the Dieudonné modules $\mathbb{D}(\mathfrak{p}_{K^+})$ and $\mathbb{D}(\mathfrak{p}_K)$, such that $\mathbb{D}(\mathfrak{p}_{K^+}) = \oplus_\alpha \mathbb{D}(\mathfrak{p}_{K^+}, \alpha)$ and $\mathbb{D}(\mathfrak{p}_K) = \oplus_\alpha \mathbb{D}(\mathfrak{p}_K, \alpha)$. $\mathbb{D}(\mathfrak{p}_{K^+}, \alpha)$ is a vector space of dimension $2e(\mathfrak{p}_{K^+}/p)$, which is a free rank 2 module over $\bar{\mathbb{F}}_p[t]/(t^e)$ on which $\mathcal{O}_{K^+,\mathfrak{p}_{K^+}} = \mathcal{O}^{\mathrm{ur}}_{K^+,\mathfrak{p}_{K^+}}[\pi]$ acts via the map $\bar{\alpha} : \mathcal{O}^{\mathrm{ur}}_{K^+,\mathfrak{p}_{K^+}} \to \bar{\mathbb{F}}_p$ and $\pi$, which is an Eisenstein element, acts via $t$. A similar and compatible description is obtained for $\mathbb{D}(\mathfrak{p}_K, \alpha)$. Frobenius induces maps $\mathbb{D}(\mathfrak{p}_{K^+}, \alpha) \to \mathbb{D}(\mathfrak{p}_{K^+}, \sigma \circ \alpha)$.

Implicit in our considerations is the identification of $\mathrm{Hom}(K, N)$ with $\mathrm{Hom}(K, \bar{\mathbb{Q}}_p)$, where $N$ is a normal closure of $K$. This identification is done as discussed in detail above. In particular, we note that the subspace $\mathbb{D}(\mathfrak{p}_K, \alpha)$ is associated with the prime ideal $\mathfrak{p}_{K,\alpha^{-1}}$. Since $H^0(\bar{A}, \Omega^1_{\bar{A},\bar{\mathbb{F}}_p}) \subset \mathbb{D}$, any $\alpha \in \Phi$ contributes 1 to the dimension of the kernel of Frobenius on $\mathbb{D}(\mathfrak{p}_{K,\alpha^{-1}})$. This often allows us to conclude that $\mathrm{Fr}^2 = 0$ on $\mathbb{D}$. In this case, since $\mathrm{Im}(F) = \mathrm{Ker}(V)$ on $\mathbb{D}$, we conclude that $\mathrm{Ker}(V)$ is a two-dimensional $\bar{\mathbb{F}}_p$-vector space on which both $F$ and $V$ act as zero. Thus, $\mathrm{Ker}(V)$ is the Dieudonné module of $\alpha_p \oplus \alpha_p$, which implies $a = 2$ (and so $f = 0$); that is, we have superspecial reduction (see Section 3.2).

Another useful tool to quickly decide some properties of the reduction is the following relation. Let $K^*$ be the reflex field defined by the CM type of the abelian variety under consideration and let $\Phi^*$ be the reflex type. Let $\mathfrak{p}_{K^*,1} = \mathfrak{p}_{N,1} \cap K^*$. Then some power of $\mathrm{Norm}_{\Phi^*}(\mathfrak{p}_{K^*,1})$ is equal to a power of Fr, viewed as endomorphisms of the reduction. One can be more precise (see [33]), but we note that this suffices to calculate the $f$-number of the reduction, because the $f$-number is equal to $\dim_{\bar{\mathbb{F}}_p}(F^n \mathbb{D})$ for $n \gg 0$.

### 3.4 $K$ cyclic Galois

In this case, $K = N = K^*$. The Galois group is cyclic of order 4, generated by $g$, say, where $g^2$ is the complex conjugation. The CM type is $\{1, g\}$, $\{g, g^2\}$, $\{g^2, g^3\}$, or $\{g^3, 1\}$. Since the

**Table 3.** Reduction in the cyclic case

| | $I$ | $D$ | Decomposition of $p$ in $K = K^*$ | Decomposition of $p$ in $K^+$ | $\mathrm{Norm}_{\Phi^*}(\mathfrak{p}_{K,1})$ | $a$ | $f$ | ssp? |
|---|---|---|---|---|---|---|---|---|
| i | $\{1\}$ | $\{1\}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,g}\mathfrak{p}_{K,g^2}\mathfrak{p}_{K,g^3}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,g}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,g^3}$ | 0 | 2 | × |
| ii | $\{1\}$ | $\{1, g^2\}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,g}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,g}$ | $p$ | 2 | 0 | √ |
| iii | $\{1\}$ | $G$ | $\mathfrak{p}_{K,1}$ | $\mathfrak{p}_{K^+,1}$ | $p^2$ | 1 | 0 | × |
| iv | $\{1, g^2\}$ | $\{1, g^2\}$ | $\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,g}^2$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,g}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,g}$ | 2 | 0 | √ |
| v | $\{1, g^2\}$ | $G$ | $\mathfrak{p}_{K,1}^2$ | $\mathfrak{p}_{K^+,1}$ | $p$ | 2 | 0 | √ |
| vi | $G$ | $G$ | $\mathfrak{p}_{K,1}^4$ | $\mathfrak{p}_{K^+,1}^2$ | $\mathfrak{p}_{K,1}^2$ | 2 | 0 | √ |

reduction type does not depend on the way $K$ is embedded in $A$, namely we can compose with an automorphism $K \to K$, we may assume that the CM type is $\{1, g\}$. The reflex CM field $K^*$ is $K$ and $\Phi^* = \{1, g^{-1}\}$. The possibilities are listed in Table 3.

The unramified case appears in [19], but we shall do one case to illustrate our method. Consider the case (ii). We have a decomposition

$$\mathbb{D} = \mathbb{D}(\mathfrak{p}_{K^+,1}) \oplus \mathbb{D}(\mathfrak{p}_{K^+,g}),$$

and $\mathbb{D}(\mathfrak{p}_{K^+,i})$, $i = 1, g$, is a two-dimensional $\bar{\mathbb{F}}_p$-vector space that does not decompose further relative to the $\mathcal{O}_{K^+}$ action. However, $\mathbb{D}(\mathfrak{p}_{K^+,i}) = \mathbb{D}(\mathfrak{p}_{K,i})$, because $\mathfrak{p}_{K^+,i}$ is inert in $K$, and

$$\mathbb{D}(\mathfrak{p}_{K,i}) = \mathbb{D}(\mathfrak{p}_{K,i}, \alpha) \oplus \mathbb{D}(\mathfrak{p}_{K,i}, \sigma \circ \alpha),$$

where $\alpha$ is an embedding $K \to \bar{\mathbb{Q}}_p$ associated with $\mathfrak{p}_{K,i}$. Frobenius takes $\mathbb{D}(\mathfrak{p}_{K,i}, \alpha)$ to $\mathbb{D}(\mathfrak{p}_{K,i}, \sigma \circ \alpha)$, and vice-versa. The CM type is $\{1, g\}$ and we note that $g$ switches $\mathfrak{p}_{K,1}$ and $\mathfrak{p}_{K,g}$. This means that the cotangent space, or rather $H^0(A, \Omega^1_{A/\bar{\mathbb{F}}_p}) \otimes_{\bar{\mathbb{F}}_p,\sigma} \bar{\mathbb{F}}_p = \mathbb{D}(\mathrm{Ker}\,\mathrm{Fr})$, which is an $\mathcal{O}_K$-module, is not contained completely in any of $\mathbb{D}(\mathfrak{p}_{K,i})$. Thus, Frobenius has a kernel on each of $\mathbb{D}(\mathfrak{p}_{K,i})$. It follows that $\mathrm{Fr}^2$ is zero on each $\mathbb{D}(\mathfrak{p}_{K,i})$ and hence on $\mathbb{D}$ and that implies that $a(\bar{A}) = 2$ and $f(\bar{A}) = 0$, as explained in Section 3.3.

In case (iv) we again have

$$\mathbb{D} = \mathbb{D}(\mathfrak{p}_{K^+,1}) \oplus \mathbb{D}(\mathfrak{p}_{K^+,g}),$$

and $\mathbb{D}(\mathfrak{p}_{K^+,i})$ is a two-dimensional $\bar{\mathbb{F}}_p$-vector space that does not decompose further relative to the $\mathcal{O}_{K^+}$ action. However, $\mathbb{D}(\mathfrak{p}_{K^+,i}) = \mathbb{D}(\mathfrak{p}_{K,i})$ and $\mathbb{D}(\mathfrak{p}_{K,i})$ becomes a rank 1 module

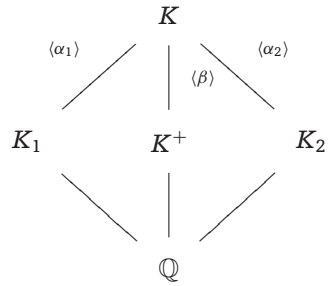
over $\bar{\mathbb{F}}_p[t]/(t^2)$ by using the $\mathcal{O}_K$ action and Frobenius is a module homomorphism. Once more, since $g$ permutes $\mathfrak{p}_{K^+,1}$ and $\mathfrak{p}_{K^+,g}$, it follows that Frobenius has a kernel on each of $\mathbb{D}(\mathfrak{p}_{K^+,i})$ and since the dimension of the kernel of Frobenius is two, it follows that the kernel of Frobenius must be $(t) \oplus (t) \subset D(\mathfrak{p}_{K,1}) \oplus D(\mathfrak{p}_{K,g})$ and $\mathrm{Fr}^2 = 0$.

In case (v), after a similar analysis we reach the conclusion that $\mathbb{D} = \bar{\mathbb{F}}_p[t]/(t^2) \oplus \bar{\mathbb{F}}_p[t]/(t^2)$ and that Frobenius, which commutes with the $\bar{\mathbb{F}}_p[t]/(t^2)$ structure, permutes the components. Whether the kernel of Frobenius is one of the components, or the submodule $(t) \oplus (t)$, we have $\mathrm{Fr}^2 = 0$ (in fact, taking into consideration the CM type we must have that the kernel is $(t) \oplus (t)$, but this is not important at present).

In case (vi) we conclude that $\mathbb{D} = \bar{\mathbb{F}}_p[t]/(t^4)$ and that Frobenius acts as a $\bar{\mathbb{F}}_p[t]/(t^4)$-module homomorphism. It follows that the kernel of Frobenius, being an $\bar{\mathbb{F}}_p[t]/(t^4)$-module is $(t^2)$ and so is the image. Hence $\mathrm{Fr}^2 = 0$ again.

### 3.5 $K$ biquadratic

In this case $K = N$ is the compositum $K_1K_2$ where $K_i$ are quadratic imaginary fields. Recall that we also call $K$ imprimitive since, in this case, every CM type is imprimitive, namely, induced from a CM type of a quadratic imaginary subfield. Let $K^+$ be the totally real subfield of $K$. Write the Galois group is $\{1, \alpha_1, \alpha_2, \beta\}$ where $K_i$ is fixed by $\alpha_i$ and $\beta$ is the complex conjugation. We have the following diagram:




The possible CM types are $\{1, \alpha_i\}$ and $\{\beta, \alpha_i\}$ and twisting the action of $\mathcal{O}_K$ by an automorphism we may assume the CM type is $\{1, \alpha_1\}$ or $\{1, \alpha_2\}$. The situation being symmetric, we assume w.l.o.g that the CM type is $\{1, \alpha_1\}$ (it is induced from the CM type $\{1\}$ of $K_2$). The reflex CM field is $K_1$ and the reflex CM type is $\{1\}$. In this case $A$ is isogenous to $E \otimes_{\mathbb{Z}} \mathcal{O}_L$, or equivalently to $E \otimes_{K_1} K$, where $E$ is an elliptic curve with CM by $\mathcal{O}_{K_1}$. Thus, $\bar{A}$ is ordinary if $p$ is split in $K_1$ and supersingular otherwise (and in that case one still needs to figure out its $a$-number). Now, $p$ is split in $K_1$ if and only if $\langle D, \alpha_1 \rangle \neq G$.

**Table 4.** Reduction in the bi-quadratic case

| | $I$ | $D$ | Decomposition of $p$ in $K = K^*$ | Decomposition of $p$ in $K^+$ | $\mathrm{Norm}_{\Phi^*}(\mathfrak{p}_{K,1})$ | $a$ | $f$ | ssp? |
|---|---|---|---|---|---|---|---|---|
| i | $\{1\}$ | $\{1\}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,\alpha_1}\mathfrak{p}_{K,\beta}\mathfrak{p}_{K,\alpha_2}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,\alpha_1}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,\alpha_1}$ | 0 | 2 | × |
| ii | $\{1\}$ | $\{1,\alpha_1\}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,\beta}$ | $\mathfrak{p}_{K^+,1}$ | $\mathfrak{p}_{K,1}^2$ | 0 | 2 | × |
| iii | $\{1\}$ | $\{1,\beta\}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,\alpha_1}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,\alpha_1}$ | $p$ | 2 | 0 | √ |
| iv | $\{1\}$ | $\{1,\alpha_2\}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,\beta}$ | $\mathfrak{p}_{K^+,1}$ | $p$ | 2 | 0 | √ |
| v | $\{1,\alpha_1\}$ | $\{1,\alpha_1\}$ | $\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,\beta}^2$ | $\mathfrak{p}_{K^+,1}^2$ | $\mathfrak{p}_{K,1}^2$ | 0 | 2 | × |
| vi | $\{1,\alpha_1\}$ | $G$ | $\mathfrak{p}_{K,1}^2$ | $\mathfrak{p}_{K^+,1}^2$ | $p$ | 2 | 0 | √ |
| vii | $\{1,\beta\}$ | $\{1,\beta\}$ | $\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,\alpha_1}^2$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,\alpha_1}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,\alpha_1}$ | 2 | 0 | √ |
| viii | $\{1,\beta\}$ | $G$ | $\mathfrak{p}_{K,1}^2$ | $\mathfrak{p}_{K^+,1}$ | $p$ | 2 | 0 | √ |
| ix | $\{1,\alpha_2\}$ | $\{1,\alpha_2\}$ | $\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,\beta}^2$ | $\mathfrak{p}_{K^+,1}^2$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,\alpha_1}$ | 2 | 0 | √ |
| x | $\{1,\alpha_2\}$ | $G$ | $\mathfrak{p}_{K,1}^2$ | $\mathfrak{p}_{K^+,1}^2$ | $p$ | 2 | 0 | √ |
| xi | $G$ | $G$ | $\mathfrak{p}_{K,1}^4$ | $\mathfrak{p}_{K^+,1}^2$ | $\mathfrak{p}_{K,1}^2$ | 2 | 0 | √ |

Consider for example case (vi). After the usual analysis we find that $\mathbb{D} \cong \bar{\mathbb{F}}_p[t]/(t^2) \oplus \bar{\mathbb{F}}_p[t]/(t^2)$, where Fr is $\bar{\mathbb{F}}_p[t]/(t^2)$ $\sigma$-linear and switches the components. Its kernel is then either one of the components, or the submodule $(t) \oplus (t)$. In any case, $\mathrm{Fr}^2 = 0$ and so $a = 2$. Cases vii, viii and x lead exactly to the same setting.

In case (ix), once again $\mathbb{D} \cong \bar{\mathbb{F}}_p[t]/(t^2) \oplus \bar{\mathbb{F}}_p[t]/(t^2)$ but now Fr acts on each component separately. $\bar{A}$ is ordinary if the kernel of Fr is one of the components and is supersepecial if the kernel is $(t) \oplus (t)$. Since ordinary is not possible, because $p$ is inert in $K_1$ (or, we can argue by using the CM type that Frobenius has a kernel on each component), we are in the superspecial case.

In case (xi), we find that $\mathbb{D} \cong \bar{\mathbb{F}}_p[t]/(t^4)$ and we must have that the kernel of Frobenius is the submodule $(t^2)$. It follows that $\mathrm{Fr}^2 = 0$.

### 3.6 $K$ non-Galois

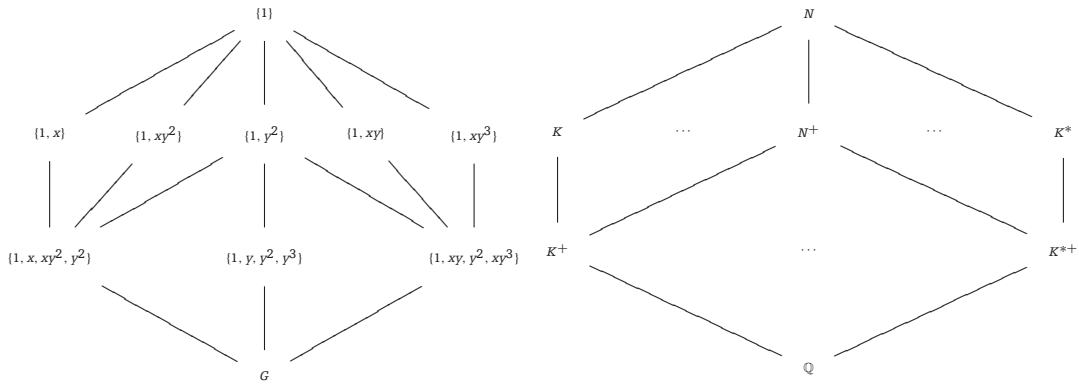
In this case, the normal closure of $K$ is a Galois extension $N/\mathbb{Q}$ of degree 8 and Galois group $D_4$. As above, we view $N$ as embedded in $\mathbb{C}$. $K$ is the fixed field of a noncentral involution we call $x$. Let $y$ be an element of order 4, then $y^2$ is the complex conjugation and $xyx = y^{-1} = y^3$. We identify $\mathrm{Hom}(K, \mathbb{C})$ with $\{1, y, y^2, y^3\}$ and the CM types are $\{1, y\}, \{y^2, y^3\}, \{1, y^3\}$, and $\{y, y^2\}$. We may twist the action of $K$ by complex conjugation and so assume that the CM type is $\{1, y\}$ or $\{1, y^3\}$. If it is $\{1, y^{-1}\}$ we can change the presentation of our group by using the generator $y^{-1}$ instead of $y$. We can therefore assume

**Table 5.** Reduction in the non Galois case

| | $I$ | $D$ | decomposition of $p$ in $N$ | decomposition of $p$ in $K$ | decomposition of $p$ in $K^+$ | decomposition of $p$ in $K^*$ | decomposition of $p$ in $K^{*+}$ | $N_{\Phi^*}(\mathfrak{p}_{K^*,1})$ | $a$ | $f$ | ssp? |
|---|---|---|---|---|---|---|---|---|---|---|---|
| i | $\{1\}$ | $\{1\}$ | $\prod_{\alpha\in G}\mathfrak{p}_{N,\alpha}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}\mathfrak{p}_{K,y^2}\mathfrak{p}_{K,y^3}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}\mathfrak{p}_{K^*,y^2}\mathfrak{p}_{K^*,y^3}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}$ | 0 | 2 | × |
| ii | $\{1\}$ | $\langle x\rangle$ | $\mathfrak{p}_{N,1}\mathfrak{p}_{N,y}\mathfrak{p}_{N,y^2}\mathfrak{p}_{N,y^3}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}\mathfrak{p}_{K,y^2}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y^2}$ | $\mathfrak{p}_{K^{*+},1}$ | $\mathfrak{p}^2_{K,1}\mathfrak{p}_{K,y}$ | 1 | 1 | × |
| iii | $\{1\}$ | $\langle xy\rangle$ | $\mathfrak{p}_{N,1}\mathfrak{p}_{N,y}\mathfrak{p}_{N,y^2}\mathfrak{p}_{N,y^3}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^2}$ | $\mathfrak{p}_{K^+,1}$ | $\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}\mathfrak{p}_{K^*,y^3}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $p$ | 2 | 0 | √ |
| iv | $\{1\}$ | $\langle xy^2\rangle$ | $\mathfrak{p}_{N,1}\mathfrak{p}_{N,y}\mathfrak{p}_{N,y^2}\mathfrak{p}_{N,y^3}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}\mathfrak{p}_{K,y^3}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}$ | $\mathfrak{p}_{K^{*+},1}$ | $\mathfrak{p}_{K,1}\mathfrak{p}^2_{K,y^3}$ | 1 | 1 | × |
| v | $\{1\}$ | $\langle xy^3\rangle$ | $\mathfrak{p}_{N,1}\mathfrak{p}_{N,y}\mathfrak{p}_{N,y^2}\mathfrak{p}_{N,y^3}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^2}$ | $\mathfrak{p}_{K^+,1}$ | $\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}\mathfrak{p}_{K^*,y^2}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $\mathfrak{p}^2_{K,1}$ | 0 | 2 | × |
| vi | $\{1\}$ | $\langle y^2\rangle$ | $\mathfrak{p}_{N,1}\mathfrak{p}_{N,x}\mathfrak{p}_{N,y}\mathfrak{p}_{N,xy}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}_{K^*,1}\mathfrak{p}_{K^*,y}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $p$ | 2 | 0 | √ |
| vii | $\{1\}$ | $\langle y\rangle$ | $\mathfrak{p}_{N,1}\mathfrak{p}_{N,x}$ | $\mathfrak{p}_{K,1}$ | $\mathfrak{p}_{K^+,1}$ | $\mathfrak{p}_{K^*,1}$ | $\mathfrak{p}_{K^{*+},1}$ | $p^2$ | 1 | 0 | × |
| viii | $\langle y^2\rangle$ | $\langle y^2\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,x}\mathfrak{p}^2_{N,y}\mathfrak{p}^2_{N,xy}$ | $\mathfrak{p}^2_{K,1}\mathfrak{p}^2_{K,y}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}^2_{K^*,1}\mathfrak{p}^2_{K^*,y}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$ | 2 | 0 | √ |
| ix | $\langle y^2\rangle$ | $\langle y\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,x}$ | $\mathfrak{p}^2_{K,1}$ | $\mathfrak{p}_{K^+,1}$ | $\mathfrak{p}^2_{K^*,1}$ | $\mathfrak{p}_{K^{*+},1}$ | $p$ | 2 | 0 | √ |
| x | $\langle y^2\rangle$ | $\langle x, y^2\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,y}$ | $\mathfrak{p}^2_{K,1}\mathfrak{p}^2_{K,y}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}^2_{K^*,1}$ | $\mathfrak{p}_{K^{*+},1}$ | $p$ | 2 | 0 | √ |
| xi | $\langle y^2\rangle$ | $\langle xy, y^2\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,y}$ | $\mathfrak{p}^2_{K,1}$ | $\mathfrak{p}_{K^+,1}$ | $\mathfrak{p}^2_{K^*,1}\mathfrak{p}^2_{K^*,y}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $p$ | 2 | 0 | √ |
| xii | $\langle x\rangle$ | $\langle x\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,y}\mathfrak{p}^2_{N,y^2}\mathfrak{p}^2_{N,y^3}$ | $\mathfrak{p}_{K,1}\mathfrak{p}^2_{K,y}\mathfrak{p}_{K,y^2}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}^2_{K^*,1}\mathfrak{p}^2_{K^*,y^2}$ | $\mathfrak{p}^2_{K^{*+},1}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$ | 1 | 1 | × |
| xiii | $\langle x\rangle$ | $\langle x, y^2\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,y}$ | $\mathfrak{p}_{K,1}\mathfrak{p}^2_{K,y}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}^2_{K^*,1}$ | $\mathfrak{p}^2_{K^{*+},1}$ | $p$ | 2 | 0 | √ |
| xiv | $\langle xy^2\rangle$ | $\langle xy^2\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,y}\mathfrak{p}^2_{N,y^2}\mathfrak{p}^2_{N,y^3}$ | $\mathfrak{p}^2_{K,1}\mathfrak{p}_{K,y}\mathfrak{p}_{K,y^3}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}^2_{K^*,1}\mathfrak{p}^2_{K^*,y}$ | $\mathfrak{p}^2_{K^{*+},1}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}$ | 1 | 1 | × |
| xv | $\langle xy^2\rangle$ | $\langle x, y^2\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,y}$ | $\mathfrak{p}^2_{K,1}\mathfrak{p}_{K,y}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}^2_{K^*,1}$ | $\mathfrak{p}^2_{K^{*+},1}$ | $p$ | 2 | 0 | √ |
| xvi | $\langle xy\rangle$ | $\langle xy\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,y}\mathfrak{p}^2_{N,y^2}\mathfrak{p}^2_{N,y^3}$ | $\mathfrak{p}^2_{K,1}\mathfrak{p}^2_{K,y^3}$ | $\mathfrak{p}^2_{K^+,1}$ | $\mathfrak{p}^2_{K^*,1}\mathfrak{p}_{K^*,y}\mathfrak{p}_{K^*,y^3}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}$ | 2 | 0 | √ |
| xvii | $\langle xy\rangle$ | $\langle xy, y^2\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,y}$ | $\mathfrak{p}^2_{K,1}$ | $\mathfrak{p}^2_{K^+,1}$ | $\mathfrak{p}^2_{K^*,1}\mathfrak{p}_{K*,y}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $p$ | 2 | 0 | √ |
| xviii | $\langle xy^3\rangle$ | $\langle xy^3\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,y}\mathfrak{p}^2_{N,y^2}\mathfrak{p}^2_{N,y^3}$ | $\mathfrak{p}^2_{K,1}\mathfrak{p}^2_{K,y}$ | $\mathfrak{p}^2_{K^+,1}$ | $\mathfrak{p}_{K^*,1}\mathfrak{p}^2_{K^*,y}\mathfrak{p}_{K^*,y^2}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $\mathfrak{p}^2_{K,1}$ | 0 | 2 | √ |
| xix | $\langle xy^3\rangle$ | $\langle xy, y^2\rangle$ | $\mathfrak{p}^2_{N,1}\mathfrak{p}^2_{N,y}$ | $\mathfrak{p}^2_{K,1}$ | $\mathfrak{p}^2_{K^+,1}$ | $\mathfrak{p}^2_{K^*,1}\mathfrak{p}_{K^*,y}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $p$ | 2 | 0 | √ |
| xx | $\langle y\rangle$ | $\langle y\rangle$ | $\mathfrak{p}^4_{N,1}\mathfrak{p}^4_{N,x}$ | $\mathfrak{p}^4_{K,1}$ | $\mathfrak{p}^2_{K^+,1}$ | $\mathfrak{p}^4_{K^*,1}$ | $\mathfrak{p}^2_{K^{*+},1}$ | $\mathfrak{p}^2_{K,1}$ | 2 | 0 | √ |
| xxi | $\langle y\rangle$ | $G$ | $\mathfrak{p}^4_{N,1}$ | $\mathfrak{p}^4_{K,1}$ | $\mathfrak{p}^2_{K^+,1}$ | $\mathfrak{p}^4_{K^*,1}$ | $\mathfrak{p}^2_{K^{*+},1}$ | $p$ | 2 | 0 | √ |
| xxii | $\langle x, y^2\rangle$ | $\langle x, y^2\rangle$ | $\mathfrak{p}^4_{N,1}\mathfrak{p}^4_{N,y}$ | $\mathfrak{p}^2_{K,1}\mathfrak{p}^2_{K,y}$ | $\mathfrak{p}_{K^+,1}\mathfrak{p}_{K^+,y}$ | $\mathfrak{p}^4_{K^*,1}$ | $\mathfrak{p}^2_{K^{*+},1}$ | $\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$ | 2 | 0 | √ |
| xxiii | $\langle x, y^2\rangle$ | $G$ | $\mathfrak{p}^4_{N,1}$ | $\mathfrak{p}^2_{K,1}$ | $\mathfrak{p}_{K^+,1}$ | $\mathfrak{p}^4_{K^*,1}$ | $\mathfrak{p}^2_{K^{*+},1}$ | $p$ | 2 | 0 | √ |
| xxiv | $\langle xy, y^2\rangle$ | $\langle xy, y^2\rangle$ | $\mathfrak{p}^4_{N,1}\mathfrak{p}^4_{N,y}$ | $\mathfrak{p}^4_{K,1}$ | $\mathfrak{p}^2_{K^+,1}$ | $\mathfrak{p}^2_{K^*,1}\mathfrak{p}^2_{K^*,y}$ | $\mathfrak{p}_{K^{*+},1}\mathfrak{p}_{K^{*+},y}$ | $\mathfrak{p}^2_{K,1}$ | 2 | 0 | √ |
| xxv | $\langle xy, y^2\rangle$ | $G$ | $\mathfrak{p}^4_{N,1}$ | $\mathfrak{p}^4_{K,1}$ | $\mathfrak{p}^2_{K^+,1}$ | $\mathfrak{p}^2_{K^*,1}$ | $\mathfrak{p}_{K^{*+},1}$ | $p$ | 2 | 0 | √ |
| xxvi | $G$ | $G$ | $\mathfrak{p}^4_{N,1}$ | $\mathfrak{p}^4_{K,1}$ | $\mathfrak{p}^2_{K^+,1}$ | $\mathfrak{p}^4_{K^*,1}$ | $\mathfrak{p}^2_{K^{*+},1}$ | $p$ | 2 | 0 | √ |

that $K$ is fixed by $x$, the Galois group is $\langle x, y | x^2, y^4, xyxy\rangle$ and the CM type is $\{1, y\}$. The reflex CM field $K^*$ is then fixed by $\{1, xy^3\}$ (follow the recipe in [33, Chapter 1, Theorem 5.1]) and the reflex CM type is $\{1, y^{-1}\}$.

We have the following diagrams of fields and subgroups:




The analysis of the reduction of $A$ proceeds along the same lines as above. Namely, one considers the decomposition of the Dieudonné module as a module over $\mathcal{O}_K \otimes \bar{\mathbb{F}}_p$ and the induced action of Frobenius, which is $1 \otimes \sigma$-linear, so to say. In most cases, this suffices to determine the $a$ and $f$ numbers, but in certain cases one needs to decide between two possibilities, and there the CM type matters. The interpretation of the CM type mod $p$ is done through the formalism of Section 3.1.

For example, referring to Table 5, in case (viii) we find that $\mathbb{D} \cong \bar{\mathbb{F}}_p[t]/(t^2) \oplus \bar{\mathbb{F}}_p[t]/(t^2)$ and Frobenius acts $\sigma$-$\bar{\mathbb{F}}_p[t]/(t^2)$ linearly (meaning, it acts $\sigma$-linearly on $\bar{\mathbb{F}}_p$ and commutes with $t$) on each component. The kernel, a priori could be one of the components or the submodule $(t) \oplus (t)$. Taking the CM type into consideration, we see that Frobenius has a kernel in each component and so its kernel is $(t) \oplus (t)$. It follows that $\mathrm{Fr}^2 = 0$. Case (x) is the same.

Case (ix) is easier as in this case $\mathbb{D} \cong \bar{\mathbb{F}}_p[t]/(t^2) \oplus \bar{\mathbb{F}}_p[t]/(t^2)$, where Fr is acting $\sigma$-$\bar{\mathbb{F}}_p$-linearly, but permutes the components. The kernel is either one of the components or the submodule $(t) \oplus (t)$ and, regardless, $\mathrm{Fr}^2 = 0$. Case (xi) is the same.

### 3.7 **Examples**

Take a curve $C$ of genus 2 over $\mathbb{Q}$ (to simplify). Given a prime $p$ at which $C$ has good reduction $\bar{C}$, one has a simple method of writing down the Hasse–Witt matrix $M$ of

$\bar{A} = \mathrm{Jac}(\bar{C})$ and so deciding the $a$-number and $f$-number of $\bar{A}$: the $f$-number is the rank of $M^{(p)}M$ and the $a$-number is the co-rank of $M$. In general, it is hard to decide the reduction type by examining $M$, but in certain cases we can do that and compare our results with the results above when $A = \mathrm{Jac}(C)$ has complex multiplication.

Let $C : y^2 = f(x)$, where $f(x) = x^5 + a_4x^4 + \cdots + a_0$, be a hyperelliptic curve and write $f(x)^{(p-1)/2} = \sum_{j\geq 0} c_j x^j$. Then the Hasse–Witt matrix $M$ is given by $\left(\begin{smallmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{smallmatrix}\right)$, and $M^{(p)}$ is $\left(\begin{smallmatrix} c_{p-1}^p & c_{p-2}^p \\ c_{2p-1}^p & c_{2p-2}^p \end{smallmatrix}\right)$. Exactly the same recipe works if $f(x)$ is a sextic. See [27, p. 129].

### 3.7.1 *Cases* (i), (ii), (iii) *and* (v) *in Table 3 for Galois cyclic fields*

**Example 3.2.** Let $C : y^2 = x^5 + 1$. The curve has good reduction outside $2 \cdot 5$. The Jacobian has complex multiplication by $\mathbb{Q}(\zeta_5)$ and the automorphism group of the curve in characteristic zero is $\mu_{10}$. The coefficient of $x^n$ in $f(x)^{(p-1)/2}$ is 0 if $5 \nmid n$ and is $\binom{(p-1)/2}{n/5}$ if $5|n$. We divide the analysis to several cases:

- If $p \equiv 1 \pmod 5$, then $M = \left(\begin{smallmatrix} \binom{(p-1)/2}{(p-1)/5} & 0 \\ 0 & \binom{(p-1)/2}{(2p-2)/5} \end{smallmatrix}\right)$ has rank 2 and we conclude that $\bar{A}$ is ordinary. Note that $p$ splits completely in this case. Namely we are in case (i) of the cyclic Galois case.
- If $p \equiv 2 \pmod 5$, $p > 2$, $M = \left(\begin{smallmatrix} 0 & \binom{(p-1)/2}{(p-2)/5} \\ 0 & 0 \end{smallmatrix}\right)$ has rank 1 and $M^{(p)}M = 0$. Thus, $f = 0$ and $a = 1$. This is supersingular, but not superspecial reduction, in accordance with case (iii).
- If $p \equiv 3 \pmod 5$, $M = \left(\begin{smallmatrix} 0 & 0 \\ \binom{(p-1)/2}{(2p-1)/5} & 0 \end{smallmatrix}\right)$ has rank 1 and $M^{(p)}M = 0$. Thus, $f = 0$ and $a = 1$. This is a supersingular, but not a superspecial reduction, in accordance with case (iii) again.
- If $p \equiv -1 \pmod 5$, $M = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ has rank 0 and we have superspecial reduction, in accordance with case (ii).
- $p = 5$. It follows from Igusa's classification of genus 2 curves with many automorphisms [28, Section 8] that the reduction of a stable model of $y^2 = x^5 + 1$ modulo 5 is isomorphic, possibly after base change, to the curve $y^2 = f(x)$, where $f(x) = x(x-1)(x+1)(x-2)(x+2)$. That is, since the characteristic is 5, $f(x) = x^5 - x$. Then $f(x)^2 = x^{10} - 2x^6 + x^2$ and the Hasse–Witt matrix is the zero matrix, giving us superspecial reduction. This agrees with case (v).
- In characteristic 2, Igusa's classification gives us the model $y^2 - y = x^5$. According to our table, since we are in case (iii), this curve should be supersingular, but not superspecial. The fact that the curve is supersingular, which in genus 2 is equivalent to $f = 0$, follows from the theory of Artin–Schreier

coverings, cf. [44, Lemma 2.6]. According to [27, Theorem 3.3] there are no superspecial nonsingular curves of genus 2 in characteristic 2. Therefore, we have supersingular and not superspecial reduction. □

### 3.7.2 *Cases* (v) *and* (vi) *of Table 3 for Galois cyclic fields*

**Example 3.3.** Consider the curve $y^2 = -8x^6 - 64x^5 + 1120x^4 + 4760x^3 - 48400x^2 + 22627x - 91839$, which has complex multiplication by the ring of integers of $K = \mathbb{Q}(\sqrt{-65 + 26\sqrt{5}})$ according to [54, 55]. The field is a cyclic Galois extension with a totally real field $K^+ = \mathbb{Q}(\sqrt{5})$. Its discriminant is $5^3 \cdot 13^2$. The prime 5 decomposes as $\mathfrak{p}_{K^+}^2 = \mathfrak{p}_K^4$ and belongs to case (vi), the prime 13 decomposes as $\mathfrak{q}_{K^+} = \mathfrak{q}_K^2$ and belongs to case (v). In any case, we have superspecial reduction. And, indeed, in both cases one finds that the Hasse–Witt matrix is identically zero modulo the corresponding prime. For example, for $p = 5$ we have $f(x)^2 = 64x^{12} + 1024x^{11} - 13824x^{10} - 219520x^9 + 1419520x^8 + 16495568x^7 - 87185232x^6 - 398328128x^5 + 2352249680x^4 - 3064600880x^3 + 9401996329x^2 - 4156082106x + 8434401921$ and the Hasse–Witt matrix is $\left(\begin{smallmatrix} 2352249680 & -3064600880 \\ -219520 & 1419520 \end{smallmatrix}\right) \equiv 0 \pmod 5$. □

Examples 3.4 and 3.5 also demonstrate cases (v) and (vi) in the table for Galois cyclic fields. For both, we take the Galois cyclic field $K = \mathbb{Q}[x]/(x^4 + 238x^2 + 833)$, with real quadratic subfield $\mathbb{Q}(\sqrt{17})$. It can be constructed by adjoining $\sqrt{-119 + 28\sqrt{17}}$ to $\mathbb{Q}$. The class number of $K$ is 2 and the field discriminant is $7^2 17^3$.

The three Igusa Class polynomials are as follows:

$$h_1(x) = x^2 + \frac{3^{16} \cdot 11 \cdot 163 \cdot 4801 \cdot t_1 \cdot t_2}{2^{23} \cdot 7^6 \cdot 43^{12} \cdot 179^{12}} x - \frac{3^{30} \cdot 62273^5 \cdot 173166943^5}{2^{22} \cdot 7^{12} \cdot 43^{12} \cdot 179^{12}},$$

$$h_2(x) = x^2 + \frac{3^{11} \cdot 5 \cdot 967 \cdot t_3}{2^9 \cdot 7^3 \cdot 43^8 \cdot 179^8} x - \frac{3^{22} \cdot 5^2 \cdot 19^2 \cdot 191 \cdot 62273^3 \cdot 173166943^3}{2^6 \cdot 7^8 \cdot 43^8 \cdot 179^8},$$

$$h_3(x) = x^2 + \frac{3^9 \cdot 1823 \cdot t_4}{2^{11} \cdot 7^3 \cdot 43^8 \cdot 179^8} x - \frac{3^{18} \cdot 359 \cdot 1667 \cdot 1811 \cdot t_5}{2^{10} \cdot 7^8 \cdot 43^8 \cdot 179^8},$$

where $t_1, \ldots, t_5$ are primes and $t_1 = 712465984819$, $t_2 = 152160175753014902257305649143422239021984895543$, $t_3 = 199763665249568296384949088855973069605073$, $t_4 = 819734099639522362577121888804614972466874 9$ and $t_5 = 228122997426508267522036684197215571753 7$.

**Example 3.4** (Case (v)). The prime 7 decomposes in $K$ as the square of an inert prime with inertia degree 2. Modulo 7 the class polynomials reduce badly, since 7 is in the denominator. The two CM curves each reduce to a product of elliptic curves with product polarization modulo 7, and the Galois action takes one curve to the other. Both have superspecial reduction. □

**Example 3.5** (Case (vi)). The prime 17 is totally ramified in $K$. Modulo 17 the reduction of the Igusa class polynomials is:

$$h_1(x) = (x+13)^2 \pmod{17}, \quad h_2(x) = (x+12)^2 \pmod{17}, \quad h_3(x) = (x+2)^2 \pmod{17}.$$

Taking the absolute Igusa invariants $[i_1, i_2, i_3] = [-13, -12, -2]$ modulo 17, we recover a 4-tuple of Igusa–Clebsch invariants $[A : B : C : D] = [1 : 14 : 8 : 13]$ via the formulas: $A = 1$, $D = A^5/i_1$, $B = i_2 \cdot D/A^3$, and $C = i_3 \cdot D/A^2$. Using Magma's implementation of Mestre's algorithm, we obtain a genus 2 curve $C : y^2 = x^6 + 16$ with these invariants over $\mathbb{F}_{17}$. Taking $f(x) = x^6 + 16 \pmod{17}$, we compute the $(p-1)/2 = 8^{\text{th}}$ power and compute the Hasse–Witt matrix. The only nonzero coefficients of $f$ are for terms whose degree is 0 (mod 6), so the Hasse–Witt Matrix is zero and the reduction is superspecial. □

### 3.7.3 *Cases* (xii), (xiv), (xvii) *and* (xix) *in Table 5 for non-Galois fields*

In Examples 3.6 and 3.7 we deal with cases (xii) and (xiv) (Example 3.7) and cases (xvii) and (xix) (Example 3.6) in the table for non-Galois fields. We work with a non-Galois quartic CM field, given by $K = \mathbb{Q}[x]/(x^4 + 134x^2 + 89)$ with reflex field given by $K^* = \mathbb{Q}[x]/(x^4 + 268x^2 + 17600)$. The class number of $K$ is 4 and the discriminant is $2^4 11^2 89$.

For typographical reasons, we list the class polynomials in modified form. To get the class polynomials $h_i(x)$ from the polynomials $h_i^*(x)$ listed below, divide by the leading coefficient in each case.

$$h_1^* = 46786168500827419831582500859570065480089664861245464225306306576334606367462143339253088925033807754516601562 5 \cdot x^8 + 55544914984551752820183085463077470228846020683654003234780668955704468066812106738036411695702554425224661827087402343750000 0 \cdot x^7 + 18403368676473300391621439332312$$

$$
\begin{aligned}
&1759307266571653588212097779374278645161702524660416788572844592879230\\
&4725110405869781970977783203125000000 \cdot x^6 - 1853252819671361096624873505\\
&9989496921744294218655209931046129134295796866360219594850246272816241\\
&0933211857453102565395344929130648498535156250000000000 \cdot x^5 - 1495176157\\
&7386221607707550178552613566439016379414477407296451553911287348517794\\
&6865799467841097175021951747554258225537368778725711443911431489057222\\
&3000000000000 \cdot x^4 - 2745002127877863203631749224519874186562888955642541\\
&6852671533372575037558556384959106460164764658831329000379776543259072\\
&6575728145151773922402693224283121273394262179840 \cdot, x^3 - 1297531069082446\\
&2049428048723892236585223008161239232354502537340424218996558059300177\\
&1951508989819214516847958284764562224480102456678890713123681109259524\\
&8135449429095219200000 \cdot x^2 + 7581619812043016425321000003017780983364056\\
&7679756337667150872417366816696541961643959188545195655300066960181143\\
&4342720043906982109112415240533721325054782428254517780807680000000000 \cdot\\
&x - 1665610762592188745243803916186278124592006299523777285406029610\\
&2410270027835247550412464024850182603102460369557884286225502239544621\\
&4265265991340473323825199368431179137024000000000000000
\end{aligned}
$$

$$
\begin{aligned}
h_2^* = {} & 1226209932245339908542669795721685899004071950912475585937500000 \cdot x^8\\
&+ 7485929269991071436519019319213472872675919432653818688502883911132812500000 \cdot x^7 + 1279115905734294297640612524226266479096350362335466486236041767631125823183776855468750000 \cdot x^6 - 4328014693023989701205639341434863079486256354344323252772261688698955439431510858034378897460937500 \cdot x^5 - 7098975722037134589753904078350700421024098996960488931189373791394\\
&1059181926255773255664903749716042965625 \cdot x^4 + 1412145839537492587461\\
&9003891297821593782870891378302331148263540097872948880292889091382293
\end{aligned}
$$

$$590512658722099151091 2 \cdot x^3 - 3247309744253473149174880508572156550385390$$
$$994944181119931887975608935788334464574063164679998777171297279904405 1$$
$$3280000 \cdot x^2 + 2878258800484146973496313274835799307245769049641717521354$$
$$166360884626643674126222273800205511215767305294130902374400000000 \cdot$$
$$x - 875776675051081603171574386294121650913389467088993679908740136586$$
$$915776656894551107952370791602333047060237323765990400000000000$$

$$h_3^* = 313909742654807016586923467704751590145042419433593750000000000000 \cdot x^8$$
$$+ 4933483238933925123221878822018364806571909097212211545662353515 62$$
$$500000000000 \cdot x^7 + 2168443965418989986038492688067403045710941961035989$$
$$372240912887706777245531152343750000000 \cdot x^6 - 2302525585957788818152082$$
$$352653829396337430793844914883168947610481921539535736987830563608984 3$$
$$75000 \cdot x^5 - 1523807620913740204347998372771177159741848758098650529755 61$$
$$585447684346918113356183254740900302324932628125 \cdot x^4 + 1012610953382711$$
$$904905306871718700690348631657961951220321310061019202268877697760125 1$$
$$774144342956667543232947 5648 \cdot x^3 - 8239423089006805080914763566055762368$$
$$562996561889322796612566681186008040742903064207777053844466019122791 0$$
$$486571712000 \cdot x^2 - 1926409131567661484196961498816000531174411060031335 2$$
$$222081307885719402039037153539661898189132747133562158783462400000 0 \cdot$$
$$x - 1870374669751414608923737345184889994628232369194056109733545677 63$$
$$841138329115928200250893082698796913156181577557721600000000 0$$

**Example 3.6** (cases (xvii), (xix))**.** The prime decomposition of 11 in $K$ is such that it is ramified in $K^+$ and the prime above it in $K^+$ is inert in $K$. Further, 11 is split in $K^{*+}$, and mixed in $K^*$ (one degree-one prime ideal with ramification index 2, and one unramified prime ideal of degree 2). The prime 11 appears in the denominator, so at least one of the curves with CM by $K$ is superspecial. □

**Remark.** One can strengthen the conclusion: In fact, all the curves are superspecial: although Table 5 assumes a fixed CM type,while the class polynomials do not, it is clear that changing the CM type would lead to a situation where $I$ is still generated by a noncentral involution and $D$ has 4 elements. These are cases (xiii), (xv), (xvii), and (xix) in the table, and in all of them we have superspecial reduction. □

**Example 3.7** (cases (xii) and (xiv))**.** The prime decomposition of 89 in $K$ is mixed: one ramified prime of degree 1 and two unramified primes of degree 1. It is split in $K^+$, ramified in $K^{*+}$, and that prime in $K^{*+}$ then splits in $K^*$. Modulo 89 the class polynomials factor as a product of the squares of two quadratic polynomials:

$$h_1 = (x^2 + 17x + 9)^2(x^2 + 18x + 25)^2 \pmod{89},$$

$$h_2 = (x^2 + 37x + 67)^2(x^2 + 69x + 57)^2 \pmod{89},$$

$$h_3 = (x^2 + 83x + 83)^2(x^2 + 85x + 45)^2 \pmod{89}.$$ □

Note that in this case, it is not obvious from the polynomials how to match up roots of the three polynomials to form triples of Igusa invariants. A common approach has been to use the knowledge of the CM field to determine the possible group orders of the Jacobian of the curve, and then to run through all triples of roots of these polynomials until the correct triples and the corresponding curves are found. In the case that the prime $p$ splits completely in the field $K$ (case (i) in Table 5), a method for determining the possible group orders was given in [12, Proposition 4; 57], and the resulting CM curves constructed there were indeed ordinary. For other decompositions of the prime $p$ in $K$, alternative algorithms are needed to compute the possible group orders. In the case of $p$-rank 1, a solution of the problem of calculating the group order was given in [25]. In some of the other examples, we show how to determine the group orders for other cases below.

The possible group orders in the case considered here (Example 3.7) are $\#J(C)(\mathbb{F}_{89^2}) = 62045284$ or 63439556, for a genus 2 curve $C$ over $\mathbb{F}_{89^2}$ with CM by $K$. This can be seen as follows: Let $p = 89$ then $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$. In this case, it can be verified using Magma or Pari that both of the ideals $\mathfrak{p}_1\mathfrak{p}_3$ and $\mathfrak{p}_2\mathfrak{p}_3$ are principal, generated by $\pi$ and $\bar{\pi}$, and $(\pi\bar{\pi}) = (p)$. Using methods similar to [25], we find the Weil $p^2$-numbers $\beta = \pm\pi\bar{\pi}^{-1}p$. Then the corresponding group orders for these Weil $p^2$-numbers are $N = \prod_\sigma(1 - \beta^\sigma)$, where $\sigma$ ranges over the complex embeddings of $K$.

Represent $\mathbb{F}_{89^2} = \mathbb{F}_{89}[\alpha]$, where $\alpha$ satisfies $\alpha^2 + 82\alpha + 3 = 0$. The four curves are

$$y^2 = f_1(x) = \alpha^{5245}x^6 + \alpha^{2244}x^5 + \alpha^{7129}x^4 + \alpha^{1567}x^3 + \alpha^{2060}x^2 + \alpha^{5783}x + \alpha^{3905},$$

$$y^2 = f_2(x) = \alpha^{2667}x^6 + \alpha^{795}x^5 + \alpha^{1956}x^4 + \alpha^{5619}x^3 + \alpha^{5331}x^2 + \alpha^{7272}x + 52,$$

$$y^2 = f_3(x) = \alpha^{6464}x^6 + \alpha^{795}x^5 + \alpha^{4574}x^4 + \alpha^{2946}x^3 + \alpha^{1544}x^2 + \alpha^{6684}x + \alpha^{803},$$

$$y^2 = f_4(x) = \alpha^{132}x^6 + \alpha^{3403}x^5 + \alpha^{2326}x^4 + \alpha^{3493}x^3 + \alpha^{5184}x^2 + \alpha^{1943}x + \alpha^{4418}.$$

Calculating the Hasse–Witt matrix for the first curve, one computes $f_1^{44}$ and finds $c_{88} = \alpha^{7555}$, $c_{87} = \alpha^{7787}$, $c_{177} = \alpha^{950}$, and $c_{176} = \alpha^{1182}$, and that both $M$ and $M^{(p)}M$ have rank 1, so both the $f$-number and the $a$-number equal 1. The same is true for the other three curves as well.

### 3.7.4 *Cases* (ii) *and* (iv) *in Table 5 for non-Galois fields*

We still refer to the field $K = \mathbb{Q}[x]/(x^4 + 134x^2 + 89)$ and the class polynomials given above.

**Example 3.8.** To give an example for cases (ii) and (iv) in Table 5 for non-Galois fields, we let $p = 313$. The prime $p = 313$ decomposes in $K$ as the product of two prime ideals of degree 1 and one prime ideal with residue degree 2. Modulo 313, the class polynomials factor as a product of four degree-2 polynomials:

$$h_1(x) = (x^2 + 25x + 273)(x^2 + 137x + 39)(x^2 + 200x + 108)(x^2 + 312x + 249) \pmod{313},$$

$$h_2(x) = (x^2 + 20x + 121)(x^2 + 90x + 119)(x^2 + 138x + 297)(x^2 + 173x + 78) \pmod{313},$$

$$h_3(x) = (x^2 + 105x + 276)(x^2 + 133x + 230)(x^2 + 232x + 183)(x^2 + 289x + 91) \pmod{313}.$$

The two possible group orders are $\#J(C)(\mathbb{F}_{89^2}) = 9607909136$ or $9588315136$, for a genus 2 curve $C$ over $\mathbb{F}_{313^2}$ with CM by $K$. This can be seen because both of the prime ideals of $K$ of degree 1 lying above $p$ are principal, and letting $\pi$ and $\bar{\pi}$ be the generators, we find the Weil $p^2$-numbers $\beta = \pm\pi\bar{\pi}^{-1}p$ (this is also explained in [25]). Then the corresponding group orders for these Weil $p^2$-numbers are $N = \prod_\sigma (1 - \beta^\sigma)$, where $\sigma$ ranges over the complex embeddings of $K$. Represent $\mathbb{F}_{313^2} = \mathbb{F}_{313}[\alpha]$, where $\alpha$ satisfies $\alpha^2 + 310\alpha + 10 = 0$. We find eight curves defined over $\mathbb{F}_{313^2}$. For example, the first one is the hyperelliptic

curve defined over $\mathbb{F}_{313^2}$ by

$$y^2 = f(x) = \alpha^{20046}x^6 + \alpha^{18815}x^5 + \alpha^{77496}x^4 + \alpha^{26504}x^3 + \alpha^{19266}x^2 + \alpha^{53721}x + \alpha^{1332}.$$

Calculating $f(x)^{156}$, one finds that the coefficients of the Hasse–Witt matrix $M$ are: $c_{p-1} = \alpha^{91834}$, $c_{p-2} = \alpha^{18900}$, $c_{2p-1} = \alpha^{62990}$, and $c_{2p-2} = \alpha^{88024}$. The determinant of both $M$ and $M^{(p)}M$ is 0 and the rank is 1. The same is true for all 8 curves: they all have $a = 1$ and $f = 1$. □

### 3.7.5 *Cases* (iii) *and* (v) *in Table 5 for non-Galois fields*

This next set of cases is very interesting, because we can see here that the decomposition of the prime in $K$ only determines the reduction of the abelian surface in combination with the CM type. This is our first example of both superspecial and ordinary reduction modulo the same prime (of CM abelian surfaces with CM by the same field $K$, but different CM type). This phenomenon does not occur in genus 1.

We again work with the primitive quartic CM field $K = \mathbb{Q}[x]/(x^4 + 134x^2 + 89)$ and the class polynomials given above. Let $p = 47$. As in cases (iii) and (v) in Table 5, the prime $p = 47$ decomposes in $K$ as a product of two prime ideals of degree 2: $p$ is inert in $K^+$, the real quadratic subfield of $K$, and then splits in $K$. The class polynomials factor modulo 47 as

$$h_1(x) = (x + 18)^2(x^2 + 22x + 12)(x^2 + 33x + 19)(x^2 + 37x + 6) \pmod{47},$$

$$h_2(x) = (x + 23)^2(x^2 + 10x + 46)(x^2 + 6x + 17)(x^2 + 9x + 39) \pmod{47},$$

$$h_3(x) = (x + 2)^2(x^2 + 42x + 26)(x^2 + x + 19)(x^2 + 27x + 7) \pmod{47}.$$

**Example 3.9** (case (v))**.** Both degree 2 prime ideals lying over $p = 47$ are principal in this case, and we denote the generators by $\pi$ and $\bar{\pi}$. In this case, $\pi\bar{\pi} = 47u$, where $u$ is a unit. Setting $\beta = \pm p^2/u$, gives two possible Weil $p^2$-numbers. Two possible group orders are $\#J(C)(\mathbb{F}_{47^2}) = \prod_\sigma (1 - \beta^\sigma) = 4901092$ or 4865732, where $\sigma$ ranges over the complex embeddings of $K$. There are four ordinary CM points corresponding to these possible group orders.

Represent $\mathbb{F}_{47^2} = \mathbb{F}_{47}[\alpha]$, where $\alpha$ satisfies $\alpha^2 + 45\alpha + 5 = 0$. Then the four curves with these group orders are:

$$y^2 = \alpha^{829}x^6 + \alpha^{1842}x^5 + \alpha^{622}x^4 + \alpha^{1262}x^3 + \alpha^{956}x^2 + \alpha^{398}x + \alpha^{1255},$$
$$y^2 = \alpha^{929}x^6 + \alpha^{1219}x^5 + \alpha^{1483}x^4 + \alpha^{1511}x^3 + \alpha^{251}x^2 + \alpha^{224}x + \alpha^{1437},$$
$$y^2 = \alpha^{1852}x^6 + \alpha^{2038}x^5 + \alpha^{1790}x^4 + \alpha^{1078}x^3 + \alpha^{1166}x^2 + \alpha^{1634}x + \alpha^{1518},$$
$$y^2 = \alpha^{1783}x^6 + \alpha^{892}x^5 + \alpha^{1454}x^4 + \alpha^{665}x^3 + \alpha^{1014}x^2 + \alpha^{871}x + \alpha^{1754}.$$

For all four curves, we checked that the Hasse–Witt matrix $M$ and $M^{(p)}M$ both have rank 2, so these curves are indeed all ordinary. □

**Example 3.10** (case (iii))**.** Each of the three class polynomials has one linear factor modulo 47. The curve over $\mathbb{F}_{47}$ with those $\mathbb{F}_{47}$-rational invariants is the hyperelliptic curve defined by

$$y^2 = 40x^6 + 22x^5 + 43x^4 + x^3 + 29x^2 + 8x + 28.$$

Its Jacobian has $\#J(C)(\mathbb{F}_{47}) = p^2 + 2p + 1 = 2304$ points and $\#C(\mathbb{F}_{47}) = p + 1 = 48$. The Hasse–Witt matrix $M$ is identically 0 modulo 47, so the curve is superspecial. This curve occurs "with multiplicity two" modulo 47. □

The other two CM abelian surfaces reduce to curves defined over $\mathbb{F}_{47^2}$. They are the hyperelliptic curves defined by

$$y^2 = \alpha^{487}x^6 + \alpha^{977}x^5 + \alpha^{1698}x^4 + \alpha^{1530}x^3 + \alpha^{1790}x^2 + \alpha^{1618}x + \alpha^{1063},$$
$$y^2 = \alpha^{809}x^6 + \alpha^{1759}x^5 + \alpha^{318}x^4 + \alpha^{1254}x^3 + \alpha^{226}x^2 + \alpha^{974}x + \alpha^{1385}.$$

They both have $\#J(C)(\mathbb{F}_{47^2}) = p^4 - 2p^2 + 1 = 4875264$ points and $\#C(\mathbb{F}_{47^2}) = p^2 + 1 = 2210$. They both have the property that the Hasse–Witt matrix $M$ is identically 0 modulo 47, so the curves are both superspecial.

In fact the referee pointed out that this is also a nice illustration of the computational utility of another aspect of our tables: the column which lists $N_{\Phi^*}(\mathfrak{p}_{K^*,1})$. If our starting point is the results in the table then, since $N_{\Phi^*}(\mathfrak{p}_{K^*,1}) = p$, in the first case we conclude that the Weil-numbers must be $\pm i\sqrt{p}$ and this predicts a group order of 48; in the second case, we have $p^2$-Weil numbers which would have to be $\pm ip$ and so the group order would have to be 2210.

### 3.7.6 *Case* (vii) *in Table 5 for non-Galois fields*

**Example 3.11.** We again work with the non-Galois quartic CM field $K = \mathbb{Q}[x]/(x^4 + 134x^2 + 89)$ and the class polynomials given above. The prime $p = 13$ is totally inert in $K$. Modulo 13, the class polynomials are:

$$h_1(x) = (x^2 + 2x + 9)(x^2 + 6x + 1)(x^4 + 8x^3 + 10x^2 + 12) \pmod{13},$$

$$h_2(x) = (x^2 + 5x + 1)(x^2 + 8x + 1)(x^4 + 7x^3 + 6x^2 + 7x + 8) \pmod{13},$$

$$h_3(x) = (x^2 + 2)(x^2 + 11)(x^4 + 6x^3 + 4x^2 + 5) \pmod{13}.$$

Among the curves whose invariants satisfy these $h_i \pmod{13}$, we look for curves over $\mathbb{F}_{13^2}$ with $\#J(C)(\mathbb{F}_{13^2}) = (p^4 + 2p^2 + 1) = 28900$. Such curves have Weil-numbers $\pm ip$ and so are supersingular. Represent $\mathbb{F}_{13^2} = \mathbb{F}_{13}[\alpha]$, where $\alpha$ satisfies $\alpha^2 + 12\alpha + 2 = 0$. We find four curves over $\mathbb{F}_{13^2}$, for example the first one is:

$$y^2 = \alpha^{99}x^6 + \alpha^{47}x^5 + \alpha^{156}x^4 + \alpha^{75}x^3 + \alpha^{27}x^2 + x + \alpha^{148}.$$

The invariants of this curve are $(i_1, i_2, i_3) = (-\alpha^{36}, -\alpha^{96}, -\alpha^{133})$. These invariants satisfy the polynomials $x^2 + 6x + 1$, $x^2 + 8x + 1$ and $x^2 + 2$, over $\mathbb{F}_{13}$, respectively. The curve's Hasse–Witt matrix $M$ has rank 1 and the rank of $M^{(p)}M$ is 0, so $a = 1$ and $f = 0$ as predicted in the tables. The same is true of the other three curves as well. We further remark that the four CM curves defined over $\mathbb{F}_{13^4}$ have Jacobian group order equal to either $(1 + p^2)^4$ or $(1 - p^2)^4$. All four curves have $a = 1$ and $f = 0$ as predicted. □

## 4 The Moduli Space of Pairs of Elliptic Curves

Let $n$ be a positive integer. Consider the functor $\mathbb{B}_n$ on schemes associating to a scheme $S$ the isomorphism class of triples

$$(E_1, E_2, \gamma),$$

where $\pi_i : E_i \to S, i = 1, 2,$ are elliptic curves over $S$ and $\gamma$ is a symplectic level structure on $E_1[n] \times E_2[n]$, namely, an isomorphism,

$$\gamma : E_1[n] \times E_2[n] \to (\mathbb{Z}/n\mathbb{Z})^4,$$

which is symplectic relative to the Weil pairing on $E_1 \times E_2$ (obtained as the product of the Weil pairings on each elliptic curve, or, equivalently, associated to the product polarization on $E_1 \times E_2$) and the pairing on $(\mathbb{Z}/n\mathbb{Z})^4$ given by the matrix $\begin{pmatrix} 0 & 1 & & \\ -1 & 0 & & \\ & & 0 & 1 \\ & & -1 & 0 \end{pmatrix}$.

An isomorphism $\varphi\colon (E_1, E_2, \gamma) \to (E_1', E_2', \gamma')$ of two such triples over $S$ is a pair of isomorphisms of $S$-group schemes, $\varphi_i : E_i \to E_i'$, such that $\gamma = \gamma' \circ (\varphi_1 \times \varphi_2)$.

The functor $\mathbb{B}_n$ is naturally equivalent to the functor parameterizing isomorphism classes of quadruples $(A, \lambda, e, \gamma)$ over $S$, where $(A, \lambda)$ is a principally polarized abelian surface over $S$, $e \in \mathrm{End}_S(A)$ is a nontrivial idempotent, fixed under the $\lambda$-Rosati involution, and $\gamma$ is a symplectic level $n$ structure. Indeed, given a triple $(E_1, E_2, \gamma)$ associate to it $(E_1 \times E_2, \lambda_1 \times \lambda_2, e, \gamma)$, where $\lambda_i$ are the canonical principal polarizations on $E_i$ and $e$ is the idempotent endomorphism $(x, y) \mapsto (x, 0)$. The converse construction associates to $A$ the triple $(E_1, E_2, \gamma)$, where $E_1 = \mathrm{Ker}(1 - e)$, $E_2 = \mathrm{Ker}(e)$. It is not hard to verify that these constructions give a natural equivalence between the functors.

**Lemma 4.1.** For $n \geq 3$ the moduli problem is rigid. Namely, any automorphism $\varphi$ of a triple $(E_1, E_2, \gamma)$ is the identity. □

**Proof.** Such an automorphism induces an automorphism of $(A, \lambda, \gamma)$, where $A = E_1 \times E_2$. It is well known that such an automorphism must be the identity. ■

It follows then from standard techniques that for $n \geq 3$ the functor $\mathbb{B}_n$ is representable by a quasi-projective scheme $\mathcal{B}_n$ over $\mathbb{Z}[\zeta_n, n^{-1}]$.

**Proposition 4.2.** Let $n \geq 2$. Let $J$ be the automorphism of $\mathcal{B}_n$ whose effect on points is

$$(E_1, E_2, \gamma) \mapsto (E_2, E_1, \gamma \circ s),$$

where $s$ is the natural "switch", $s : E_1[n] \times E_2[n] \to E_2[n] \times E_1[n]$. There is a geometric quotient $\mathcal{B}_n/\langle J \rangle$ for this action. We have a commutative diagram,

$$\begin{array}{ccc} \mathcal{B}_n & & \\ \downarrow & \searrow^{\beta} & \\ \mathcal{B}_n/\langle J \rangle & \xrightarrow{\beta_J} & \mathcal{A}_{2,n} \end{array}$$

where the diagonal arrow $\beta$ is the natural morphism $(E_1, E_2, \gamma) \mapsto (E_1 \times E_2, \lambda_1 \times \lambda_2, \gamma)$, the vertical arrow is an étale Galois cover with Galois group $\mathbb{Z}/2\mathbb{Z}$ and the bottom arrow $\beta_J$ is a closed immersion, induced by $\beta$, whose image is the Humbert surface $\bar{\mathcal{H}}_{1,n}$ in $\mathcal{A}_{2,n}$, the Zariski closure in $\mathcal{A}_{2,n}$ of $\mathcal{H}_{1,n} \subset \mathcal{A}_{2,n}(\mathbb{C})$. □

**Proof.** The existence of the quotient follows immediately from [40, Theorem, p. 66] and the remark following that theorem. We first show that the morphism $\mathcal{B}_n \to \mathcal{B}_n/\langle J \rangle$ is unramified. Suppose that $J(E_1, E_2, \gamma) = (E_2, E_1, \gamma \circ s)$ is isomorphic to $(E_1, E_2, \gamma)$. There are then isomorphisms $\varphi_1 : E_2 \to E_1$, $\varphi_2 : E_1 \to E_2$ such that $\gamma \circ s = \gamma \circ (\varphi_1 \times \varphi_2)$ and so $s = \varphi_1 \times \varphi_2$ on $E_1[n] \times E_2[n]$. But, for $(a, b) \in E_1[n] \times E_2[n]$ we have $s(a, b) = (b, a)$, while $\varphi_1 \times \varphi_2(a, b) = (\varphi_1(a), \varphi_2(b))$, which obviously cannot hold for every pair $(a, b)$ if $n \geq 2$.

The morphism $\mathcal{B}_n \to \mathcal{B}_n/\langle J \rangle$, being a quotient by a finite group, is a finite morphism. We conclude that it is a finite étale cover with Galois group $\mathbb{Z}/2\mathbb{Z}$. The natural morphism $\beta : \mathcal{B}_n \to \mathcal{A}_{2,n}$ clearly factors through $\mathcal{B}_n/\langle J \rangle$ and we denote the induced morphism

$$\beta_J : \mathcal{B}_n/\langle J \rangle \to \mathcal{A}_{2,n}.$$

We claim that this is a geometrically injective morphism. Suppose that

$$(E_1 \times E_2, \lambda_1 \times \lambda_2, \gamma) \cong (E_1' \times E_2', \lambda_1' \times \lambda_2', \gamma').$$

By a theorem of Weil [56], after possibly switching $E_1'$ with $E_2'$, we may assume that $E_1 \cong E_1'$, $E_2 \cong E_2'$ and therefore, under these identifications, that $\gamma = \gamma'$. Namely, up to applying $J$, every point in the image has a unique pre-image.

The morphism $\beta_J$ is also proper. This follows from the valuative criterion of properness. As we shall see below, the scheme $\mathcal{B}_n$ is a union of products of modular curves, in particular, it is noetherian and so we can use discrete valuation rings in the criterion. To apply it, we must show that if $R$ is a discrete valuation ring with field of fractions $K$, $(A, \lambda, \gamma)/R$ is an abelian scheme whose generic fiber is isomorphic over $K$ to $(E_1 \times E_2, \lambda_1 \times \lambda_2, \gamma)$ then the elliptic curves $E_i$ extend to elliptic curves over $R$ and then so does the isomorphism. The fact that the elliptic curves extend follows from the theory of Néron models (since $E_1 \times E_2 = A \otimes_R K$ obviously has good reduction). The extension of the isomorphism follows from the fact that $\mathcal{A}_{2,n}$ has a toroidal compactification, which is proper over $\mathbb{Z}[\zeta_n, n^{-1}]$. Since both $\mathcal{B}_n/\langle J \rangle$ and $\mathcal{A}_{2,n}$ are reduced and the morphism $\beta_J$ is proper and injective (hence quasi-finite), $\beta_J$ is a finite injective morphism. We will conclude that it is an isomorphism onto its image, the Humbert surface $\bar{\mathcal{H}}_{1,n}$ by showing

that for a geometric point $x$ of $\mathcal{B}_n/\langle J\rangle$ and its image $y$ in $\mathcal{A}_{2,n}$ the completed local rings are isomorphic. Note that the Humbert divisor $\bar{\mathcal{H}}_{1,n}$ is the image of $\beta_J$, since they have the same generic fiber and both are the closure of their generic fiber.

Indeed, suppose that $y$ is the image of the $k$-geometric point $(y_1, y_2)$ of $\mathcal{B}_n$. The completed local ring on $\mathcal{B}_n$ is then just isomorphic to $W(k)[\![t_1, t_2]\!]$, as $\mathcal{B}_n$ is a product of smooth curves. Moreover, if $E_i$ is the elliptic curve corresponding to $y_i$, then $t_i$ is the parameter arising via the local deformation theory for elliptic curves (the level structure need not be a product level structure; regardless it extend uniquely by étaleness). On the other hand, the completed local ring on $\mathcal{A}_{2,n}$ of the point $y$ corresponding to $(A, \lambda, \gamma) = (E_1 \times E_2, \lambda_1 \times \lambda_2, \gamma)$ is isomorphic to the ring $W(k)[\![t_{11}, t_{1,2}, t_{2,1}, t_{2,2}]\!]/(t_{1,2} - t_{2,1})$ and $\bar{\mathcal{H}}_{1,n}$ contains locally the closed formal subscheme defined by the ideal $(t_{1,2}, t_{2,1})$, as is clear from the interpretation of the variables through local deformation theory. Since $\mathcal{B}_n/\langle J\rangle$ is locally irreducible and the morphism is geometrically injective also $\bar{\mathcal{H}}_{1,n}$ is locally irreducible. It follows that $\bar{\mathcal{H}}_{1,n}$ is defined locally by the ideal $(t_{1,2}, t_{2,1})$ and that the morphism is an isomorphism on every completed local ring, which is sufficient to conclude the proof.

Another way to conclude the proof is to prove that the morphism $\beta_J$ is universally injective (or a monomorphism) and then use EGA IV, Section 8.11, Proposition (8.11.5). Since $\mathcal{B}_n/\langle J\rangle$ is the categorical quotient of $\mathcal{B}_n$, we know it as a functor of points and so injectivity boils down to the following statement: Given elliptic curves $E_1, \ldots, E_4$ over a connected scheme $S$ such that $E_1 \times E_2 \cong E_3 \times E_4$ as principally polarized abelian schemes over $S$ then, either $E_1 \cong E_3$ and $E_2 \cong E_4$, or $E_1 \cong E_4$ and $E_2 \cong E_3$. Note that to identify $E_1$ in $E_3 \times E_4$ is equivalent to giving an endomorphism. Choose a geometric point $x$ of $S$ and use Weil's theorem as above together with Grothendieck's theorem $\mathrm{End}_S(E_3 \times E_4) \hookrightarrow \mathrm{End}_{k(x)}((E_3 \times E_4) \otimes k(x))$. ■

We next discuss the complex uniformization of $\mathcal{B}_n$. Recall the classical construction of the modular curves: Given $\tau \in \mathfrak{H}$ one lets $E_\tau = \mathbb{C}/\langle 1, \tau\rangle$ be the corresponding elliptic curve, and we get a symplectic isomorphism $E_\tau[n] \to (\mathbb{Z}/n\mathbb{Z})^2$ by sending $1/n$ to ${}^t(1, 0)$ and $\tau/n$ to ${}^t(0, 1)$. We call this level structure $\gamma_0$. Let $\sigma = M\tau$, where $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then the isomorphism $E_\sigma \to E_\tau$ is given by multiplication by $j(M, \tau) = c\tau + d$. Since $\gamma_0(A + B\sigma)/n = {}^t(A, B)$ and $1/n$ is sent to $(d + c\tau)/n$, while $\sigma/n$ is sent $(b + a\tau)/n$, we find that $(E_\sigma, \gamma_0)$ is isomorphic to $(E_\tau, \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right) \circ \gamma_0)$. We remark that $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto {}^\dagger M := \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right)$ is an outer automorphism of $\mathrm{SL}_2(\mathbb{Z})$ given by conjugating by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{Z})$. We conclude that

$$(E_\tau, \gamma_0) \cong (E_{M\tau}, {}^\dagger M^{-1} \circ \gamma_0).$$

Consider the space

$$\mathfrak{H} \times \mathfrak{H} \times \mathrm{Sp}_4(\mathbb{Z}/n\mathbb{Z}).$$

(The symplectic group is relative to the pairing fixed at the beginning of this section.) To a point $(\tau_1, \tau_2, \gamma)$ of this space we associate the triple $(E_{\tau_1}, E_{\tau_2}, \gamma \circ (\gamma_0 \times \gamma_0))$. The group $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ acts on the space by

$$(M_1, M_2) * (\tau_1, \tau_2, \gamma) = (M_1\tau_1, M_2\tau_2, \gamma \circ \mathrm{diag}({}^{\dagger}{M_1}^{-1}, {}^{\dagger}{M_2}^{-1})).$$

The space of orbits is isomorphic to $\mathcal{B}_n(\mathbb{C})$. Furthermore, choose a complete set of representatives $\gamma_1, \ldots, \gamma_t$ $(t = t(n))$ for $\mathrm{Sp}_4(\mathbb{Z}/n\mathbb{Z})/(\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}))$. Then,

$$\mathcal{B}_n(\mathbb{C}) \cong \coprod_{i=1}^{t} (\Gamma(n)\backslash\mathfrak{H})^2 = \coprod_{i=1}^{t} Y(n) \times Y(n).$$

Via this identification, we associate to a pair $(\tau_1, \tau_2)$ in the $i$th (or $\gamma_i$th, if one prefers) component of $\mathcal{B}_n(\mathbb{C})$ the triple $(E_{\tau_1}, E_{\tau_2}, \gamma_i \circ (\gamma_0 \times \gamma_0))$.

The involution $J$ takes the $\gamma_i$-component to $\gamma_j$-component where $\gamma_j$ is determined by $\gamma_i \circ (\gamma_0 \times \gamma_0) \circ s \in (\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))\gamma_j \circ (\gamma_0 \times \gamma_0)$. We always have $\gamma_j \neq \gamma_i$; that is, $J$ acts on the set of components as an involution with no fixed points. In fact, the components of $\mathcal{B}_n$ are parameterized by $\mathrm{Sp}_4(\mathbb{Z}/n\mathbb{Z})/(\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}))$, while the components of $\mathcal{B}_n/\langle J\rangle$ are parameterized by $\mathrm{Sp}_4(\mathbb{Z}/n\mathbb{Z})/[(\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}))H]$, where $H = \{1, \left(\begin{smallmatrix} 0 & I_2 \\ I_2 & 0 \end{smallmatrix}\right)\}$. One has $(\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}))H = H(\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}))$ and $(\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}))H \cong (\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})) \rtimes H$.

## 5 A Lemma in Arithmetic Intersection Theory

Let $R$ be a Dedekind ring, finite over $\mathbb{Z}_p$, $\mathfrak{p} \lhd R$ a prime ideal. Let $\pi : S \to \mathrm{Spec}(R)$ be a smooth scheme of finite type over $\mathrm{Spec}(R)$. Let $x \in S$ be a closed point of characteristic $p$ lying over $\mathfrak{p}$. Then $\mathcal{O}_S^{\wedge x}$, the completed local ring at $S$ is isomorphic to $\tilde{R}[\![x_1, \ldots, x_n]\!]$ where $n$ is the relative dimension of $S$ over $R$ and $\tilde{R} = R \otimes_{R_0} W(R/\mathfrak{p})$, where $R_0$ the maximal unramified subring of $R$. See Cohen [8]. In particular, $\mathcal{O}_S^{\wedge x}$ is a noetherian unique factorization domain. As a consequence, every divisor on $\mathrm{Spf}(\mathcal{O}_S^{\wedge x})$ is principal, a fact used in the following lemma. (We remark that in fact this latter fact follows directly from the Auslander–Buchsbaum theorem without need for Cohen's theorem.)

**Lemma 5.1.** Let $S \to \mathrm{Spec}(R)$ be a smooth integral scheme of finite type over a Dedekind ring $R$ containing $\mathbb{Z}$. Let $B$ be a Dedekind ring containing $R$, $K$ its field of fractions and $\eta$ the generic point of $\mathrm{Spec}(B)$. Let

$$\iota : \mathrm{Spec}(B) \to S,$$

be a morphism of schemes over $R$. Let $f$ be a rational function on $S$ such that the divisor of $f$ intersects the image of $\iota$ properly (in particular, $f(\iota(\eta)) = \iota^* f$ is a well-defined element of $K$; we shall abuse notation and write simply $f(\eta)$). Let the divisor of $f$ equal $(f)_0 - (f)_\infty = \sum m_i D_i$, where the $m_i$ are nonzero integers and $D_i$ irreducible reduced effective divisors. Let $Z$ be the closed reduced subscheme that is the support of $(f)_0$.

Let $\mathfrak{p}$ be a nonzero prime ideal of $B$ and $x$ its image under $\iota$. Suppose that $\mathrm{val}_{\mathfrak{p}}(f(\eta)) = \alpha > 0$. Then $d = \max\{m_i : x \in D_i\} > 0$. Let $a = \lceil \alpha/d \rceil$. Then $a > 0$ and the morphism $\iota : \mathrm{Spec}(B/\mathfrak{p}^a)$ factors through $Z$:

$$\begin{array}{ccccc} \mathrm{Spec}(B/\mathfrak{p}^a) & \longrightarrow & \mathrm{Spec}(B) & \xrightarrow{\iota} & S \\ & \searrow & & & \uparrow \\ & & & & Z \end{array} \tag{5.1}$$

□

**Remark.** We shall apply this lemma later, in the following context: $S$ will be the modular scheme $\mathcal{A}_{2,n}$, $f$ will be a function such that $f = \Theta^k/g$, where $g$ is a modular form of weight $10k$ with rational Fourier coefficients, the morphism $\iota$ will be such that $\iota(\eta)$ is a CM point and our assumption will be that $\mathrm{val}_{\mathfrak{p}}(f(\eta)) = \alpha > 0$. □

**Proof.** We first argue that we may replace $S$ by $\mathrm{Spf}(\mathcal{O}_S^{\wedge x})$. Indeed, on the one hand, if the dashed arrow in diagram (5.1) exists then, by passing to completions at $x$, we get a diagram

$$\begin{array}{ccc} \mathrm{Spec}(B/\mathfrak{p}^a) & \longrightarrow & \mathrm{Spf}(\mathcal{O}_S^{\wedge x}) \\ & \searrow & \uparrow \\ & & Z \cap \mathrm{Spf}(\mathcal{O}_S^{\wedge x}) \end{array} \tag{5.2}$$

On the other hand, diagram (5.2), if true, is coming from unique continuous morphisms $\mathcal{O}_S^{\wedge x} \to B/\mathfrak{p}^a$ etc., that arise from morphisms $\mathcal{O}_S \to B/\mathfrak{p}^a$, etc. Hence, it is enough to show that diagram (5.2) holds.

In $\mathrm{Spf}(\mathcal{O}_S^{\wedge x})$ every divisor is principal and so we may write there $D_i' = (f_i)$ where $f_i \in \mathcal{O}_S^{\wedge x}$, and $D_i'$ is the induced divisor on $\mathrm{Spf}(\mathcal{O}_S^{\wedge x})$. $D_i'$ may be reducible, but it is reduced. If $x \notin D_i$, then $f_i$ is a unit in $\mathcal{O}_S^{\wedge x}$. Via the morphism $\mathrm{Spec}(B_\mathfrak{p}) \to \mathrm{Spec}(B) \to S$, which induces a morphism $\mathrm{Spec}(B_\mathfrak{p}) \to \mathrm{Spf}(\mathcal{O}_S^{\wedge x})$, we may view $f(\eta)$ as an element of $K_\mathfrak{p}$, which is equal, up to a unit, to $\prod_i f_i(x)^{m_i}$ and so:

$$\begin{aligned}\alpha = \mathrm{val}_\mathfrak{p}(f(\eta)) &= \sum_{\{i:x\in D_i\}} m_i \cdot \mathrm{val}_\mathfrak{p}(f_i(\eta)) \\ &= \sum_{\{i:x\in D_i, m_i>0\}} m_i \cdot \mathrm{val}_\mathfrak{p}(f_i(\eta)) + \sum_{\{i:x\in D_i, m_i<0\}} m_i \cdot \mathrm{val}_\mathfrak{p}(f_i(\eta)). \end{aligned} \tag{5.3}$$

We note that if $x \in D_i$ then $\mathrm{val}_\mathfrak{p}(f_i) \geq 1$ (it may be strictly bigger, of course). In particular, $d > 0$. Consider $\alpha' = \sum_{\{i:x\in D_i, m_i>0\}} \mathrm{val}_\mathfrak{p}(f_i(\eta))$; clearly $\alpha' \cdot d \geq \alpha$ and so $\alpha' \geq \lceil \alpha/d \rceil$ and so it will be enough to prove that diagram (5.2) holds with $\alpha'$. Consider the function $f_Z = \prod_{\{i:x\in D_i, m_i>0\}} f_i$ which defines $Z \cap \mathrm{Spf}(\mathcal{O}_S^{\wedge x})$. To show diagram (5.2) holds is equivalent to proving that $f_Z$, when pulled back to $\mathrm{Spec}(B_\mathfrak{p})$ has valuation at least $\alpha'$. But the valuation is precisely $\sum_{\{i:x\in D_i, m_i>0\}} \mathrm{val}_\mathfrak{p}(f_i(\eta))$ and we are done. ■

### 5.1 Examples

The whole theory is developed precisely to deal with situations where one cannot just "write down everything explicitly", and so our examples are a bit artificial.

- Consider the scheme $S = \mathrm{Spec}(\mathbb{Z}[y])$ and the function $f(y) = y^2 - 1$. The divisor of $f$ is
$$D_1 + D_2, \quad D_1 = \mathrm{div}(y-1), \quad D_2 = \mathrm{div}(y+1).$$
Let $x = 3$ corresponding to the point determined by the homomorphism $\mathbb{Z}[y] \to \mathbb{Z}$, $y \mapsto 3$. We have $\mathrm{val}_2(f(x)) = \mathrm{val}_2(8) = 3$. We examine the situation on the completed local ring of the point $(2, y-3) = (2, y-1) = (2, y+1)$ (the reduction of $x$ modulo 2). Also at this completed local ring the divisor of $f$ is given by $D_1 = \mathrm{div}(y-1)$, $D_2 = \mathrm{div}(y+1)$ (with a slight abuse of notation). It follows from our lemma that the morphism $\mathrm{Spec}(\mathbb{Z}) \to \mathrm{Spec}(\mathbb{Z}[y])$ corresponding to $x$ induces a morphism
$$\mathrm{Spec}(\mathbb{Z}/2^3\mathbb{Z}) \to D_1 \cup D_2,$$
where by $D_1 \cup D_2$ we mean the closed reduced subscheme whose support is $D_1 \cup D_2$, namely $\mathrm{Spec}(\mathbb{Z}[y]/(y^2-1))$. Indeed, this is nothing but saying that there is indeed a well defined homomorphism $\mathbb{Z}[y]/(y^2-1) \to \mathbb{Z}/2^3\mathbb{Z}$ taking $y$ to 3.

An interesting feature of this example is that the morphism $\mathrm{Spec}(\mathbb{Z}) \to \mathrm{Spec}(\mathbb{Z}[y])$ only induces a well-defined morphism $\mathrm{Spec}(\mathbb{Z}/2^i\mathbb{Z}) \to D_i$ (where $D_i$ is the reduced closed scheme supported on $D_i$, namely $\mathrm{Spec}(\mathbb{Z}[y]/(y-1))$ for $i=1$ and $\mathrm{Spec}(\mathbb{Z}[y]/(y+1))$ for $i=2$). Moreover, the divisors $D_1$ and $D_2$ intersect transversely, the intersection being $(y-1, y+1)$. The subtlety is in the scheme structure on $D_1 \cup D_2$ and in particular in the fact that $\mathbb{Z}[y]/(y^2-1) \subsetneq \mathbb{Z}[y]/(y-1) \times \mathbb{Z}[y]/(y+1)$.

- Once more $S = \mathrm{Spec}(\mathbb{Z}[y])$ but now $f(y) = y^2+1$, which is irreducible. The point $x=2$ corresponds to the homomorphism $\mathbb{Z}[y] \to \mathbb{Z}$, $y \mapsto 2$. We have $\mathrm{val}_5(f(x)) = \mathrm{val}_5(5) = 1$. We have an induced morphism $\mathrm{Spec}(\mathbb{Z}/5\mathbb{Z}) \to \mathrm{Spec}(\mathbb{Z}[y]/(y^2+1))$, which amount to the fact that there is a homomorphism $\mathbb{Z}[y]/(y^2+1) \to \mathbb{Z}/5\mathbb{Z}$ taking $y$ to 2.

  In the completed local ring of the point $(5, y-2)$ the function $f$ decomposes as $f(y) = (y-i)(y+i)$ where $i$ is an element of $\mathbb{Z}_5$ whose square is $-1$ and whose reduction is 2 modulo 5. Thus, the function $y-i$ vanishes to first order at this point, while the function $y+i$ is a unit. The divisor of $f$ is locally $D_1 = \mathrm{div}(y+i)$ and the lemma, or, rather, its proof, states that we have an induced morphism $\mathrm{Spec}(\mathbb{Z}/5\mathbb{Z}) \to \mathrm{Spf}(\mathbb{Z}_5[\![(y-2)]\!]/(y-i))$, which amounts to the fact that there is a well-defined continuous homomorphism $\mathbb{Z}_5[\![(y-2)]\!]/(y-i) \to \mathbb{Z}/5\mathbb{Z}$ taking $y$ to 2.

## 6 A Problem in Deformation Theory

### 6.1 Deforming endomorphisms

Let $A$ be an abelian variety of dimension $g$ over a perfect field $k$ of characteristic $p$ and let $r$ be the rank over $\mathbb{Z}$ of $\mathrm{End}_k(A)$ (it is finite and at most $4g^2$). Let $(R, \mathfrak{m}_R)$ be a local artinian ring with residue field $k = R/\mathfrak{m}_R$ of characteristic $p$. Let $n_R$ be the minimal positive integer such that $\mathfrak{m}_R^{n_R} = 0$. Let $t_R$ be the least positive integer such that $p^{t_R} \in \mathfrak{m}_R^{p-1}$.

Let $\mathbb{A}/R$ be a deformation of $A$. By that we mean that $\mathbb{A} \to \mathrm{Spec}(R)$ is an abelian scheme and that there are given closed immersions:

$$\begin{array}{ccc} \mathbb{A} & \hookleftarrow & A \\ \downarrow & & \downarrow \\ \mathrm{Spec}(R) & \hookleftarrow & \mathrm{Spec}(k) \end{array}$$

By a fundamental result of Grothendieck, we have an inclusion of rings

$$\mathrm{End}_R(\mathbb{A}) \hookrightarrow \mathrm{End}_k(A).$$

Let us define the magnitudes (a priori possibly infinite)

$$i(\mathbb{A}/R) = [\mathrm{End}_k(A) : \mathrm{End}_R(\mathbb{A})]$$

(the index of $\mathrm{End}_R(\mathbb{A})$ in $\mathrm{End}_k(A)$), and

$$\mathfrak{i}(R) = \inf\{i(\mathbb{A}/R) : \mathbb{A}/R \text{ a deformation of } A\}, \tag{6.1}$$

$$\mathfrak{I}(R) = \sup\{i(\mathbb{A}/R) : \mathbb{A}/R \text{ a deformation of } A\}. \tag{6.2}$$

These depend on $A$ but we suppress that from the notation. We are interested in studying $i(\mathbb{A}/R)$, $\mathfrak{i}(R)$ and $\mathfrak{I}(R)$. Although we provide below some general results, our focus later is on the case of elliptic curves. The general case certainly deserves further study, but it will not be carried out here. The proof of the following proposition is given Section 6.3, after we review Grothendieck's crystalline deformation theory.

**Proposition 6.1.** The quantity $i(\mathbb{A}/R)$ is finite and is a power of $p$. So are $\mathfrak{i}(R)$ and $\mathfrak{I}(R)$. The following inequalities hold:

$$1 \le \mathfrak{i}(R) \le \mathfrak{I}(R) \le p^{(r-1)t_R\lceil (n_R-1)/(p-1)\rceil}. \qquad \square$$

**Corollary 6.2.** Let $K$ be a CM field and $\mathcal{O}'$ an order of $K$. Let $A \to \mathrm{Spec}(R)$ be an abelian scheme over a d.v.r. $(R, \mathfrak{m}_R)$ whose residue field is a perfect field $k$ of characteristic $p$, and suppose that we are given an optimal embedding $\iota : \mathcal{O}' \hookrightarrow \mathrm{End}_R(A)$, that is, $\iota(K) \cap \mathrm{End}_R(A) = \mathcal{O}'$. Let $\mathcal{O} \supseteq \mathcal{O}'$ be the optimally embedded order of $K$ in $\mathrm{End}_k(A \otimes k)$. Then $[\mathcal{O} : \mathcal{O}']$ is a power of $p$. $\square$

**Proof.** Let $\mathbb{A}_n = A \pmod{\mathfrak{m}_R^n}$ and $R_n = R/\mathfrak{m}_R^n$. We have

$$\mathcal{O}' = \bigcap_n \iota(K) \cap \mathrm{End}_{R_n}(\mathbb{A}_n).$$

Thus, $[\mathcal{O} : \mathcal{O}'] = \inf_n\{[\mathcal{O} : \iota(K) \cap \mathrm{End}_{R_n}(\mathbb{A}_n)]\}$, which must be equal to $[\mathcal{O} : \iota(K) \cap \mathrm{End}_{R_{n_0}}(\mathbb{A}_{n_0})]$ for any sufficiently large $n_0$. Since $[\mathcal{O} : \iota(K) \cap \mathrm{End}_{R_{n_0}}(\mathbb{A}_{n_0})]$ divides $[\mathrm{End}_{R_1}(A_1) : \mathrm{End}_{R_{n_0}}(\mathbb{A}_{n_0})]$, it is a power of $p$. ■

**Example 6.3** (of Corollary 6.2)**.** Suppose that $E$ is an elliptic curve over a number field $M$ with complex multiplication by an optimally embedded order $\mathcal{O}'$ of a quadratic imaginary field $K$. Let $\mathfrak{p}$ be a prime ideal of $M$ of residue characteristic $p$, and assume that $E$ has good reduction modulo $\mathfrak{p}$, denoted $E'$, and that the conductor of $\mathcal{O}'$ is prime to $p$. Then $\mathcal{O}'$ is optimally embedded in $\mathrm{End}(E')$.

On the other hand, the conductor always becomes smaller when it is divisible by $p$. Suppose that $E$ has supersingular reduction, $\mathcal{O}_K = \mathbb{Z}[\delta]$ and $\mathcal{O}' = \mathbb{Z}[pr\delta]$, where $r \in \mathbb{Z}$. One verifies that $pr\delta$ has degree divisible by $p^2$. Since $E'$ is supersingular any isogeny of degree $p^2$ vanishes on $E'[p]$ and it follows that $r\delta$ is also an isogeny of $E'$. It is an interesting situation. Because $\mathcal{O}'$ is optimally embedded in $\mathrm{End}(E)$, the kernel of the multiplication-by-$p$ map on the finite flat group scheme $\mathrm{Ker}[pr\delta]$ has order $p$ generically, but order $p^2$ modulo $p$. This example is well known but is usually proved by other techniques. See, for example [34, Theorem 5, Section 13.2]. □

**Proposition 6.4.** Let $A$ be an abelian variety over an algebraically closed field $k$ of characteristic $p$.

1. Let $\mathcal{O} \subset \mathrm{End}(A)$ be a set. Let $R^u$ be the universal formal deformation space of $A$. There is closed subscheme $Z_{\mathcal{O}}$ which is universal for the property of extending $\mathcal{O}$ to a deformation.
2. Let $n$ be an integer. There is a closed subscheme of $R^u$ that is universal for deformations $\mathbb{A}$ of $A$ such that $[\mathrm{End}(A) : \mathrm{End}(\mathbb{A})] | p^n$. (The same holds true if we wish to work with elementary divisors for the quotient abelian group $\mathrm{End}(A)/\mathrm{End}(\mathbb{A})$.) □

Proposition 6.4 is folklore. The first assertion is proved in [11, Lemma 4.3.5]. The proof consists of verifying Schlessinger's criteria for pro-representability. The second assertion follows immediately from the first given that there are only finitely many subrings of a given index (let alone of given elementary divisors) and they are all finitely generated as $\mathbb{Z}$-modules.

### 6.2 Crystalline deformation theory

Our main reference here is Grothendieck's monograph [23]. First recall the notion of *divided powers structure* (*d.p.*) on a pair $(R, I)$ consisting of a ring $R$ and an ideal $I \lhd R$ [23, Chapitre IV, Section 1.1]. This is a sequence of functions $\gamma_n : I \to I$, $n = 1, 2, 3, \ldots$ that

"behave like" $x^n/n!$, $n=1,2,3,\ldots$, that is, the following properties hold true:

1. $\gamma_1(x)=x$;
2. $\gamma_n(x+y)=\gamma_n(x)+\sum_{i=1}^{n-1}\gamma_{n-i}(x)\gamma_i(y)+\gamma_n(y)$;
3. $\gamma_n(xy)=x^n\gamma_n(y)$ for $x\in R$, $y\in I$;
4. $\gamma_m(\gamma_n(x))=\frac{(mn)!}{(n!)^m m!}\gamma_{mn}(x)$;
5. $\gamma_m(x)\gamma_n(x)=\frac{(m+n)!}{m!n!}\gamma_{m+n}(x)$.

The axioms imply the identities

$$x^n=n!\gamma_n(x),\quad x\in I,\quad n=1,2,3\ldots.$$

Hence, if $R$ is an integral domain, whose quotient field is of characteristic 0, there is at most one d.p. structure on $I$. It is given by $\gamma_n(x)=x^n/n!$. This d.p. structure is well defined if $x^n/n!\in I$ for all $x\in I$, $n=1,2,3,\ldots$. A d.p. structure is called *nilpotent* if there is an $N$, such that for any positive integers $a_1,\ldots,a_r$ with $\sum_{i=1}^r a_i\geq N$ and elements $x_1,\ldots,x_r$ of $I$, we have $\gamma_{a_1}(x_1)\gamma_{a_2}(x_2)\cdots\gamma_{a_r}(x_r)=0$. Note that $I$ itself is then nilpotent.

**Example 6.5.** Let $p$ be a prime. Suppose that $I^p=0$ and that $1,2,3,\ldots p-1$ are invertible in $R$, then we may define $\gamma_n(x)=x^n/n!$, $n=1,2,\ldots,p-1$ and $\gamma_n(x)=0$, $n\geq p$. This is a nilpotent d.p. structure with $N=p$. □

**Example 6.6.** Let $(R,I)$ be a discrete valuation ring of mixed characteristic $(0,p)$ and uniformizer $\pi$. Normalize the valuation so that $\mathrm{val}(p)=1$ and $\mathrm{val}(\pi)=1/e$. We have $\pi^n/n!\in I$ if and only if $n/e\geq(n-s_n)/(p-1)$, where $s_n$ is the sum of the digits in the $p$-adic development of $n$. See [23, Chapter IV, Section 1.3.] That is, $\pi^n/n!\in I$ for all $n\geq 1$ iff $e\leq p-1$.

If $R$ has a d.p. structure, that is, $e\leq p-1$, then we have an induced d.p. structure on $(R/I^N, I/I^N)$, which is nilpotent of level $N$ if $e<p-1$, and say then that the d.p. structure on $(R,I)$ is topologically nilpotent. The condition $e<p-1$ is necessary for that. □

The theorem that we need is in [23, Chapter V, Section 4]. Following the notation there, we use $\mathbb{D}^*(A)_S$ to denote the relative de Rham cohomology $\mathbb{H}^1_{\mathrm{dR}}(A/S)$. It will take us too long to define the notions of the crystalline site and crystals in general. For that see [23]. We just note a particular example of that theorem: Let $S\hookrightarrow S'$ be a closed immersion of affine schemes, $\mathrm{Spec}(R)\to\mathrm{Spec}(R')$, where $R'\to R$ is a surjective ring homomorphism with kernel $I$ that is nilpotent. This is called a "nilpotent thickening of $S$ by $S'$. We will

be interested in the case where $I$ is equipped with nilpotent d.p. If we globalize this situation, then we arrive at the assumption of the following theorem.

**Theorem 6.7.** Let $S$ be a scheme and $S'$ nilpotent thickening of $S$ with d.p. which is locally nilpotent. Consider the natural functor from abelian schemes over $S'$ to the category of couples $(A, \mathrm{Fil}^1)$ of an abelian scheme $A$ over $S$ and a submodule, locally a direct summand, $\mathrm{Fil}^1$ of $\mathbb{D}^*(A)_{S'}$, which is a prolongation of $\mathrm{Fil}^1\mathbb{D}^*(A)_S = \underline{\omega}_A$. This functor is an equivalence of categories. □

**Example 6.8.** Let $K$ be a quadratic imaginary field and $\mathcal{O}_{K,m}$ be the order of conductor $m$ in $K$ and say $p^a \| m$, $m = p^a n$. Let $E$ be a superspecial elliptic curve over $\bar{\mathbb{F}}_p$ with an action of $\mathcal{O}_{K,n}$. One may wish to calculate the deformations of $E$ to which the action of the subring $\mathcal{O}_{K,m}$ of $\mathcal{O}_{K,n}$ extends. (Note that this is the general situation by Example 6.3.) Unfortunately, such a calculation is not accessible via crystalline deformation theory. For example, consider such deformations to characteristic zero that are defined over a d.v.r. $R$ with d.p. Every such deformation $\mathbb{E}$ defines then a submodule of $H^1_{\mathrm{crys}}(E/R) = H^1_{\mathrm{crys}}(E/W(\bar{\mathbb{F}}_p)) \otimes R$, which is a direct summand of rank 1 extending the Hodge–de Rham filtration on $H^1_{\mathrm{dR}}(E/\bar{\mathbb{F}}_p)$. We assume such a deformation exists, which means that there are two embeddings $\iota_1, \iota_2 : \mathcal{O}_{K,n} \to R$, the first induced from the action of $\mathcal{O}_{K,n}$ on the tangent space and the second is its Galois twist. We have $H^1_{crys}(E/R) = \mathcal{O}_{K,n} \otimes_{\mathbb{Z}} R \hookrightarrow R \oplus R$ by $(\iota_1 \otimes 1, \iota_2 \otimes 1)$. If $p \neq 2$ is unramified, then this is an isomorphism of rings and under this isomorphism the order of conductor $m$ is sent to the subring $\mathcal{O}_a := \{(x, y) \in R \oplus R : x \equiv y \pmod{p^a}\}$, generated as an $R$-module by $(1, 1)$, $(p^a, -p^a)$. A direct summand $R$-module of rank 1 of $R^2$ is given by $(x, y)$ with either $x$ or $y$ a unit. To be preserved under $\mathcal{O}_a$ we must have $x = 0$ or $y = 0$. Thus, we see that there is a unique deformation for which the action of $\mathcal{O}_a$ extends, and then also $\mathcal{O}_0$ acts. The conclusion is that elliptic curves over a finite extension of $\mathbb{Q}_p$ on which $\mathcal{O}_{K,m}$ acts optimally are not defined over a base affording d.p. That is, the ramification index is at least $p$. Of course, the theory of complex multiplication and class field theory give more precise results. It remains an interesting problem to actually calculate the closed subscheme of the deformation space of $E$ to which the action of $\mathcal{O}_{K,m}$ extends. □

### 6.3 Proof of Proposition 6.1

We remark that there are many cases where $\mathfrak{i}(R) = 1$. An obvious example is when $R = k[\epsilon]$ and we take the constant deformation $\mathbb{A} = A \otimes_k k[\epsilon]$. Interesting examples can be given in the case of ordinary abelian varieties using Serre–Tate local parameters [32].

Let $(R, \mathfrak{m}_R)$ be a local artinian ring with residue field $k = R/\mathfrak{m}_R$. Let $n_R$ be the minimal positive integer such that $\mathfrak{m}_R^{n_R} = 0$, as before. We define successively rings

$$R_0 = R/\mathfrak{m}_R, \quad R_1 = R/\mathfrak{m}_R^{1+(p-1)}, \quad R_2 = R/\mathfrak{m}_R^{1+2(p-1)}, \ldots, R_\ell = R/\mathfrak{m}_R^{1+\ell(p-1)},$$

where $\ell = \lceil (n_R - 1)/(p-1) \rceil$. There are canonical surjections

$$R_\ell \twoheadrightarrow R_{\ell-1} \twoheadrightarrow \cdots \twoheadrightarrow R_1 \twoheadrightarrow R_0,$$

and we let $I_j = \mathfrak{m}_R^{1+(j-1)(p-1)}/\mathfrak{m}_R^{1+j(p-1)}$, $j = 1, 2, \ldots, \ell$, be the kernel of the surjection $R_j \to R_{j-1}$. We note that $I_j^p = 0$ in $R_j$ and hence the morphism

$$\mathrm{Spec}(R_{j-1}) \hookrightarrow \mathrm{Spec}(R_j),$$

is a nil-immersion with canonical d.p. structure as in Example 6.5. Let $t_R$ be the minimal power of $p$ such that $p^{t_R} \in \mathfrak{m}_R^{p-1}$. Then $p^{t_R} I_j = 0$ in $R_j$.

Now, by arguing inductively on $j$, we reduce to the following situation. Let $A \to \mathrm{Spec}(R_{j-1})$ be an abelian scheme of relative dimension $g$ and let $\mathbb{A} \to \mathrm{Spec}(R_j)$ a deformation of it. We need to show that $[\mathrm{End}(\mathbb{A}) : \mathrm{End}(A)]$ is finite and is equal to a power of $p$. By Theorem 6.7, the closed immersion of abelian schemes $A \hookrightarrow \mathbb{A}$ corresponds functorially to a diagram

$$\begin{array}{ccc} R_j^{2g} & \twoheadrightarrow & R_{j-1}^{2g} = \mathbb{H}^1_{\mathrm{dR}}(A/R_{j-1}) \\ \cup & & \cup \\ \omega_j & \twoheadrightarrow & \omega_{j-1} = H^0(A, \Omega^1_{A/R_{j-1}}) \end{array}$$

where $\omega_{j-1}, \omega_j$ are free $R$-modules that are rank $g$ direct summands of $R_{j-1}^{2g}$ and $R_j^{2g}$, respectively. In particular, an endomorphism $f \in \mathrm{End}(A)$ acts canonically and compatibly on $R_{j-1}^{2g}$ and $R_j^{2g}$ and preserves $\omega_{j-1}$. It extends to an endomorphism of $\mathbb{A}$ if and only if it preserves $\omega_j$. Consider then $p^{t_R} f$. Let $x \in \omega_j$ and choose a $y \in \omega_j$ such that $f(x) = y \pmod{I_j}$, that is, equality holds between the images of $f(x)$ and $y$ in $\omega_{j-1}$. Then $f(x) - y$ is in the kernel of the homomorphism $\omega_j \to \omega_{j-1}$, which is certainly contained in $I_j R_j^{2g}$. Since $p^{t_R} I_j = 0$, we conclude that $p^{t_R} f(x) - p^{t_R} y = 0$ and so $p^{t_R} f(x) \in \omega_j$.

We note that the same reasoning gives that if $s \cdot f$ extends to an endomorphism of $\mathbb{A}$ and $(p, s) = 1$ then $f$ also extends, because $s$ is invertible in $R$. This can also be concluded from the Serre–Tate theory [32] that gives $\mathrm{End}(\mathbb{A}) = \{f \in \mathrm{End}(\mathbb{A}[p^\infty]) : f|_{A[p^\infty]} = g|_{A[p^\infty]}$ for some $g \in \mathrm{End}(A)\}$, namely, the endomorphisms of $\mathbb{A}$ are the endomorphisms of its $p$-divisible group whose restriction to the $p$-divisible group of $A$ is induced from a bona fide endomorphism of $A$.

We have $r - 1$ appearing in the power of $p$ in the statement of the proposition, namely there is "a saving of 1", because $\mathbb{Z} \subseteq \mathrm{End}(\mathbb{A})$ and is a direct summand in it (as an abelian group). This concludes the proof of Proposition 6.1.

### 6.4 Supersingular elliptic curves

Let $k = \bar{\mathbb{F}}_p$. Let $V$ be a complete d.v.r. containing the completion of the maximal unramified extension $W(k)$ of $\mathbb{Z}_p$ and of ramification index $e_V < p - 1$. Then $V \to k$ has topologically nilpotent d.p.'s coming from $\gamma_n(x) = x^n/n!$ in $V$. In fact, using results of Zink (see [61, remarks on p. 6]), it is enough to assume that $e_V \leq p - 1$ and so that $V$ has d.p. structure (not necessarily nilpotent). The advantage is that $p = 2$ is allowed too, as long as it is unramified.

Let $E/k$ be a supersingular elliptic curve. Recall that $\mathrm{End}(E)$ is a maximal order in the rational quaternion algebra $B_{p,\infty}$ ramified only at $p$ and $\infty$. We apply Grothendieck's crystalline deformation theory to study for a deformation $\mathbb{E}/R$ of $E$ the index $[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})]$.

**Lemma 6.9.** The following holds:

1. $[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})] = [\mathrm{End}(E) \otimes \mathbb{Z}_p : \mathrm{End}(\mathbb{E}) \otimes \mathbb{Z}_p]$.
2. $\mathrm{End}(E) \otimes \mathbb{Z}_p \cong \left\{ \left( \begin{smallmatrix} a & b \\ pb^\sigma & a^\sigma \end{smallmatrix} \right) : a, b \in W(\mathbb{F}_{p^2}) \right\} =: D$, where $\sigma$ is the Frobenius automorphism.
3. There is a basis $\{e_1, e_2\}$ of $H^1_{\mathrm{crys}}(E/W(k))$ with respect to which the action of $\mathrm{End}(E)$ is given as matrices as in the above point 2. □

**Proof.** The first claim holds, because by Proposition 6.1 the index is a power of $p$. To prove the rest, we note that $E$ can be defined over $\mathbb{F}_{p^2}$ and so $H^1_{\mathrm{crys}}(E/W(k))$ has a basis $e_1$ and $e_2$ defined over $\mathbb{F}_{p^2}$ such that the $\sigma$-linear Frobenius map is given by the matrix $\left( \begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix} \right)$ with respect to this basis. Now, we have $\mathrm{End}(E) \otimes \mathbb{Z}_p \cong \mathrm{End}(E[p^\infty])$ (this uses Tate's theorem at $p$ plus the fact that the Galois action, being in the commutant of the quaternion algebra $\mathrm{End}^0(E)$ is central), which is in turn isomorphic to the endomorphisms of

$H^1_{\mathrm{crys}}(E/W(k))$ commuting with $\left(\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right)$. The condition then comes out

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

that is,

$$\begin{pmatrix} pb & a \\ pd & c \end{pmatrix} = \begin{pmatrix} c^\sigma & d^\sigma \\ pa^\sigma & pb^\sigma \end{pmatrix},$$

from which now both (2) and (3) follow. ■

**Proposition 6.10.** In the basis $\{e_1, e_2\}$ the Hodge filtration on $H^1_{\mathrm{dR}}(E/k)$ is given by the image of the span of $e_1$ in $H^1_{\mathrm{crys}}(E/W(k))$.

Let $n$ be a positive integer. Any deformation $\mathbb{E}$ of $E$ to $R := V/\mathfrak{m}_V^n$, equipped with its canonical d.p.'s structure, is given by the span of a vector in $R^2 = H^1_{\mathrm{dR}}(E/R)$ of the form $(1, y)$ with $y \in \mathfrak{m}_R$ and so we denote it $\mathbb{E}_y$. In particular, an element $\left(\begin{smallmatrix} a & b \\ pb^\sigma & a^\sigma \end{smallmatrix}\right)$ in $\mathrm{End}(E) \otimes \mathbb{Z}_p$ extends to the deformation $\mathbb{E}_y$ if and only if

$$\begin{pmatrix} a & b \\ pb^\sigma & a^\sigma \end{pmatrix}\begin{pmatrix} 1 \\ y \end{pmatrix} \in \mathrm{Span}_R\left\langle \begin{pmatrix} 1 \\ y \end{pmatrix} \right\rangle.$$ □

(The proof is straightforward.)

**Theorem 6.11.** Let $V$ be as in Proposition 6.10. Then

$$p^{2(\lceil n/e_V \rceil - 1)} \le \mathfrak{i}(V/\mathfrak{m}_V^n) \le \mathfrak{I}(V/\mathfrak{m}_V^n) \le p^{3(n-1)}.$$

Furthermore, these bounds are optimal. □

**Proof.** Let $R = V/\mathfrak{m}_V^n$ and $D_Y = \left\{\left(\begin{smallmatrix} a & b \\ pb^\sigma & a^\sigma \end{smallmatrix}\right) : a, b \in W(\mathbb{F}_{p^2}), by^2 + (a - a^\sigma)y - pb^\sigma \equiv 0 \pmod{\mathfrak{m}_V^n}\right\}$. Note that

$$\begin{pmatrix} a & b \\ pb^\sigma & a^\sigma \end{pmatrix}\begin{pmatrix} 1 \\ y \end{pmatrix} \in \mathrm{Span}_R\left\langle \begin{pmatrix} 1 \\ y \end{pmatrix} \right\rangle \Leftrightarrow by^2 + (a - a^\sigma)y - pb^\sigma \equiv 0 \pmod{\mathfrak{m}_V^n},$$

and so $D_y$ is a ring, identified with $\mathrm{End}(\mathbb{E}_y) \otimes \mathbb{Z}_p$ by Proposition 6.10. We note that the map

$$\varphi : D \to R, \quad \begin{pmatrix} a & b \\ pb^\sigma & a^\sigma \end{pmatrix} \mapsto by^2 + (a - a^\sigma)y - pb^\sigma,$$

is a $\mathbb{Z}_p$-linear map whose kernel is $D_y$. We shall give a lower bound on $[D : D_y]$ by bounding $\sharp D/D_y = \sharp\varphi(D)$ from below.

Suppose that $p \neq 2$. Let $\{1, \alpha\}$ be a $\mathbb{Z}_p$-basis of $W(\mathbb{F}_{p^2})$ such that $\alpha^\sigma = -\alpha$ and $\alpha$ is a unit. We normalize the $p$-adic valuation so that $\mathrm{val}(p) = 1$. If $A, B \in \mathbb{Z}_p$ then $\mathrm{val}(A + B\alpha) = \mathrm{val}(A - B\alpha) = \min\{\mathrm{val}(A), \mathrm{val}(B)\}$. We note that

$$\varphi(D) = \mathrm{Span}_{\mathbb{Z}_p}\{y^2 - p, \alpha(y^2 + p), \alpha y\}.$$

Consider the linear combination

$$C(A, B) = A(y^2 - p) + B\alpha(y^2 + p), \quad A, B \in \mathbb{Z}_p.$$

We note that

$$\mathrm{val}(C(A, B)) < \gamma := \frac{n}{e_v} \Longrightarrow C(A, B) \neq 0 \quad \text{in } R = V/\mathfrak{m}_V^n.$$

Let $y$ denote also some lift of $y \in R$ to $V$. We distinguish cases:

1. $\mathrm{val}(y) > 1/2$. We write

$$C(A, B) = y^2(A + B\alpha) - p(A - B\alpha).$$

Since $\mathrm{val}(A + B\alpha) = \mathrm{val}(A - B\alpha)$ and $\mathrm{val}(y^2) > 1$, we find that

$$\mathrm{val}(C(A, B)) = 1 + \min\{\mathrm{val}(A), \mathrm{val}(B)\}.$$

It follows that as long as either $\mathrm{val}(A)$ or $\mathrm{val}(B)$ are less than $\gamma - 1$, or, equivalently, are less than $\lceil\gamma\rceil - 1$, we have $C(A, B) \neq 0 \pmod{\mathfrak{m}_V^n}$. Equivalently, the group homomorphism

$$\mathbb{Z}/p^{\lceil\gamma\rceil-1} \times \mathbb{Z}/p^{\lceil\gamma\rceil-1} \longrightarrow R, \quad (A, B) \mapsto C(A, B),$$

is injective. We conclude that $\sharp\varphi(D) \geq p^{2(\lceil\gamma\rceil-1)}$.

2. $\mathrm{val}(y) < 1/2$. In this case, $\mathrm{val}(y^2) < 1$ and so we find that $\mathrm{val}(C(A,B)) = \mathrm{val}(y^2) + \min\{\mathrm{val}(A), \mathrm{val}(B)\} < 1 + \min\{\mathrm{val}(A), \mathrm{val}(B)\}$ and we get the same estimate (we do not bother with improving it).
3. $\mathrm{val}(y) = 1/2$. In this case, we note that either $\mathrm{val}(y^2 - p) = 1$ or $\mathrm{val}(y^2 + p) = 1$. So, either $\mathrm{val}(y^2 - p) = 1$ or $\mathrm{val}(\alpha(y^2 + p)) = 1$. We assume that $\mathrm{val}(y^2 - p) = 1$, as the other case is entirely similar. In this case, we consider the linear combination

$$D(A,B) = A(y^2 - p) + B\alpha y, \quad A, B \in \mathbb{Z}_p.$$

Since $\mathrm{val}(A(y^2 - p)) = \mathrm{val}(A) + 1$ and $\mathrm{val}(B\alpha y) = \mathrm{val}(B) + 1/2$ and, in particular, are never equal, we find that

$$\mathrm{val}(D(A,B)) = \min\{1 + \mathrm{val}(A), 1/2 + \mathrm{val}(B)\},$$

and, as long as $\mathrm{val}(A) < \gamma - 1$ or $\mathrm{val}(B) < \gamma - 1/2$, $D(A,B) \neq 0 \in R$. Weakening the conclusion to $\mathrm{val}(A) < \gamma - 1$ and $\mathrm{val}(B) < \gamma - 1$, we find the previous estimate.

Next consider the case $p = 2$. Represent $W(\mathbb{F}_{p^2})$ as $W(\mathbb{F}_p)[t]$ with $t^2 + t - 1 = 0$. A key point turns out to be that $\alpha = t - t^\sigma$ is a unit, and for $A, B \in \mathbb{Z}_p$ we have

$$\mathrm{val}(A + Bt) = \mathrm{val}(A + Bt^\sigma) = \min\{\mathrm{val}(A), \mathrm{val}(B)\}.$$

One checks that

$$\varphi(D) = \mathrm{Span}_{\mathbb{Z}_p}\{y^2 - p, ty^2 - pt^\sigma, \alpha y\}.$$

We let now

$$C(A,B) = A(y^2 - p) + B(ty^2 - pt^\sigma), \quad D(A,B) = A(y^2 - p) + B\alpha y, \quad A, B \in \mathbb{Z}_p.$$

As before the analysis is divided into three cases: (i) $\mathrm{val}(y) > 1/2$, (ii) $\mathrm{val}(y) > 1/2$ and $\mathrm{val}(y) = 1/2$, which are treated in an entirely similar manner. In cases (i) and (ii) it is helpful to write $C(A,B) = y^2(A + Bt) - p(A + Bt^\sigma)$ and in case (iii) first one argues that we cannot have both $\mathrm{val}(y^2 - p) > 1$ and $\mathrm{val}(ty^2 - pt^\sigma) > 1$; assuming without loss of generality that $\mathrm{val}(y^2 - p) = 1$, one uses $D(A,B)$ for the estimate, as before.

The upper bound on $\mathfrak{I}(V/\mathfrak{m}_V^n)$ follows using the same technique as in the proof of Proposition 6.1, which itself gives a slightly weaker exponent $(3 \cdot \lceil \frac{p-1}{e_V} \rceil \cdot \lceil \frac{n-1}{p-1} \rceil)$.

We now show that the bounds in Theorem 6.11 are optimal.

Let $E$ be a supersingular elliptic curve over $\bar{\mathbb{F}}_p$ with an action of the ring of integers $\mathcal{O}_K$ of a quadratic imaginary field $K$. The prime $p$ is either inert or ramified in $K$. Let $K_{\mathfrak{p}}$ denote the completion of $K$ at the prime $\mathfrak{p}$ above $p$. Let $V$ be the valuation ring of $W(\bar{\mathbb{F}}_p) \otimes_{W(\mathcal{O}_K/\mathfrak{p})} K_{\mathfrak{p}}$. Gross [22] studies the deformations of $E$ to which the action of $\mathcal{O}_K$ extends. He obtains that the endomorphism ring of such a deformation over $V/(\mathfrak{m}_V^{e_V n}) = V/(p^n)$ is precisely $\mathcal{O}_K + p^{n-1}\mathrm{End}_{\bar{\mathbb{F}}_p}(E)$ and, in particular, of index $p^{2(n-1)}$ in $\mathrm{End}(E)$. This shows that our lower bound for $\mathfrak{i}(V/\mathfrak{m}_V^n)$ is the best possible.

A concrete case of a deformation where index $p^{2(n-1)}$ is achieved is the case when $V = W(\mathbb{F}_{p^2})$, $y = p > 2$, $n = 2$ and $e_V = 1$. Note that in that case the target of the map $\varphi$ is $W(\mathbb{F}_{p^2})/(p^2)$, which has cardinality $p^4$. It is also easily verified that $\varphi(D)$ is generated in this case over $\mathbb{Z}_p/(p^2)$ by $p$ and $\alpha p$ and so has cardinality $p^2$. We conclude that $D_y$ has index $p^2$. In fact, $D_y$ are the matrices in $D$ defined by the condition $a - a^\sigma = b^\sigma \pmod{p}$. Thus, $D_y$ contains $pD$ and modulo $pD$ it is given by the basis $(a, b) = (1, 0)$ and $(a, b) = (\alpha, -2\alpha^\sigma)$. If we take any quadratic imaginary field $K = \mathbb{Q}(\sqrt{-d})$ ($d$ square-free integer) in which $p$ is inert and let $\alpha = \sqrt{-d}$ then we find one of the deformations considered by Gross for $K$. This finishes the discussion of the lower bound.

Now consider the case of a $(V, \mathfrak{m}_V)$, which is unramified over $\mathbb{Q}_p$, where $p > 2$, and $V$ satisties some additional conditions stipulated below. Let $y \in \mathfrak{m}_V$ be an element with valuation 1, such that $y \notin W(\mathbb{F}_{p^2})$, and such that $\mathrm{val}(y - y') = 1$ for every Galois conjugate $y' \neq y$ of $y$ over $\mathbb{Q}_p$. For example, $y$ could be $p\zeta$ where $\zeta$ is an $\ell$th root of unity where $\ell \neq p$ is a large enough prime. The ring $V$ must be large enough to contain such an element $y$, and that is the only condition put on it.

For such a choice of $y$, suppose that there are $A, B, C \in \mathbb{Z}_p$ such that

$$A(y^2 - p) + B\alpha(y^2 + p) + C\alpha y = (B\alpha + A) \cdot y^2 + C\alpha \cdot y + p(B\alpha - A) \equiv 0 \pmod{\mathfrak{m}_V^n}. \quad (6.3)$$

Observe that $\mathrm{val}(B\alpha - A) = \mathrm{val}(B\alpha + A)$. If $\mathrm{val}(B\alpha + A) < n - 1$ then, since $\mathrm{val}(y) = 1$, Equation (6.3) implies that $\mathrm{val}(C) = \mathrm{val}(B\alpha - A)$ and so $\mathrm{val}(C) = \mathrm{val}(B\alpha + A)$ as well. We get an equation

$$y^2 + \frac{C\alpha}{B\alpha + A} y + p\frac{B\alpha - A}{B\alpha + A} \equiv y\left(y + \frac{C\alpha}{B\alpha + A}\right) \equiv 0 \pmod{\mathfrak{m}_V},$$

which is an equation with integral coefficients that holds in $V/\mathfrak{m}_V$. By Hensel's lemma it follows that the polynomial $Y^2 + \frac{C\alpha}{B\alpha+A} Y + p\frac{B\alpha-A}{B\alpha+A}$ in the variable $Y$ has a solution,

say $y_0$, in $W(\mathbb{F}_{p^2})$ lifting 0. Moreover, if $y_0'$ is the other solution (so that $f(Y) = Y^2 + \frac{C\alpha}{B\alpha+A}Y + p\frac{B\alpha-A}{B\alpha+A} = (Y-y_0)(Y-y_0')$) then $\mathrm{val}(y_0 - y_0') = 0$, as $y_0'$ reduces to a unit modulo the maximal ideal. Note that, since $\mathrm{val}(B\alpha + A) < n-1$ and $(B\alpha + A)f(y) \equiv 0 \pmod{\mathfrak{m}_V^n}$, we have $f(y) = (y-y_0)(y-y_0') \equiv 0 \pmod{\mathfrak{m}_V^2}$. Since $\mathrm{val}(y) = 1$, $y - y_0'$ is a unit and so $\mathrm{val}(y - y_0) \geq 2$. It follows that $y_0$ is closer to $y$ than any of $y$'s conjugates and so, by Krasner's lemma, $y \in \mathbb{Q}_p(y_0) = W(\mathbb{F}_{p^2}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and that is a contradiction.

Thus, for $y$ chosen as above, a congruence (6.3) implies that $\mathrm{val}(B\alpha + A) \geq n-1$. We get then that $\min\{\mathrm{val}(A), \mathrm{val}(B)\} = n-1$ and then (6.3) gives that $\mathrm{val}(C) \geq n-1$ as well. This shows that for such a choice of $y$ we get that $\sharp\,\varphi(D) \pmod{p^n}$ is $p^{3(n-1)}$ and so the upper bound in the theorem can be achieved. This shows that the bounds are optimal. ■

### 6.5 **Bound in the case of high ramification**

As above, let $V$ be a discrete valuation ring, which is a finite extension of $\mathbb{W}(\bar{\mathbb{F}}_p)$ with absolute ramification index $e_V$. As before, let $E$ be a supersingular elliptic curve over $\bar{\mathbb{F}}_p$. The purpose of this section is to provide a lower bound on $\mathfrak{i}(V/\mathfrak{m}_V^n)$ (defined in terms of deformations $\mathbb{E}$ of $E$ to $V/\mathfrak{m}_V^n$) which is valid regardless of whether the ramification index $e_V$ is smaller than $p$ or not. The proof uses different techniques than those used above.

Consider a deformation $\mathbb{E}$ over $R$ where $R = V/\mathfrak{m}_V^n$. The Hodge filtration

$$0 \to H^0(\mathbb{E}, \Omega^1_{\mathbb{E}/R}) \to \mathbb{H}^1_{\mathrm{dR}}(\mathbb{E}/R),$$

is stable under $\mathrm{End}(\mathbb{E})$ and so there is a resulting ring homomorphism

$$\varphi : \mathrm{End}(\mathbb{E}) \to T(R),$$

where $T(R)$ are the upper triangular matrices with entries in $R$,

$$T(R) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in R \right\}.$$

Let $\mathcal{O}' = \mathrm{End}(\mathbb{E}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$. As we have proved above, $[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})] = [\mathcal{O} : \mathcal{O}']$, where $\mathcal{O}$ is the maximal order of $B_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ obtained as the $p$-completion of $\mathrm{End}(E)$.

Let $\mathcal{O}'' \subseteq \mathcal{O}'$ be a sub-order. There is an induced ring homomorphism

$$\varphi : \mathcal{O}'' \to T(R).$$

Let $K = \mathrm{Ker}(\varphi)$, let

$$I(R) = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : a, b, d \in R \right\},$$

and let $P = \varphi^{-1}(I(R))$. Note that $I(R)$ is the kernel of the ring homomorphism

$$T(R) \to R \oplus R, \quad \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in R \right\} \mapsto (a, d).$$

It follows that $I(R)$ is a two-sided ideal, such that $T(R)/I(R)$ is a commutative ring. Moreover, $I(R)^2 = 0$. As consequence, $P$ is a two-sided ideal of $\mathcal{O}''$ such that $P^2 \subset K$, where $K = \ker(\varphi)$ and $\mathcal{O}''/P$ is commutative.

The following lemmas will be proved in the next subsection.

**Lemma 6.12.** Let $\mathcal{O}_N = \mathbb{Z}_p + p^N\mathcal{O}$. Then, $\mathcal{O}_N$ is an order of $B_{p,\infty} \otimes \mathbb{Q}_p$ contained in $\mathcal{O}$. In the situation above, suppose that $\mathcal{O}' \supseteq \mathcal{O}_N$, then, in the ring $R$, $p^{4N+2} = 0$. □

**Lemma 6.13.** For an order $\mathcal{O}' \subseteq \mathcal{O}$, let $\mathrm{Ind}(\mathcal{O}') = \log_p([\mathcal{O} : \mathcal{O}'])$ and $\mathrm{Appr}(\mathcal{O}') = \min\{N : \mathcal{O}' \supseteq \mathcal{O}_N\}$. Then, $\mathrm{Appr}(\mathcal{O}') \leq \mathrm{Ind}(\mathcal{O}')$. □

Assume the lemmas. Given the order $\mathcal{O}'$, we have $\mathcal{O}' \supseteq \mathcal{O}_N$, where $N = \mathrm{Appr}(\mathcal{O}')$ and, by Lemma 6.12, $p^{4N+2} = 0$. Since the minimal power of $p$ which is zero in $R$ is $\lceil n/e_V \rceil$ we conclude that $(4 \cdot \mathrm{Appr}(\mathcal{O}') + 2) \geq \lceil n/e_V \rceil$. Combining it with Lemma 6.13, we find that $\mathrm{Ind}(\mathcal{O}') \geq \frac{1}{4}(\lceil n/e_V \rceil - 2)$. To summarize, we have proved the following theorem.

**Theorem 6.14.** With the above notation,

$$p^{\frac{1}{4}(\lceil n/e_V \rceil - 2)} \leq \mathrm{i}(V/\mathfrak{m}_V^n).$$ □

### 6.5.1 *Proof of the lemmas*

We use the presentation for the maximal order $\mathcal{O}$ given above,

$$\mathcal{O} = \left\{ \begin{pmatrix} a & b \\ pb^\sigma & a^\sigma \end{pmatrix} : a, b \in W(\mathbb{F}_p^2) \right\}.$$

The first statement in Lemma 6.12 is clear. Consider the situation where $\mathcal{O}' \supseteq \mathcal{O}_N = \mathbb{Z}_p + p^N\mathcal{O}$. We have a homomorphism $\varphi : \mathcal{O}_N \to T(R)$ with kernel $K$ and the

ideal $P = \varphi^{-1}(I(R))$. As we have noted $P^2 \subseteq K$. Let $[x, y] := xy - yx$. Since $\mathcal{O}_N/P$ is commutative, we must have $[x, y] \in P$ for all $x, y \in \mathcal{O}_n$, and so $[x, y]^2 \in K$ for all $x, y \in \mathcal{O}_N$. Consider the elements

$$x = p^N \begin{pmatrix} & 1 \\ p & \end{pmatrix}, \quad y = p^N \begin{pmatrix} & t \\ pt^\sigma & \end{pmatrix},$$

where for $p \neq 2$ we choose $t$ to be a unit in $W(\mathbb{F}_{p^2})$ such that $t^\sigma = -t$ and for $t = 2$ we choose $t \in W(\mathbb{F}_{p^2})$ such that $t^2 + t - 1 = 0$. In both cases $t - t^\sigma$ is a unit whose square is a unit in $\mathbb{Z}_p$, hence in $\mathcal{O}_N$. Now,

$$[x, y] = p^{2N+1} \begin{pmatrix} t^\sigma - t & \\ & t - t^\sigma \end{pmatrix}.$$

We conclude that

$$p^{4N+2} \begin{pmatrix} (t^\sigma - t)^2 & \\ & (t - t^\sigma)^2 \end{pmatrix} \in K$$

and so that $p^{4N+2} = 0$ in $R$. Lemma 6.12 follows.

Lemma 6.13 is in fact trivial. The abelian group $\mathcal{O}/\mathcal{O}'$ has order $p^{\mathrm{Ind}(\mathcal{O}')}$ and thus, if $a \in \mathcal{O}$ then $p^{\mathrm{Ind}(\mathcal{O}')} \cdot a = 0$ in $\mathcal{O}/\mathcal{O}'$, namely $p^{\mathrm{Ind}(\mathcal{O}')} \cdot \mathcal{O} \subseteq \mathcal{O}'$.

**Remark.** One may ask whether the bound in Lemma 6.13 can be improved. The answer to that is *no*. The reader is referred to a paper by Brzezinski [5]. In particular, in Proposition 5.6 of that paper, we find the classification of all Gorenstein orders in $\mathcal{O}$. Examination of the classification shows that our lemma cannot be improved; More precisely, in cases (a)–($c_1$) one actually finds that $\mathrm{Appr}(\mathcal{O}') \leq \lceil \mathrm{Ind}(\mathcal{O}')/2 \rceil$ (and the passage to non-Gorenstein order is not a problem using Proposition 1.4 of that paper), but this does not persist in case ($c_2$). □

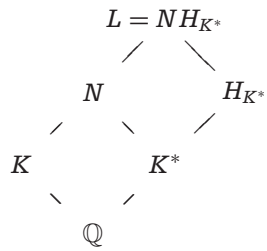
## 7 The Main Theorem

Let $K$ be a primitive CM field of degree four over $\mathbb{Q}$. Let $K^+ = \mathbb{Q}(\sqrt{d})$ where $d$ is a positive square-free integer. Write

$$K = \mathbb{Q}(\sqrt{d})(\sqrt{r}), \quad r = \alpha + \beta\sqrt{d} \ll 0, \quad \alpha, \beta \in \mathbb{Z}.$$

(That is, $r$ is negative under both embeddings of $K^+$ into $\mathbb{R}$.)

Let $\tau \in \mathrm{Sp}(4,\mathbb{Z})\backslash\mathfrak{H}_2$ be a point such that the associated principally polarized abelian variety $A_\tau$ has CM by $\mathcal{O}_K$. Let $L = NH_{K^*}$, where $N$ is the normal closure of $K$ over $\mathbb{Q}$, $K^*$ is the reflex field of $K$ with respect to the CM type determined by $\tau$, and $H_{K^*}$ is the Hilbert class field of $K^*$. Let $\mathfrak{p}_L$ be a prime of $L$ above the rational prime $p$. We fix the notation as in Section 3. In particular, the CM type is $\Phi$ as given there and we have prime ideals $\mathfrak{p}_{N,1} = \mathfrak{p}_L \cap N$, $\mathfrak{p}_{K,1} = \mathfrak{p}_L \cap K$, $\mathfrak{p}_{K^*,1} = \mathfrak{p}_L \cap K^*$, and $p$, corresponding to the fields in the diagram:




(where possibly $K = K^*$, in which case $N = K$ as well). Let $e = e(\mathfrak{p}_{N,1}/p)$ be the ramification index of $\mathfrak{p}_{N,1}$ over $p$.

**Theorem 7.1.** Let $\tau$ be a CM point, as above. Let $f = g/\Theta^k$ be a modular function of level one on $\mathfrak{H}_2$ where:

1. The modular form $\Theta$ is $-4\chi_{10}$ in Igusa's notation, and is equal to the product of the squares of the ten Riemann theta constants with even integral characteristics, normalized to have Fourier coefficients that are integers and of g.c.d. 1.
2. The modular form $g$ is a level one modular form of weight $10k$ with integral Fourier coefficients.

Then $f(\tau) \in L$. If $\mathrm{val}_{\mathfrak{p}_L}(f(\tau)) < 0$ then

$$\mathrm{val}_{\mathfrak{p}_L}(f(\tau)) \geq \begin{cases} -2ek[\log_p(d \cdot \mathrm{Tr}(r)^2) + 1], & e \leq p-1, \\ -16ek[\log_p(d \cdot \mathrm{Tr}(r)^2) - \frac{1}{2}], & \text{any other case.} \end{cases} \tag{7.1}$$

Furthermore, unless we are in the situation of superspecial reduction, namely, we have a check mark in the last column of the tables in Section 3, $\mathrm{val}_{\mathfrak{p}_L}(f(\tau)) \geq 0$. The valuation $\mathrm{val}_{\mathfrak{p}_L}$ is normalized so that a uniformizer at $\mathfrak{p}_L$ has valuation 1. In addition, if $\mathrm{val}_{\mathfrak{p}_L}(f(\tau)) < 0$, then

$$p \leq 4 \cdot d \cdot \mathrm{Tr}(r)^2. \qquad \square$$

**Remark.** We note that $\mathrm{val}_{\mathfrak{p}_N} = \mathrm{val}_{\mathfrak{p}_L}$; that is, the ramification index $e$ is determined by the decomposition of $p$ in $N$ and so is visibly bounded. In addition, $f(\tau) \in H_{K^*}$ and if we normalize the valuation differently, taking a valuation $\mathrm{val}_p$ such that $\mathrm{val}_p(p) = 1$, we can restate (7.1) as follows:

$$\mathrm{val}_p(f(\tau)) \geq \begin{cases} -2k[\log_p(d \cdot \mathrm{Tr}(r)^2) + 1], & e \leq p-1, \\ -16k[\log_p(d \cdot \mathrm{Tr}(r)^2) - \frac{1}{2}], & \text{any other case.} \end{cases} \tag{7.2}$$

Finally, we remark that the expression $\log_p(d \cdot \mathrm{Tr}(r)^2) - \frac{1}{2}$ is always nonnegative if $p \leq 4 \cdot d \cdot \mathrm{Tr}(r)^2$. □

**Proof.** To begin with, the last statement of the theorem is the main result of [21]; that the estimates of [21] in fact yield a slightly sharper inequality than stated there was pointed to us by Marco Streng.

Let $v = \mathrm{val}_{\mathfrak{p}_L}(f(\tau))$. We may assume that $v < 0$. To conceptualize the proof, we divide it into steps.

*Step 1: Adding level structure.* Let $n \geq 3$ be an integer prime to $p$. We abuse notation and identify $\mathcal{A}_{2,n}(\mathbb{C})$ with $\Gamma(n)\backslash\mathfrak{H}_2$, where $\Gamma(n) \subseteq \mathrm{Sp}(4, \mathbb{Z})$ is the principal congruence subgroup of matrices congruent to 1 modulo $n$. Let $\tau_n \in \mathcal{A}_{2,n}$ such that

$$\pi_n(\tau_n) = \tau,$$

where $\pi_n \colon \mathcal{A}_{2,n} \to \mathcal{A}_{2,1}$ is the natural projection. The point $\tau_n$ can be defined over the field $L_n$, where $L_n = L(A_\tau[n])$ is the field obtained from $L$ by adjoining the $n$-torsion points of $A_\tau$. The extension $L_n/L$ is unramified at $p$ (cf. proof of Lemma 2.3). We let $\mathfrak{p}_{L_n}$ be a prime of $L_n$ such that $\mathfrak{p}_{L_n} \cap L = \mathfrak{p}_L$.

**Lemma 7.2.** Let $f_n = f \circ \pi_n$. Then,

$$\mathrm{val}_{\mathfrak{p}_{L_n}}(f_n(\tau_n)) = \mathrm{val}_{\mathfrak{p}_L}(f(\tau)).$$

□

**Proof.** This is clear: $f_n(\tau_n) = f(\tau)$ and the extension $L_n/L$ is unramified at $\mathfrak{p}_L$. ■

It is therefore enough to prove the same bound given in (7.1) but for $\mathrm{val}_{\mathfrak{p}_{L_n}}(f_n(\tau_n))$.

*Step 2: Reducing to a geometric problem.*

**Lemma 7.3.** Let $(f_n)$ be the divisor of $f_n$ on $\mathcal{A}_{2,n}$. Let $(f)_\infty$ be its polar part. Let $\bar{\mathcal{H}}_{1,n}$ be the Humbert divisor of invariant 1 on $\mathcal{A}_{2,n}$. Then,

$$(f)_\infty = 4k \cdot \bar{\mathcal{H}}_{1,n}.$$

□

**Proof.** It is well known that $\Theta$ vanishes to order 2 on $\bar{\mathcal{H}}_{1,1}$. The lemma then follows immediately from Lemma 2.2. ■

By Lemma 2.3, the abelian variety $A_{\tau_n}$ has good reduction at $\mathfrak{p}_{L_n}$. Let $\Lambda$ be the ring of integers of $\tilde{L}_n$ (the completion of $L_n$ at $\mathfrak{p}_{L_n}$) and $\mathfrak{P}$ its maximal ideal. Then there is a morphism

$$\iota : \Lambda \to \mathcal{A}_{2,n},$$

corresponding to $A_{\tau_n}$.

**Proposition 7.4.** Let $A := A_{\tau_n}$. There is an unramified field extension $M$ of $\tilde{L}_n$ of degree at most 2, with ring of integers $V$, such that

$$A \otimes (V/\mathfrak{m}_V^w) \cong \mathbb{E} \times \mathbb{E}',$$

as polarized abelian varieties, where $\mathbb{E}$ and $\mathbb{E}'$ are elliptic curves over $V/\mathfrak{m}_V^w$, and where

$$w = \lceil -v/4k \rceil. \qquad \square$$

**Proof.** By Lemma 5.1, applied to $1/f$, the morphism $\iota$ induces a morphism

$$\iota : \Lambda/\mathfrak{P}^w \to \bar{\mathcal{H}}_{1,n}.$$

In the notation of Proposition 4.2, we have $\bar{\mathcal{H}}_{1,n} = \beta(\mathcal{B}_n)$.

Consider the cartesian diagram

$$\begin{array}{ccc} S & \longrightarrow & \mathcal{B}_n \\ \downarrow & \square & \downarrow \beta \\ \mathrm{Spec}(\Lambda/\mathfrak{P}^w) & \longrightarrow & \bar{\mathcal{H}}_{1,n} \end{array}$$

Since $\beta : \mathcal{B}_n \to \bar{\mathcal{H}}_{1,n}$ is étale of degree 2, the morphism $S \to \mathrm{Spec}(\Lambda/\mathfrak{P}^w)$ is étale and affine, and so $S$ is an affine scheme, possibly disconnected. We can then choose a field $M$, as in the statement of the proposition, such that $\mathrm{Spec}(V/\mathfrak{m}_V^w)$ is equal to $S$ (or one of its

connected components). We therefore get a point

$$\mathrm{Spec}(V/\mathfrak{m}_V^w) \to \mathcal{B}_n,$$

lifting $\iota$, and that means precisely that $A \otimes V/\mathfrak{m}_V^w$ is isomorphic, as a polarized abelian variety with level $n$ structure, to a product of elliptic curves over $V/\mathfrak{m}_V^w$, with the natural product polarization and some level $n$ structure. ■

Note that $\mathrm{val}_{\mathfrak{m}_V}(f_n(\tau_n)) = \mathrm{val}_{\mathfrak{p}_{L_n}}(f_n(\tau_n))$ and so it is enough to show that (7.1) holds for $\mathrm{val}_{\mathfrak{m}_V}(f_n(\tau_n))$. Let us reset our notation and recall that at this point we have a principally polarized abelian surface $A = A_{\tau_n} \otimes V$ with CM by $\mathcal{O}_K$, having good reduction at $\mathfrak{m}_V$ and such that

$$A \otimes V/\mathfrak{m}_V^w \cong (\mathbb{E} \times \mathbb{E}', \lambda_1 \times \lambda_2),$$

where $\mathbb{E}$ and $\mathbb{E}'$, are elliptic curves over $V/\mathfrak{m}_V^w$. Recall also that $V$ is an unramified extension of the completion of $L = NH_{K^*}$ at the prime $\mathfrak{p}_L$.

*Step 3: Reduction to a statement about* $\mathrm{End}(\mathbb{E})$.

Our notation for the field $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$ is precisely as in [21]. As in [21], one argues that $\mathbb{E}$ and $\mathbb{E}'$ have supersingular reduction, denoted $E$ and $E'$, respectively. One writes

$$\sqrt{d} \mapsto \begin{pmatrix} a & b \\ b^\vee & -a \end{pmatrix}, \quad \sqrt{r} \mapsto \begin{pmatrix} x & y \\ -y^\vee & w \end{pmatrix},$$

as elements of

$$\mathrm{Hom}(\mathbb{E} \times \mathbb{E}') = \begin{pmatrix} \mathrm{End}(\mathbb{E}) & \mathrm{Hom}(\mathbb{E}', \mathbb{E}) \\ \mathrm{Hom}(\mathbb{E}, \mathbb{E}') & \mathrm{End}(\mathbb{E}') \end{pmatrix}.$$

(We are using $\vee$ to denote the dual isogeny. The $w$ appearing in the matrix should not be confused with the $w$ defined in Proposition 7.4; the notation is chosen so as to make comparison with [21] easier and should not cause confusion.) Note that $b \in \mathrm{Hom}(\mathbb{E}', \mathbb{E})$ is an isogeny of degree $bb^\vee \leq d$. Using $b$, we may view $\mathrm{End}(\mathbb{E} \times \mathbb{E}')$ as a subring of $M_2(\mathrm{End}^0(\mathbb{E}))$ by

$$\begin{pmatrix} \varphi_{ij} \end{pmatrix} \mapsto \begin{pmatrix} 1 & \\ & (b^\vee)^{-1} \end{pmatrix} \begin{pmatrix} \varphi_{ij} \end{pmatrix} \begin{pmatrix} 1 & \\ & b^\vee \end{pmatrix}.$$

Appying this to the matrices defining $\sqrt{d}$ and $\sqrt{r}$, we find the matrices

$$\begin{pmatrix} a & bb^\vee \\ 1 & -a \end{pmatrix}, \quad \begin{pmatrix} x & yb^\vee \\ -\frac{1}{bb^\vee} by^\vee & \frac{1}{bb^\vee} bwb^\vee \end{pmatrix}.$$

As in [21], the elements $1, x, yb^\vee$, and $xyb^\vee$, which are *endomorphisms* of $\mathbb{E}$ (and not just rational endomorphisms), must be linearly independent over $\mathbb{Z}$ (one shows that otherwise they generate a quadratic imaginary subfield $K_1$ of $B_{p,\infty}$ such that we have $K \hookrightarrow M_2(K_1)$, leading to a contraction). As in [21, p. 464], one finds that the norms of these elements are bounded, respectively, by

$$1, \delta_2, d\delta_1, d\delta_1\delta_2,$$

where

$$\delta_1 = |\alpha| - |\beta| \cdot |a|, \quad \delta_2 = |\alpha| + |\beta| \cdot |a|.$$

It follows that

$$[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})] \leq [\mathrm{End}(E) : \mathbb{Z}[1, x, yb^\vee, xyb^\vee]] \leq 4d(\delta_1\delta_2)/p.$$

(Cf. [21, p. 460] for the last inequality.)

*Step 4: Input from deformation theory.* We now utilize the results of Section 6 to bound the index $[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})]$ from below. Recall that $\mathbb{E}$ is an elliptic curve over $V/\mathfrak{m}_V^w$ and $V$ is an unramified extension of the completion of $L = NH_{K^*}$, hence of $N$ completed at the prime $\mathfrak{p}_{N,1}$. Thus, $e_V$ – the absolute ramification index of $V$ – is equal to $e = e(\mathfrak{p}_{N,1}/p)$.

1. *Small ramification.* Suppose that $e \leq p - 1$. By Theorem 6.11,

$$[\mathrm{End}(E) : \mathrm{End}(\mathbb{E})] \geq p^{2(\lceil w/e \rceil - 1)},$$

and so $2(\lceil w/e \rceil - 1) \leq \log_p(4d(\delta_1\delta_2)/p)$. Since $\delta_1\delta_2 = \alpha^2 - \beta^2 a^2 \leq \alpha^2 = \frac{1}{4}(\mathrm{Tr}(r))^2$, we find that $w/e \leq \lceil w/e \rceil \leq \frac{1}{2}[\log_p(d \cdot \mathrm{Tr}(r)^2) + 1]$. Since $w = \lceil -v/4k \rceil$, it follows that $-v \leq 4kw \leq 2ek[\log_p(d \cdot \mathrm{Tr}(r)^2) + 1]$.

2. *High ramification.* Suppose that $e > p-1$. By Theorem 6.14,

$$[\mathrm{End}(E):\mathrm{End}(\mathbb{E})] \geq p^{\frac{1}{4}(\lceil w/e \rceil - 2)}.$$

Similar computations yield $-v \leq 16ek\left[\log_p(d\cdot \mathrm{Tr}(r)^2) - \frac{1}{2}\right]$. ■

### 7.1 Factorization of class invariants and denominators of Igusa class polynomials

We derive several consequences of Theorem 7.1.

**Corollary 7.5.** Let $K$ be a quartic primitive CM field, as in the beginning of Section 7 and let $\mathfrak{h}_i(x)$, $i=1,2,3$, be the class polynomial defined using the function $f_i/\Theta^{k(i)}$ as in Section 2.4, Equation (2.10), where $k(i)=6,4,4$ for $i=1,2,3$, respectively. In the notation of Theorem 7.1, the coefficient of $x^{\deg(\mathfrak{h}_i)-t}$ in $\mathfrak{h}_i(x)$, which is a rational number, is either an integer at $p$, and, otherwise, has valuation $\mathrm{val}_p$ greater or equal to

$$\begin{aligned} &-2t\cdot k(i)[\log_p(d\cdot \mathrm{Tr}(r)^2)+1], \quad e\leq p-1,\\ &-16t\cdot k(i)\left[\log_p(d\cdot \mathrm{Tr}(r)^2)-\frac{1}{2}\right], \quad \text{else.}\end{aligned}$$

□

**Proof.** Straightforward from Theorem 7.1. ■

**Remark.** We remark that this corollary is crucial in bounding the complexity of construction of CM curves of genus 2, by the methods currently used. The corollary is proved for the invariants that we find convenient; with little effort one can deduce easily such bound for the Igusa class polynomials appearing in Equation (2.9), which are often used in the literature. Further, we could have equally proved the corollary for class polynomials formed out of the Igusa coordinates $\gamma_i$ (see Section 2.3). In principle, this is "the right thing to do", on the other hand, given Proposition 2.1, in practice it suffices to deal only with (some set of) absolute Igusa invariants. □

**Corollary 7.6.** Let $u(\Phi;\mathfrak{a},\mathfrak{b})$ be the class invariant defined in [10], associated to fractional ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $K$. Let $\mathfrak{p}_L$ be a prime of $L$, as in Theorem 7.1 and $\mathfrak{p}_{H_{K^*}} = \mathfrak{p}_L \cap H_{K^*}$. We note that $u(\Phi;\mathfrak{a},\mathfrak{b}) \in H_{K^*} \subseteq L$. We have

$$|\mathrm{val}_{\mathfrak{p}_{H_{K^*}}}(u(\Phi;\mathfrak{a},\mathfrak{b}))| \leq \begin{cases} 4e^*\cdot[\log_p(d\cdot \mathrm{Tr}(r)^2)+1], & e\leq p-1,\\ 32e^*\cdot[\log_p(d\cdot \mathrm{Tr}(r)^2)-\frac{1}{2}], & \text{else,}\end{cases} \tag{7.3}$$

where $e^*$ is the ramification index of $\mathfrak{p}_{K^*}=\mathfrak{p}_{K^*,1}$ over $p$. □

**Proof.** We refer to [10] for the detailed definitions. We have

$$u(\Phi, \mathfrak{a}) = \frac{\Theta(\Phi(\mathfrak{a}^{-1}))}{\Theta(\Phi(\mathcal{O}_K))},$$

which may also be written as

$$u(\Phi, \mathfrak{a}) = \left(\frac{\Theta|_\gamma}{\Theta}\right)(\tau),$$

where $\tau$ is a period matrix for $\Phi(\mathcal{O}_K)$ and, for $\mathfrak{a}^{-1}$ an integral ideal, $\gamma \in \mathrm{GSp}(4, \mathbb{Q})$ is a matrix with integral entries and determinant $\mathrm{Norm}(\mathfrak{a})$ (cf. [10, p. 786 and Section 3.2]). We remark that we may also write

$$u(\Phi, \mathfrak{a}) = \left(\frac{\Theta}{\Theta|_{\gamma^{-1}}}\right)(\tau'),$$

where $\tau'$ is a period matrix corresponding to $\mathfrak{a}^{-1}$.

Now fix a prime ideal $\mathfrak{P}$ of $\bar{\mathbb{Q}}$ above the rational prime $p$. Assume $\mathfrak{a}^{-1}$ is an integral ideal of norm $n \geq 3$, which is relatively prime to $\mathfrak{P}$. We note that both $\frac{\Theta|_\gamma}{\Theta}$ and $\frac{\Theta}{\Theta|_{\gamma^{-1}}}$ are modular functions of level $n$, defined over $\mathbb{Q}(\zeta_n)$, and $u(\Phi, \mathfrak{a})$ is obtained by evaluating them at a point with CM by $\mathcal{O}_K$. We can therefore apply Theorem 7.1, or, more precisely, the result we have obtained in its proof by passing to level $n$. We consider both $\left(\frac{\Theta|_\gamma}{\Theta}\right)(\tau)$ and $\left(\frac{\Theta}{\Theta|_{\gamma^{-1}}}\right)(\tau')$ to get from one a bound on the denominator of $u(\Phi, \mathfrak{a})$ at $\mathfrak{P}$ and, from the other, a bound on the numerator. The points $\tau$ and $\tau'$ correspond to abelian varieties with CM by $\mathcal{O}_K$ defined over the compositum $L'$ of $L$ and $\mathbb{Q}(\zeta_n)$, which does not increase the ramification index $e$ of $p$ at $\mathfrak{p}_L = \mathfrak{P} \cap L$. We may then consider the valuation at $\mathfrak{p}_{L'} = \mathfrak{P} \cap L'$. We conclude that

$$|\mathrm{val}_{\mathfrak{p}_{L'}}(u(\Phi, \mathfrak{a}))| \leq \begin{cases} 4e \cdot [\log_p(d \cdot \mathrm{Tr}(r)^2) + 1], & e \leq p-1, \\ 32e \cdot [\log_p(d \cdot \mathrm{Tr}(r)^2) - \frac{1}{2}], & \text{else.} \end{cases} \tag{7.4}$$

However, the algebraic number $u(\Phi, \mathfrak{a})$ actually lies in $H_{K^*}$ and so we get

$$|\mathrm{val}_{\mathfrak{p}_{H_{K^*}}}(u(\Phi, \mathfrak{a}))| \leq \begin{cases} 4e^* \cdot [\log_p(d \cdot \mathrm{Tr}(r)^2) + 1], & e \leq p-1, \\ 32e^* \cdot [\log_p(d \cdot \mathrm{Tr}(r)^2) - \frac{1}{2}], & \text{else.} \end{cases}$$

where $e^* = e(\mathfrak{p}_{K^*}/p)$.

Let us now consider $u(\Phi; \mathfrak{a}, \mathfrak{b})$. The class invariant $u(\Phi; \mathfrak{a}, \mathfrak{b})$ depends only on the ideal class of $\mathfrak{a}$ and $\mathfrak{b}$ in the class group of $K$. Having fixed $\mathfrak{P}$, we may assume therefore that $\mathfrak{a}^{-1}, \mathfrak{b}^{-1}$ are integral and of norm prime to $p$ and $\geq 3$. We note the expressions:

$$u(\Phi; \mathfrak{a}, \mathfrak{b}) = \frac{u(\Phi, \mathfrak{a}\mathfrak{b})}{u(\Phi, \mathfrak{a})u(\Phi, \mathfrak{b})} = \frac{\Theta(\Phi(\mathfrak{a}^{-1}\mathfrak{b}^{-1}))\Theta(\Phi(\mathcal{O}_K))}{\Theta(\Phi(\mathfrak{a}^{-1}))\Theta(\Phi(\mathfrak{b}^{-1}))}.$$

Instead of using directly our bound above, we note that for $\mathfrak{a}^{-1}$ and $\mathfrak{b}^{-1}$ integral ideals, we may write

$$u(\Phi; \mathfrak{a}, \mathfrak{b}) = \left(\frac{\Theta|_\gamma}{\Theta}\right)(\tau') \Big/ \left(\frac{\Theta|_\beta}{\Theta}\right)(\tau),$$

where $\tau$ is a period matrix for $\Phi(\mathcal{O}_K)$, $\tau'$ is a period matrix for $\Phi(\mathfrak{a}^{-1})$, $\beta, \gamma \in \mathrm{GSp}(4, \mathbb{Q})$ are matrices with integral entries and determinants prime to $p$. Thus, repeating the consideration above, we conclude the bound in the corollary. ■

**Acknowledgements**

We would like to thank the anonymous referee for a very careful reading of the manuscript resulting in numerous suggestions that helped improve the quality of this paper and fine tune some of our results. We thank C.-L. Chai, B. Conrad, B. Howard and J. Milne for interesting comments concerning complex multiplication. E.Z.G. thank the hospitality of Microsoft Research, Redmond, during a visit when much of this paper was written.

## References

[1] Belding, J., R. Bröker, A. Enge, and K. Lauter. "Computing Hilbert class polynomials." *Algorithmic Number Theory* 282–95. Lecture Notes in Computer Science 5011. Berlin: Springer, 2008.

[2] Bernstein, D. J. "Multidigit modular multiplication with the explicit chinese remainder theorem." Ph.D. thesis, University of California at Berkeley, Chapter 4.

[3] Bolza, O. "Darstellung der rationalen ganzen Invarianten der Binärform sechsten Grades durch die Nullwerthe der zugehörigen $\theta$-Functionen." *Mathematische Annalen* 30, no. 4 (1887): 478–95.

[4] Bruinier, J. H. and T. Yang. "CM-values of Hilbert modular functions." *Inventiones Mathematicae* 163, no. 2 (2006): 229–88.

[5] Brzezinski, J. "On orders in quaternion algebras." *Communications in Algebra* 11, no. 5 (1983): 501–22.

[6] Chai, C.-L. "Siegel moduli schemes and their compactifications over $\mathbb{C}$." In *Arithmetic Geometry*, edited by G. Cornell and J. H. Silvermann, 231–51. (Storrs, Conn., 1984), New York: Springer, 1986.

[7] Clebsch, A. "Zur Theorie der binären algebraischen Formen." *Mathematische Annalen* 3, no. 2 (1870): 265–67.

[8] Cohen, I. S. "On the structure and ideal theory of complete local rings." *Transactions of the American Mathematical Society* 59, no. 1 (1946): 54–106.

[9] Cohen, H. *Number Theory. Vol. I. Tools and Diophantine Equations*. Graduate Texts in Mathematics 239. New York: Springer, 2007.

[10] De Shalit, E. and E. Z. Goren. "On special values of theta functions of genus two." *Université de Grenoble. Annales de l'Institut Fourier* 47, no. 3 (1997): 775–99.

[11] Dokchitser, T. "Deformations of $p$-divisible groups and $p$-descent on elliptic curves." Ph.D. Thesis. Utrecht 2000.

[12] Eisentraeger, K. and K. Lauter. "A CRT algorithm for constructing genus 2 curves over finite fields." *Arithmetic, Geometry and Coding Theory* (AGCT 2005), 161–76, Séminaires et Congrès 21, 2009.

[13] Faltings, G. and C.-L. Chai. *Degeneration of Abelian Varieties*, With an appendix by David Mumford. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 22. Berlin: Springer, 1990.

[14] Farkas, H. M. and I. Kra. *Riemann Surfaces*, 2nd edn. Graduate Texts in Mathematics 71. Berlin: Springer, 1992.

[15] Frey, G. and E. Kani. "Curves of genus 2 covering elliptic curves and an arithmetical application." In *Arithmetic Algebraic Geometry* (Texel, 1989), 153–76. Progress in Mathematics 89. Boston, MA: Birkhäuser Boston, 1991.

[16] Gaudry, P., T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng. "The 2-adic CM method for genus 2 curves with application to cryptography." *Advances in Cryptology, ASIACRYPT 2006*, 114–29. Lecture Notes in Computer Science 4284. Berlin: Springer, 2006.

[17] van der Geer, G. "On the geometry of a Siegel modular threefold." *Mathematische Annalen* 260, no. 3 (1982): 317–50.

[18] van der Geer, G. *Hilbert modular surfaces*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 16. Berlin: Springer, 1988.

[19] Goren, E. Z. "On certain reduction problems concerning abelian surfaces." *Manuscripta Mathematica* 94, no. 1 (1997): 33–43.

[20] Goren, E. Z. and K. E. Lauter. "Evil primes and superspecial moduli." *International Mathematics Research Notices* 2006, Art. ID 53864, 19 pp.

[21] Goren, E. Z. and K. E. Lauter. "Class invariants for quartic CM fields." *Université de Grenoble. Annales de l'Institut Fourier* 57, no. 2 (2007): 457–80.

[22] Gross, B. H. "On canonical and quasicanonical liftings." *Inventiones Mathematicae* 84, no. 2 (1986): 321–26.

[23] Grothendieck, A. *Groupes de Barsotti-Tate et cristaux de Dieudonné*. Séminaire de Mathématiques Supérieures, No. 45 (Été, 1970). Les Presses de l'Université de Montréal, Montreal, Québec, 1974.

[24] Harley, R., J.-F. Mestre, and P. Gaudry. "Counting points with the arithmetic-geometric mean." *Eurocrypt 2001*, Rump session, 2001.

[25] Hitt O'Connor, L., G. McGuire, M. Naehrig, and M. Streng. "CM construction of genus 2 curves with $p$-rank 1." *Journal of Number Theory* 131, no. 5 (2011): 920–35.

[26] Howard, B. "Complex multiplication cycles and Kudla-Rapoport divisors." 2010: preprint https://www2.bc.edu/∼howardbe/

[27] Ibukiyama, T., T. Katsura, and F. Oort. "Supersingular curves of genus two and class numbers." *Compositio Mathematica* 57, no. 2 (1986): 127–52.

[28] Igusa, J.-I. "Arithmetic variety of moduli for genus two." *Annals of Mathematics. Second Series* 72, no. 3 (1960): 612–49.

[29] Igusa, J.-I. "On Siegel modular forms of genus two." *American Journal of Mathematics* 84, no. 1 (1962): 175–200.

[30] Igusa, J.-I. "Modular forms and projective invariants." *American Journal of Mathematics* 89, no. 3 (1967): 817–55.

[31] Igusa, J.-I. "On the ring of modular forms of degree two over $Z$." *American Journal of Mathematics* 101, no. 1 (1979): 149–83.

[32] Katz, N. "Serre–Tate local moduli." *Algebraic surfaces (Orsay, 1976–78)*, 138–202. Lecture Notes in Mathematics 868. Berlin: Springer, 1981.

[33] Lang, S. *Complex Multiplication*. Grundlehren der Mathematischen Wissenschaften 255. New York: Springer, 1983.

[34] Lang, S. *Elliptic Functions*, 2nd edn. Graduate Texts in Mathematics 112. New York: Springer, 1987. With an appendix by J. Tate.

[35] Lauter, K. E. "Primes in the denominators of Igusa class polynomials." (2003): preprint arXiv:math.NT/0301240.

[36] Manin, Y. I. "The theory of commutative formal groups over fields of finite characteristic." *Russian Mathematical Surveys* 18, no. 6 (1963): 1–83.

[37] Mestre, J.-F. "Construction de courbes de genre 2 à partir de leurs modules." *Effective Methods in Algebraic Geometry* (Castiglioncello, 1990), 313–34. Progress in Mathematics 94. Boston, MA: Birkhäuser Boston, 1991.

[38] Mestre, J.-F. "Lettre adressée à Gaudry et Harley." Décembre 2000. Available from http://www.math.jussieu.fr/∼mestre/lettreGaudryHarley.ps

[39] Milne, J. S. "Abelian varieties defined over their fields of moduli. I." *The Bulletin of the London Mathematical Society* 4 (1972): 370–72. Correction: *The Bulletin of the London Mathematical Society* 6 (1974): 145–46.

[40] Mumford, D. *Abelian Varieties*. Tata Institute of Fundamental Research Studies in Mathematics 5. London : Oxford University Press, 1970.

[41] Oda, T. "The first de Rham cohomology group and Dieudonné modules." *Annales Scientifiques de l'École Normale Supérieure. Quatriéme Série* 2 (1969): 63–135.

[42] Oort, F. *Commutative Group Schemes*. Lecture Notes in Mathematics 15. Berlin: Springer, 1966.

[43] Oort, F. "Which abelian surfaces are products of elliptic curves?" *Mathematische Annalen* 214, no. 1 (1975): 35–47.

[44] Pries, R. and H. J. Zhu. "The $p$-rank stratification of Artin-Schreier curves." (2006): preprint http://front.math.ucdavis.edu/0609.5657

[45] Rubin, K. "A Stark conjecture "over Z" for abelian L-functions with multiple zeros." *Université de Grenoble. Annales de l'Institut Fourier* 46, no. 1 (1996): 33–62.

[46] Serre, J.-P. and J. Tate. "Good reduction of abelian varieties." *Annals of Mathematics. Second Series* 88, no. 3 (1968): 492–517.

[47] Shimura, G. "On the zeta-function of an abelian Variety with complex multiplication." *Annals of Mathematics. Second Series* 94, no. 3 (1971): 504–33.

[48] Shimura, G. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton Mathematical Series, 46. Princeton, NJ: Princeton University Press, 1998.

[49] Spallek, A.-M. "Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen." Ph.D. Thesis. Universität Gesamthochschule Essen, 1994.

[50] Streng, M. "Computing Igusa class polynomials." (2009) preprint arxiv.org/abs/0903.4766, 2009.

[51] Sutherland, A. "Computing Hilbert class polynomials with the Chinese Remainder Theorem." *Mathematics of Computation* 80, no. 273 (2011): 501–38.

[52] Tate, J. *Les conjectures de Stark sur les fonctions L d'Artin en* $s = 0$. Lecture notes edited by Dominique Bernardi and Norbert Schappacher. Progress in Mathematics 47. Basel: Birkhäuser, 1984.

[53] Vallieres, D. "Class invariants." McGill M.Sc. thesis, 2005. http://www.math.mcgill.ca/goren

[54] van Wamelen, P. "Examples of genus two CM curves defined over the rationals." *Mathematics of Computation* 68, no. 225 (1999): 307–20.

[55] van Wamelen, P. "Proving that a genus 2 curve has complex multiplication." *Mathematics of Computation* 68 (1999), no. 228, 1663–77.

[56] Weil, A. "Zum Beweis des Torellischen Satzes." *Nachrichten der Akademie der Wissenschaften in Gottingen* 1957, no. 2 (1957): 33–53.

[57] Weng, A. "Constructing hyperelliptic curves of genus 2 suitable for cryptography." *Mathematics of Computation* 72, no. 241 (2003): 435–58.

[58] Yafaev, A. Private communication. July, 2009.

[59] Yang, T. "Arithmetic intersection on a Hilbert modular surface and the faltings height." (2007): preprint http://www.math.wisc.edu/∼thyang/.

[60] Yu, C.-F. "The isomorphism classes of abelian varieties of CM-type." *Journal of Pure and Applied Algebra* 187, no. 1–3 (2004): 305–19.

[61] Zink, Th. "The display of a formal $p$-divisible group." *Cohomologies p-adiques et Applications Arithmétiques I.* no. 278 (2002): 127–248.