Field of definition of abelian surfaces with maximal Picard rank

Sophia Hou

February 2026

Abstract

We study the field of definition of abelian surfaces of maximal Picard rank and of the closely related singular K3 surfaces.

Such abelian surfaces decompose as a product of two isogenous CM elliptic curves and are determined (up to isomorphism) by an integer parameter measuring the relative conductors of its elliptic curve factors and by a single CM elliptic curve. In the key case where the first parameter is a power of a prime, we show that the smallest number field over which the surface can be defined is related to the ring class field attached to the larger conductor: it is either the full ring class field or its maximal real subfield, with the two cases distinguished precisely by whether the elliptic curve parameter's j-invariant is real. Our approach uses explicit constructions from CM theory and class field theory.

For the field of definition of K3 surfaces, we use the classification via quadratic forms given by Shioda and Inose to show that for a K3 surface associated with a quadratic form that has trivial square in the form class group, a smaller field of definition than the appropriately chosen ring class field can be achieved.

Contents

1 Introduction **2**

2 Background **4**

2.1 CM theory of elliptic curves 4

2.2 Ring class fields and j-invariants 5

2.3 Previous work on fields of definition 6

2.4 Abelian surfaces of maximal Picard rank 7

3 Prime-power conductor parameter: decompositions and fields of definition 8

3.1 Describing the decompositions 8

3.2 Main results 10

3.3 Abelian surfaces with more kinds of decompositions 14

4 Field of definition of a singular K3 surface 15

4.1 From intersection forms to $\mathscr{A}_{m,E}$ and back 15

5 Appendix: Computations 18

1 Introduction

A one-dimensional abelian variety (an elliptic curve) defined over a field F can be described by an equation of the form $y^2 = x^3 + ax + b$ with $a, b \in F$. Throughout this paper, when we speak about the *field of definition* of a complex elliptic curve $E/\mathbb{C}$, we mean a number field $L \subset \mathbb{C}$ such that there exists an elliptic curve E_L/L with $E_L \otimes_L \mathbb{C} \cong E$. The *minimal field of definition* of E is the intersection of all such number fields $L \subset \mathbb{C}$ over which E descends; we denote it by L_E. Remarkably, for elliptic curves one has $L_E = \mathbb{Q}(j(E))$, meaning the j-invariant encodes the minimal field of definition.

For higher-dimensional abelian varieties, the question of the minimal field of definition is much more difficult to consider. The case of abelian surfaces (and the closely related question of K3 surfaces) which have *maximal Picard rank* has been considered in the past in [4, 6, 7] among others. Surfaces of maximal Picard rank are also an object of study in their own right, such as in [1].

Such surfaces are more tractable than the case of a general abelian surface because a complex abelian surface of maximal Picard rank is always isomorphic to a product $E_1 \times E_2$ of two isogenous CM elliptic curves [2, 5].

We might assume that for an abelian surface $A = E_1 \times E_2$, the number field $\mathbb{Q}(j(E_1), j(E_2))$ is "minimal" among number fields $L \subseteq \mathbb{C}$ for which there exists an abelian surface A_L/L with $\mathscr{A}_L \times_L \mathbb{C} \cong A$ (that is, fields of definition of $\mathscr{A}$). However, there are other choices of decomposition $\mathscr{A} = E_1 \times E_2 \cong E_3 \times E_4$ such that $\mathbb{Q}(j(E_3), j(E_4))$ is not the same field and indeed may not have the same degree over $\mathbb{Q}$ as $\mathbb{Q}(j(E_1), j(E_2))$. We can classify Picard-maximal abelian surfaces up to isomorphism by two invariants $d \in \mathbb{Z}_{>0}$ and E a CM elliptic curve [4, Theorem 4.2.4]. In this paper we consider which decompositions $\mathscr{A}_{d,E} \cong E_1 \times E_2$ have their fields of definition $\mathbb{Q}(j(E_1), j(E_2)) \subseteq \mathbb{Q}(j(E), j(E_1), j(E_2))$ of minimal degree.

The invariant d, which is the *degree of primitivity* of the binary quadratic form associated to the abelian surface $\mathscr{A}$ by [8], can also be thought of as measuring the difference between the orders $\operatorname{End}(E_1), \operatorname{End}(E_2)$ for a decomposition $\mathscr{A} \cong E_1 \times E_2$. Specifically, $d = \operatorname{lcm}(f_1, f_2)/\gcd(f_1, f_2)$ for f_i the conductor of the order $\operatorname{End}(E_i) \subsetneq K$ where where K is the common CM field (equivalently, the algebra of self-isogenies $\operatorname{End}(E_i) \otimes \mathbb{Q}$). The case $d = 1$ covers Picard-maximal abelian surfaces which have $\mathscr{A} = E_1 \times E_2$ for E_i as CM elliptic curves with the same endomorphism ring; the field of definition of these *primitive* abelian surfaces has been characterized in [4, Proposition 4.2.6].

In this paper, we generalize this result to the case $d = p^n$ for a prime p. Specifically, we prove that if $j(E)$ is not real, then the minimal field of definition of the isomorphism class $\mathscr{A}_{p^n,E}$ is the full ring class field of the order in $K = \operatorname{Frac}(\operatorname{End}(E))$ which has conductor equal to $p^n \cdot \operatorname{cond}(\operatorname{End}(E))$ (Theorem 3.8). If $j(E) \in \mathbb{R}$, then the minimal field of definition of $\mathscr{A}_{p^n,E}$ is the real subfield of the same ring class field (Theorem 3.7). Similarly to [4], we use CM theory and class field theory to obtain our results.

Abelian surfaces of maximal Picard rank in characteristic 0 are closely connected to singular K3 surfaces: namely by [7] any *singular* (having Picard rank 20, which is maximal in char. 0) K3 surface over $\mathbb{C}$ is a double cover of the Kummer surface of a Picard-maximal complex abelian surface. As with abelian surfaces, we can use methods of class field theory and CM theory to prove results similar to [6] for the minimal field of definition of singular K3 surfaces.

Fields of definition: conventions

For general abelian varieties over $\overline{\mathbb{Q}}$, there need not exist a unique *minimal* field of definition: an abelian variety can descend to two subfields $K_1, K_2 \subset \overline{\mathbb{Q}}$ without descending to $K_1 \cap K_2$. In particular, one must specify what auxiliary structure is required to descend.

In this paper we work with Picard-maximal complex abelian surfaces that admit a product decomposition

$$A \;\cong\; E_1 \times E_2,$$

where each $E_i/\mathbb{C}$ has CM by an order in the same imaginary quadratic field K. Our results concern the smallest number field over which *some* model of A together with *some* such CM product decomposition exists.

More precisely, for an isomorphism class $\mathscr{A}_{d,E}$ we consider the set of triples (E_1, E_2, ι) where E_1, E_2 are CM elliptic curves and $\iota : \mathscr{A}_{d,E} \xrightarrow{\sim} E_1 \times E_2$ is a complex isomorphism of abelian surfaces. We define the *decomposition field of definition* of $\mathscr{A}_{d,E}$ to be

$$L^{\mathrm{dec}}(\mathscr{A}_{d,E}) := \min_{(E_1,E_2,\iota)} \mathbb{Q}\big(j(E),\, j(E_1),\, j(E_2)\big) \subset \mathbb{C},$$

where the minimum is taken with respect to inclusion among number fields.

This notion is intrinsic to the isomorphism class $\mathscr{A}_{d,E}$ (because we minimize over all decompositions), but it is *not* the same as the smallest field over which *all* endomorphisms of A

are defined: for example, for $A = E \times E$ the full endomorphism ring $\mathrm{End}(A) \cong M_2(\mathrm{End}(E))$ typically requires adjoining the CM field K even if $j(E) \in \mathbb{R}$. It is also distinct from the minimal number field L over which there exists $\mathscr{A}_L/L$ with $\mathscr{A}_L \times_L \mathbb{C} \cong \mathscr{A}$ (this L is generally not unique) We comment on the relation between $L^{\mathrm{dec}}(\mathscr{A}_{d,E})$ and other standard fields of definition in Remark 3.2.

The structure of this paper is as follows: In Section 2, we state the necessary background on CM elliptic curves, ideal and ring class fields, and restate key lemmas from [4]. Section 3 proves the key decomposition lemma for $\mathscr{A}_{p^n,E}$, proves the minimal field of definition lemmas, and works through several examples. Section 4 includes our results on the minimal field of definition of certain singular K3 surfaces. The Appendix gives the exact field of definition and j-invariant computations we use in the examples.

Throughout this paper, by the *minimal field of definition* of the CM abelian surface $\mathscr{A}_{p^n,E}$ we mean the smallest number field F over which there exists a model of $\mathscr{A}_{p^n,E}$ together with a CM product decomposition with specified CM orders on the two factors. In our context this field coincides with the compositum $F = \mathbb{Q}(j(E), j(E_1), j(E_2))$, as described in Remark 3.2

Acknowledgments

I would like to thank my PRIMES mentor, Sheela Devadas, for her guidance and support throughout the PRIMES program. I would also like to thank the PRIMES organizers for the opportunity to conduct math research.

2 Background

2.1 CM theory of elliptic curves

This section follows the exposition of complex multiplication theory in [3, Chapter 14]. In this section we discuss CM theory which is used in our paper, such as the correspondence between elliptic curves and lattices

Theorem 2.1 ([3], Theorem 14.3)**.** *Every elliptic curve over $\mathbb{C}$ is analytically isomorphic to a complex torus $\mathbb{C}/\Lambda$, where $\Lambda \subset \mathbb{C}$ is a lattice. For every lattice Λ the complex torus $\mathbb{C}/\Lambda$ can be given a unique structure of an elliptic curve. Moreover, every elliptic curve arises in this way.*

Definition 2.2. If two elliptic curves $E_i = \mathbb{C}/\Lambda_i$ are isogenous, there exists a complex number α such that $\alpha\Lambda_1 \subseteq \Lambda_2$. In other words, isogeny is a homothety with a sublattice. The endomorphism ring of an elliptic curve $E = \mathbb{C}/\Lambda$ is the ring of its isogenies to itself. It is a subring of the complex numbers

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}.$$

Definition 2.3. An elliptic curve $E = \mathbb{C}/\Lambda$ has CM if its endomorphism ring $\operatorname{End}(E)$ is strictly larger than $\mathbb{Z}$. For E with CM, the ring $\operatorname{End}(E)$ is an order in an imaginary quadratic number field K [9, Theorem 10.2].

Definition 2.4. Any order $\mathscr{O} \subseteq K$ is equal to $\mathbb{Z} + f\mathscr{O}_K$ for some integer f; this f is the *conductor* of $\mathscr{O}$. For $\mathscr{O}, \mathscr{O}' \subseteq K$ we have $\mathscr{O} \subseteq \mathscr{O}'$ if and only if $f' \mid f$, where f' denotes the conductor of $\mathscr{O}'$.

2.2 Ring class fields and j-invariants

In this section we discuss some class field theory based on [3, Chapter 7], including the definition of the ring class field attached to an order and its relation to j-invariants via the First Main Theorem of CM.

Theorem 2.5 ([3, Theorem 7.7])**.** *Let $\mathscr{O}$ be the order of discriminant D in an imaginary quadratic field K.*

(i) If $f(x,y) = ax^2+bxy+cy^2$ is a primitive positive definite quadratic form of discriminant D, then $[a, \frac{-b+\sqrt{D}}{2}]$ is a proper ideal of $\mathscr{O}$.

(ii) The map sending $f(x,y)$ to $[a, \frac{-b+\sqrt{D}}{2}]$ induces an isomorphism between the form class group $\operatorname{Cl}(D)$ *and the* ideal class group $\operatorname{Cl}(\mathscr{O})$*. Consequently, the order of* $\operatorname{Cl}(\mathscr{O})$ *is the class number $h(D)$.*

(iii) A positive integer m is represented by a form $f(x,y)$ if and only if $m = N(\mathfrak{a})$ for some ideal $\mathfrak{a}$ in the corresponding ideal class in $\operatorname{Cl}(\mathscr{O})$*.*

Remark 2.6. The ideal class group $\operatorname{Cl}(\mathscr{O})$ parametrizes isomorphism classes of elliptic curves with CM by $\mathscr{O}$. This correspondence sends $[\Lambda] \in \operatorname{Cl}(\mathscr{O})$ to the isomorphism class $[\mathbb{C}/\Lambda]$ for an invertible ideal $\Lambda \subseteq \mathscr{O}$. We often refer to $[E]$ and $[\Lambda]$ interchangeably for an elliptic curve (and associated lattice) $E = \mathbb{C}/\Lambda$.

We can determine some information about a CM elliptic curve E from the element $[E] \in \operatorname{Cl}(\mathscr{O})$.

Remark 2.7. The j-invariant of a CM elliptic curve $j(E)$ is real exactly when $[E] \in \operatorname{Cl}(\mathscr{O})$ has order ≤ 2.

Definition 2.8. Let K be a number field and $\mathscr{O} \subseteq \mathscr{O}_K$ an order of conductor f. The *ring class field* $L_{\mathscr{O}}$ of $\mathscr{O}$ is the *unique* abelian extension of K whose conductor divides f and for which there is an isomorphism $\operatorname{Gal}(L_{\mathscr{O}}/K) \cong \operatorname{Cl}(\mathscr{O})$.

Remark 2.9. There is a canonical choice of isomorphism $\operatorname{Gal}(L_{\mathscr{O}}/K) \cong \operatorname{Cl}(\mathscr{O})$ which is discussed in [3].

The ring class field has a close relationship to j-invariants of elliptic curves with CM by $\mathscr{O}$.

Theorem 2.10 (First Main Theorem of Complex Multiplication)**.** *Let $\mathscr{O}$ be an order in an imaginary quadratic field K, and let I be a proper fractional $\mathscr{O}$-ideal. Then the j-invariant $j(I)$ is an algebraic integer and $K(j(I))$ is the ring class field of the order $\mathscr{O}$.*

Definition 2.11. The **Hilbert class polynomial** $H_{\mathscr{O}}(x)$ of order $\mathscr{O}$ in K, is the minimal polynomial over K, for the j-invariant of a CM elliptic curves with endomorphism ring $\mathrm{End}(E)$. In fact, $H_{\mathscr{O}}(x)$ is independent of E and lies in $\mathbb{Z}[x]$.

2.3 Previous work on fields of definition

In this subsection we recall certain useful lemmas from [4] relating the fields of definition for CM elliptic curves.

We first characterize the field extension generated by two distinct CM elliptic curves with the same CM order.

Lemma 2.12 ([4], Lemma 3.2.2)**.** *Let E_1, E_2 be two nonisomorphic complex elliptic curves with CM by $\mathscr{O}$, an order in an imaginary quadratic field K. Let $L_{\mathscr{O}}$ be the ring class field of $\mathscr{O}$, which is a degree $2n$ extension of $\mathbb{Q}$ for $n = |\mathrm{Cl}(\mathscr{O})|$. Then one of the following is true:*

(i) $\mathbb{Q}(j(E_1), j(E_2)) = L_{\mathscr{O}}$,

(ii) or $\mathbb{Q}(j(E_1)) = \mathbb{Q}(j(E_2))$ *is a degree n extension of $\mathbb{Q}$, and in $\mathrm{Cl}(\mathscr{O})$ the element $[E_1][E_2]^{-1}$ has order 2.*

We also must consider the case of elliptic curves E_i which have different CM orders in the same CM field K. For orders $\mathscr{O}' \subseteq \mathscr{O}$, there is a natural map $\phi : \mathrm{Cl}(\mathscr{O}') \longrightarrow \mathrm{Cl}(\mathscr{O})$ $\phi([\Gamma]) = [\mathscr{O}\Gamma]$). In fact ϕ is the usual extension-of-scalars map on invertible $\mathscr{O}'$-modules; see [4, Lemma 3.1.5].)

Lemma 2.13 ([4], Lemma 3.2.6)**.** *Let K be an imaginary quadratic number field with $\mathscr{O}_K = \mathbb{Z}[\alpha]$, and let $c \mid a$ be positive integers. Then if E is a complex elliptic curve with CM by $\mathbb{Z}[a\alpha]$, any elliptic curve E' corresponding to the class $\phi_{c,a,\alpha}([E]) \in \mathrm{Cl}(\mathbb{Z}[c\alpha])$ has $j(E') \in \mathbb{Q}(j(E))$.*

In addition to the previous lemmas from [4], it is useful to consider the field of definition $\mathbb{Q}(j(E))$ or $\mathbb{Q}(j(\Lambda))$ as a subfield of the ring class field.

Lemma 2.14. *If Λ and Λ' have CM by the same order $\mathscr{O}$, then the j-invariants $j(\Lambda)$ and $j(\Lambda')$ are conjugate algebraic integers lying in the ring class field of $\mathscr{O}$, and in particular, $\mathbb{Q}(j(\Lambda))$ and $\mathbb{Q}(j(\Lambda'))$ are Galois conjugate subfields of the ring class field of $\mathscr{O}$.*

Proof. By the Main Theorem of Complex Multiplication, the ring class field $H_{\mathscr{O}}$ is an abelian extension of K whose Galois group $\mathrm{Gal}(H_{\mathscr{O}}/K) \cong \mathrm{Cl}(\mathscr{O})$ acts transitively on the set of j-invariants of $\mathscr{O}$-lattices, and $j(\Lambda)$ generates $H_{\mathscr{O}}$ over K. Thus, there is some $\sigma \in \mathrm{Gal}(H_{\mathscr{O}}/K)$ with $\sigma(j(\Lambda)) = j(\Lambda')$.

Since $j(\Lambda)$ is a root of the Hilbert class polynomial of $\mathscr{O}$ (which has integer coefficients), it is an algebraic integer, and therefore so is its Galois conjugate $j(\Lambda')$. Also, σ induces an isomorphism of fields $\sigma : \mathbb{Q}(j(\Lambda)) \xrightarrow{\cong} \mathbb{Q}(j(\Lambda'))$ which shows that these two number fields are conjugate subfields of $H_{\mathscr{O}}$. □

2.4 Abelian surfaces of maximal Picard rank

In this subsection we produce a set of representatives for isomorphism classes of Picard-maximal abelian surfaces.

A complex abelian surface $\mathscr{A}$ of maximal Picard rank [8] is isomorphic to a product of isogenous CM elliptic curves [8]. However, this decomposition has some ambiguity:

Theorem 2.15 (Theorem 4.2.4,[4])**.** *For $E_i = \mathbb{C}/\Lambda_i, i = 1, \ldots, 4$ pairwise isogenous CM elliptic curves with CM by the imaginary quadratic field K, we have $E_1 \times E_2 \simeq E_3 \times E_4$ if and only if $\mathrm{End}(E_1) \cap \mathrm{End}(E_2) = \mathrm{End}(E_3) \cap \mathrm{End}(E_4)$ and $\Lambda_1\Lambda_2 \sim \Lambda_3\Lambda_4$.*

It follows that $E_1 \times E_2 \cong \mathbb{C}/\mathscr{O} \times \mathbb{C}/(\Lambda_1\Lambda_2)$ for $\mathscr{O} = \mathrm{End}(E_1) \cap \mathrm{End}(E_2)$.

Definition 2.16. Let E be a CM elliptic curve with $\mathrm{End}(E) = \mathbb{Z}[\alpha]$ an order in an imaginary quadratic number field. Then $\mathscr{A}_{d,E}$ is the complex abelian surface $\mathbb{C}/\mathscr{O} \times E$ where $\mathscr{O} = \mathbb{Z}[d\alpha]$.

By Theorem 2.15 we see that every complex abelian surface of maximal Picard rank is isomorphic to $\mathscr{A}_{d,E}$ for some d, E, and $\mathscr{A}_{d,E} \cong \mathscr{A}_{d',E'}$ if and only if $d = d', E \cong E'$.

Example 2.17 (Decompositions for $d = 2$, $E = \mathbb{C}/\langle 3, 1+i\rangle$)**.** Let $E = \mathbb{C}/\langle 3, 1+i\rangle$, so $\mathrm{End}(E) = \mathbb{Z}[3i]$ and $d = 2$. By definition,

$$\mathscr{A}_{2,E} = E \times \mathbb{C}/\mathbb{Z}[6i] = \mathbb{C}/\langle 3, 1+i\rangle \times \mathbb{C}/\langle 1, 6i\rangle.$$

We note from Table 1 that any elliptic curve with CM by $\mathbb{Z}[6i]$ is isomorphic to one of:

$$\mathbb{C}/\langle 1, 6i\rangle,\ \mathbb{C}/\langle 3, 2i\rangle,\ \mathbb{C}/\langle 3, 1+2i\rangle,\ \mathbb{C}/\langle 3, 1-2i\rangle.$$

By [4, Thm 4.2.4(ii)] we have isomorphisms

$$\mathscr{A}_{2,E} \cong \mathbb{C}/\langle 3, 1+i\rangle \times \mathbb{C}/\langle 3, 2i\rangle \cong \mathbb{C}/\langle 3, 1+i\rangle \times \mathbb{C}/\langle 3, 1+2i\rangle \cong \mathbb{C}/\langle 3, 1+i\rangle \times \mathbb{C}/\langle 3, 1-2i\rangle.$$

In fact, these are all possible unordered pairs of isomorphism classes of elliptic curves $([E_1], [E_2])$ such that $\mathscr{A}_{2,E} \cong E_1 \times E_2$. (There are of course infinitely many isomorphisms $\mathscr{A}_{2,E} \xrightarrow{\sim} E_1 \times E_2$ obtained by composing with automorphisms of the product.)

3 Prime-power conductor parameter: decompositions and fields of definition

In this section, we compute the minimal field of definition of the isomorphism class $\mathscr{A}_{d,E}$ where $d = p^n$ is a power of a prime.

Lemma 3.1. *Let $\mathscr{A}_{d,E}$ be as in Definition 2.16, and suppose $\mathscr{A}_{d,E} \cong E_1 \times E_2$ with E_1, E_2 CM elliptic curves. Then the number field*

$$\mathbb{Q}\big(j(E), j(E_1), j(E_2)\big)$$

is a field of definition for the triple $(\mathscr{A}_{d,E}, E_1, E_2)$, i.e. there exists a model of $\mathscr{A}_{d,E}$ over this field admitting a compatible product presentation by curves with those j-invariants. Moreover, the intrinsic decomposition field $L^{\mathrm{dec}}(\mathscr{A}_{d,E})$ is the intersection (equivalently, the minimum under inclusion) of these fields over all decompositions.

Remark 3.2. The field $L^{\mathrm{dec}}(\mathscr{A}_{d,E})$ is the smallest field over which the elliptic curve E can be defined *and* over which $\mathscr{A}_{d,E}$ admits a product model $E_1 \times E_2$. If instead one asks for a field over which the full algebra of self-isogenies $\mathrm{End}(\mathscr{A}_{d,E}) \otimes \mathbb{Q}$ is defined, one generally must adjoin the CM field K. In particular, $L^{\mathrm{dec}}(\mathscr{A}_{d,E})$ can be totally real, while K is imaginary quadratic. The field $L^{\mathrm{dec}}(\mathscr{A}_{d,E})$ is also generally larger than the usual notion of the "minimal field of definition" of $\mathscr{A}$, which we might take to be one of the number fields $\mathbb{Q}(j(E_1), j(E_2))$ which has minimal degree (among decompositions $\mathscr{A} \cong E_1 \times E_2$); the latter notion does not give a unique field.

3.1 Describing the decompositions

In this section, we prove a key lemma (Lemma 3.3) that describes how $\mathscr{A}_{p^n,E}$ can split as a product of two CM elliptic curves. That decomposition criterion is the foundation for our main theorems on minimal fields of definition. In particular, it is not generally the case that if $\mathscr{A}_{d,E} \cong E_1 \times E_2$ there is only one choice for $\mathrm{End}(E_1), \mathrm{End}(E_2)$.

Lemma 3.3. *Let K be an imaginary quadratic field and let $\mathscr{O} \subseteq \mathscr{O}_K$ be the order of conductor f. Suppose E is an elliptic curve with $\mathrm{End}(E) = \mathscr{O}$. Let $\mathscr{O}' \subseteq \mathscr{O}$ be the order of conductor $p^n f$ for a prime p, and let*

$$\phi : \mathrm{Cl}(\mathscr{O}') \to \mathrm{Cl}(\mathscr{O}), \qquad [\Gamma] \mapsto [\mathscr{O}\,\Gamma]$$

be the natural map.

Then $\mathscr{A}_{p^n,E} \simeq E_1 \times E_2$ if and only if, after possibly swapping E_1 and E_2, we have

$$\mathrm{End}(E_1) = \mathscr{O}, \qquad \mathrm{End}(E_2) = \mathscr{O}', \qquad [E_1] \cdot \phi([E_2]) = [E] \textit{ in } \mathrm{Cl}(\mathscr{O}).$$

Proof. Set $\mathscr{A} = \mathscr{A}_{p^n,E} = E \times (\mathbb{C}/\mathscr{O}')$ by definition and $\mathscr{O}_K = \mathbb{Z}[\beta]$.

If $\mathscr{A} \cong E_1 \times E_2$: write

$$E_i = \mathbb{C}/\Lambda_i, \quad \mathrm{End}(E_i) = \mathscr{O}_i \subseteq \mathscr{O}_K, i = 1, 2.$$

By Theorem 2.15 above, we have

$$\mathrm{lcm}(\mathrm{cond}(\mathscr{O}_1), \mathrm{cond}(\mathscr{O}_2)) = p^n f, \quad \mathrm{gcd}(\mathrm{cond}(\mathscr{O}_1), \mathrm{cond}(\mathscr{O}_2)) = f,$$

so writing each $\mathscr{O}_i = \mathbb{Z}[f_i\beta]$ forces $\{f_1, f_2\} = \{f, p^n f\}$. Without loss of generality, let

$$\mathrm{End}(E_1) = \mathscr{O} = \mathbb{Z}[f\beta], \qquad \mathrm{End}(E_2) = \mathscr{O}' = \mathbb{Z}[p^n f\beta].$$

Again by Theorem 2.15, the lattice product $\Lambda_1\Lambda_2 \subset \mathbb{C}$ is homothetic to the lattice of E. By the definition of ϕ we have $\phi([\Lambda_2]) = [\mathscr{O}\Lambda_2]$. Furthermore

$$[\Lambda_1(\mathscr{O}\Lambda_2)] = [\Lambda_1][\mathscr{O}\Lambda_2]$$

by [4, Lemma 3.1.4]. It follow that in the class group of $\mathscr{O}$ we have

$$[\Lambda_1\Lambda_2] = [\Lambda_1]\phi([\Lambda_2]).$$

Since $[\Lambda_1\Lambda_2] = [E]$, we have

$$[E_1]\phi([E_2]) = [E] \in \mathrm{Cl}(\mathscr{O}).$$

This proves that if $\mathscr{A}_{p^n,E} \cong E_1 \times E_2$ then the E_i satisfy the desired conditions.

Conversely, if E_1, E_2 satisfy $\mathrm{End}(E_1) = \mathscr{O}$, $\mathrm{End}(E_2) = \mathscr{O}'$ and

$$[E_1]\phi([E_2]) = [E],$$

then $\Lambda_1\Lambda_2$ is homothetic to the lattice of E, and by [4, Thm.4.2.4(ii)] again we get

$$E_1 \times E_2 \simeq \mathbb{C}/(\Lambda_1\Lambda_2) \times \mathbb{C}/\mathscr{O}' = \mathbb{C}/\mathscr{O}' \times E \simeq \mathscr{A}.$$

This completes the proof. □

The above lemma gives exactly the class-group criteria for when the conductor is a prime power. This is an extension of [4, Proposition 4.2.6].

Example 3.4. Consider the abelian surface $A_{4,E}$ for $E = \mathbb{C}/\mathbb{Z}[2i]$. By Lemma 3.3, if $A_{4,E} \simeq E_1 \times E_2$ then the E_i satisfy

$$\mathrm{End}(E_1) = \mathbb{Z}[2i], \qquad \mathrm{End}(E_2) = \mathbb{Z}[8i], \qquad [E_1]\phi([E_2]) = [E] = [\mathbb{C}/\mathbb{Z}[2i]] \in \mathrm{Cl}(\mathbb{Z}[2i]),$$

where

$$\phi : \mathrm{Cl}(\mathbb{Z}[8i]) \longrightarrow \mathrm{Cl}(\mathbb{Z}[2i])$$

is the natural map induced by the inclusion $\mathbb{Z}[8i] \subset \mathbb{Z}[2i]$.

Example 3.5. If d is composite then there are multiple choices for $\mathrm{End}(E_1), \mathrm{End}(E_2)$ (assuming $\mathscr{A}_{d,E} \cong E_1 \times E_2$). For example,

$$\mathscr{A}_{6,\mathbb{Z}[i]} \cong \mathbb{Z}[i] \times \mathbb{Z}[6i] \cong \mathbb{Z}[2i] \times \mathbb{Z}[3i].$$

We now produce a lower bound on the degree of the minimal field of definition.

Proposition 3.6. *Let $E, p^n, \mathscr{O}, \mathscr{O}'$ be as in Lemma 3.3. For a decomposition $\mathscr{A}_{p^n,E} \cong E_1 \times E_2$, the degree of the extension $\mathbb{Q}(j(E), j(E_1), j(E_2))$ over $\mathbb{Q}$ is at least $|Cl(\mathscr{O}')|$.*

Proof. Follows from Lemma 3.3 and the fact that the minimal polynomial of the j-invariant of E with CM by $\mathscr{O}'$ is $H_{\mathscr{O}'}(X) \in \mathbb{Z}[X]$, the *Hilbert class polynomial*, which has degree $|\mathrm{Cl}(\mathscr{O}')|$. □

3.2 Main results

We now can characterize the minimal field of definition of $\mathscr{A}_{p^n,E}$ for CM E with real j-invariant. In fact the lower bound on the degree of the minimal field of definition given in Proposition 3.6 is achieved in this case.

Theorem 3.7. *Let E be a CM elliptic curve with $\mathrm{End}(E) = \mathscr{O}$ and let $\mathscr{O}'$ be the order of conductor $p^n \cdot \mathrm{cond}(\mathscr{O})$ in the same imaginary quadratic field K. Let $L_{\mathscr{O}'}$ be the ring class field of $\mathscr{O}'$.*

If $j(E) \in \mathbb{R}$, so $[E] \in \mathrm{Cl}(\mathscr{O})$ has order ≤ 2, then there exist CM elliptic curves E_1, E_2 with $\mathrm{End}(E_i) = \mathscr{O}$ such that $\mathscr{A}_{p^n,E} \simeq E_1 \times E_2$ and

$$\big[\mathbb{Q}\big(j(E), j(E_1), j(E_2)\big) : \mathbb{Q}\big] = \big|\mathrm{Cl}(\mathscr{O}')\big| = \tfrac{1}{2}\big[L_{\mathscr{O}'} : \mathbb{Q}\big].$$

Proof. We assume $[E] \in \mathrm{Cl}(\mathscr{O})$ has order ≤ 2. Let

$$E_1 = E, \qquad E_2 = \mathbb{C}/\mathscr{O}'$$

By definition, we have $\mathscr{A}_{p^n,E} \simeq E_1 \times E_2$. Hence

$$\mathbb{Q}(j(E), j(E_1), j(E_2)) = \mathbb{Q}(j(E), j(\mathbb{C}/\mathscr{O}')).$$

We have that $\phi([E_2]) = [\mathbb{C}/\mathscr{O}]$. Therefore, by [4, Lemma 3.2.6], we have $\mathbb{Q}(j(E_2)) = \mathbb{Q}(j(\mathbb{C}/\mathscr{O}')) \supseteq \mathbb{Q}(j(\mathbb{C}/\mathscr{O}))$. Furthermore, since the identity element of $\mathrm{Cl}(\mathscr{O})$ is $[\mathbb{C}/\mathscr{O}]$, we see that $[E][\mathbb{C}/\mathscr{O}]^{-1} = [E] \in \mathrm{Cl}(\mathscr{O})$ has order ≤ 2. Therefore, by [4, Lemma 3.2.2] we have $\mathbb{Q}(j(E)) = \mathbb{Q}(j(\mathbb{C}/\mathscr{O}))$. Therefore:

$$\mathbb{Q}(j(E), j(\mathbb{C}/\mathscr{O}')) = \mathbb{Q}(j(\mathbb{C}/\mathscr{O}')) \quad (\text{since } j(E) \in \mathbb{Q}(j(\mathbb{C}/\mathscr{O})) \subseteq \mathbb{Q}(j(\mathbb{C}/\mathscr{O}'))).$$

We have

$$[\mathbb{Q}(j(\mathbb{C}/\mathscr{O}')) : \mathbb{Q}] = |\mathrm{Cl}(\mathscr{O}')| = \frac{1}{2}[L_{\mathscr{O}'} : \mathbb{Q}]$$

since $j(\mathbb{C}/\mathscr{O}')$ has minimal polynomial equal to the *Hilbert class polynomial* $H_{\mathscr{O}'}(X) \in \mathbb{Z}[X]$ which has degree $|\mathrm{Cl}(\mathscr{O}')|$. Furthermore, $[\mathbb{C}/\mathscr{O}']$ is the identity element of $\mathrm{Cl}(\mathscr{O}')$, so $j(\mathbb{C}/\mathscr{O}') \in \mathbb{R}$. Then by Lemma 2.14 we see that $\mathbb{Q}(j(\mathbb{C}/\mathscr{O}'))$ is the real subfield of $L_{ord'}$. □

If E does not have real j-invariant, so $[E] \in \mathrm{Cl}(\mathscr{O})$ has order greater than 2, then our lower bound on the degree of the minimal field of definition is not achieved; the minimal field of definition is the ring class field of $\mathscr{O}'$.

Theorem 3.8. *Let $E, \mathscr{O}, p^n, \mathscr{O}'$ be as in Theorem 3.7. If $[E] \in \mathrm{Cl}(\mathscr{O})$ has order > 2, then for* any *decomposition*

$$\mathscr{A}_{p^n,E} \simeq E_1 \times E_2$$

one has $\mathbb{Q}(j(E), j(E_1), j(E_2)) = L_{\mathscr{O}'}$, so

$$[\mathbb{Q}(j(E), j(E_1), j(E_2))\colon \mathbb{Q}] = 2|\mathrm{Cl}(\mathscr{O}')| = [L_{\mathscr{O}'}\colon \mathbb{Q}].$$

Proof. Assume $[E] \in \mathrm{Cl}(\mathscr{O})$ has order > 2. By Lemma 3.3, if $\mathscr{A}_{p^n,E} \simeq E_1 \times E_2$, we must have $\mathrm{End}(E_1) = \mathscr{O}$ and $\mathrm{End}(E_2) = \mathscr{O}'$, and $[E_1]\phi([E_2]) = [E] \in \mathrm{Cl}(\mathscr{O})$ for the natural map $\phi\colon \mathrm{Cl}(\mathscr{O}') \to \mathrm{Cl}(\mathscr{O})$.

We consider now the field $\mathbb{Q}(j(E), j(E_1), j(E_2))$.

By [4, Lemma 3.2.2], either

(a) $[E][E_1]^{-1}$ has order > 2 and $\mathbb{Q}(j(E), j(E_1)) = L_{\mathscr{O}}$, the ring class field of $\mathscr{O}$,

(b) or $[E][E_1]^{-1}$ has order ≤ 2 and $\mathbb{Q}(j(E)) = \mathbb{Q}(j(E_1))$.

We will handle these cases separately. Note that $[E][E_1]^{-1} = \phi([E_2])$.

(a) Assume $[E][E_1]^{-1} = \phi([E_2])$ has order > 2 and $\mathbb{Q}(j(E), j(E_1)) = L_{\mathscr{O}}$, the ring class field of $\mathscr{O}$.

By the first main theorem of complex multiplication, $L_{\mathscr{O}} = K(j(E)) = K(j(E_1))$ and $L_{\mathscr{O}'} = K(j(E_2))$ since E, E_1 have CM by $\mathscr{O}$ and E_2 has CM by $\mathscr{O}'$.

Since

$$K(j(E_1)) = L_{\mathscr{O}} \subseteq \mathbb{Q}(j(E), j(E_1), j(E_2)) \subseteq K(j(E_2)) = L_{\mathscr{O}'},$$

Galois theory forces $\mathbb{Q}(j(E), j(E_1), j(E_2)) = L_{\mathscr{O}'}$.

(b) Assume $[E][E_1]^{-1} = \phi([E_2])$ has order ≤ 2 and $\mathbb{Q}(j(E)) = \mathbb{Q}(j(E_1))$. Fix some elliptic curve $E_{2,\phi}$ with $[E_{2,\phi}] = \phi([E_2]) \in \mathrm{Cl}(\mathscr{O})$. We now compare $\mathbb{Q}(j(E_{2,\phi}))$ and $\mathbb{Q}(j(E))$. To do so we will consider the group element $[E][E_{2,\phi}]^{-1} = [E]\phi([E_2])^{-1}$.

If $[E][E_{2,\phi}]^{-1}$ has order ≤ 2, then so does

$$[E][E_{2,\phi}]^{-1}\phi([E_2]) = [E][E_{2,\phi}]^{-1}[E_{2,\phi}] = [E],$$

giving a contradiction. Hence $[E][E_{2,\phi}]^{-1}$ has order > 2 and by [4, Lemma 3.2.2] we obtain

$$\mathbb{Q}(j(E), j(E_{2,\phi})) = L_{\mathscr{O}}$$

the ring class field of $\mathscr{O}$.

By [4, Lemma 3.2.6] we have $\mathbb{Q}(j(E_{2,\phi})) \subseteq \mathbb{Q}(j(E_2))$. Therefore

$$\mathbb{Q}(j(E), j(E_{2,\phi})) = L_{\mathscr{O}} \subseteq \mathbb{Q}(j(E), j(E_2)).$$

Hence $L_{\mathscr{O}} = K(j(E)) \subseteq \mathbb{Q}(j(E), j(E_2))$. It follows that

$$K(j(E_2)) \subseteq \mathbb{Q}(j(E), j(E_2)) \subseteq \mathbb{Q}(j(E), j(E_1), j(E_2)) \subseteq L_{\mathscr{O}'}.$$

Thus $\mathbb{Q}(j(E), j(E_1), j(E_2)) = L_{\mathscr{O}}$.

Thus in both subcases a) and b),

$$\mathbb{Q}(j(E), j(E_1), j(E_2)) : \mathbb{Q} = 2|\mathrm{Cl}(\mathscr{O}')| = [L_{\mathscr{O}'} : \mathbb{Q}]$$

□

Example 3.9. Let

$$E = \mathbb{C}/\langle 3, 2i\rangle, \quad \mathrm{End}(E) = \mathbb{Z}[6i],$$

so $[E]$ has order 2 in $\mathrm{Cl}(\mathbb{Z}[6i])$. We also note from Table 1 that $j(E) \in \mathbb{R}$.

In the first row of Table 3 we can find a decomposition

$$\mathscr{A}_{2,E} \simeq E_1 \times E_2 \quad \text{with} \quad E_1 = \mathbb{C}/\langle 1, 6i\rangle, E_2 = \mathbb{C}/\langle 3, 1+2i\rangle,$$

and indeed $\mathrm{End}(E_i) = \mathbb{Z}[6i]$ for $i = 1, 2$. Then

$$\mathbb{Q}(j(E), j(E_1), j(E_2)) = \mathbb{Q}(\sqrt{2}, \sqrt[4]{3}), \quad [\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}) : \mathbb{Q}] = 8 = |\mathrm{Cl}(\mathbb{Z}[12i])|$$

as we would expect given Theorem 3.7.

The full ring class field $L_{\mathbb{Z}[12i]}$ satisfies

$$[L_{\mathbb{Z}[12i]} : \mathbb{Q}] = 2 \cdot |\mathrm{Cl}(\mathbb{Z}[12i])| = 16$$

which is strictly larger than the degree of $\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$ over $\mathbb{Q}$.

Example 3.10. Let $K = \mathbb{Q}(i)$ and $\mathscr{O} = \mathbb{Z}[6i] \subset \mathscr{O}_K$, so that $\mathrm{Cl}(\mathscr{O}) \cong \mathbb{Z}/4\mathbb{Z}$, and choose $E = \mathbb{C}/\Lambda, \quad \Lambda = \langle 3, 1-2i\rangle$, whose class has order 4 in $\mathrm{Cl}(\mathbb{Z}[6i])$ (Table 1). Then one computes

$$\mathrm{cond}(\mathscr{O}) = 6, \qquad \mathscr{O}' = \text{order of conductor } 12 = \mathbb{Z}[12i],$$

and

$$L_{\mathscr{O}'} = K(\sqrt{2}, \sqrt[4]{3}), \quad [L_{\mathscr{O}'} : \mathbb{Q}] = 16, \quad |\mathrm{Cl}(\mathscr{O}')| = 8.$$

For any decomposition (these are in the second half of Table 3)

$$\mathscr{A}_{2,E} \simeq E_1 \times E_2 \quad (\mathrm{End}(E_i) = \mathbb{Z}[6i]),$$

one then checks

$$\mathbb{Q}(j(E), j(E_1), j(E_2)) = L_{\mathscr{O}'}, \quad [L_{\mathscr{O}'} : \mathbb{Q}] = 16 = 2|\mathrm{Cl}(\mathscr{O}')|.$$

This illustrates Theorem 3.8 since E has order > 2 in $\mathrm{Cl}(\mathscr{O})$, every splitting yields the full ring class field $L_{\mathscr{O}'}$.

Theorem 3.11. *Let $E, \mathscr{O}, p^n, \mathscr{O}'$ be as in Theorem 3.7. Let $G = \mathrm{Cl}(\mathscr{O})$. Assume that*

$$[E] \in G^2 \cdot G[2]$$

that is, there exist elliptic curves E', E'' with $\mathrm{End}(E') = \mathrm{End}(E'') = \mathscr{O}$ and

$$[E] = [E']^2 \cdot [E''], \qquad [E'']^2 = 1 \text{ in } \mathrm{Cl}(\mathscr{O}).$$

Then there exists a decomposition

$$\mathscr{A}_{p^n,E} \simeq E_1 \times E_2$$

such that

$$[\mathbb{Q}(j(E_1), j(E_2)) : \mathbb{Q}] = |\mathrm{Cl}(\mathscr{O}')|.$$

Remark 3.12. Compared with Theorems 3.7 and 3.8, Theorem 3.11 differs in both hypothesis and target field. First, instead of splitting by whether $[E] \in \mathrm{Cl}(\mathscr{O})$ has order ≤ 2 (equivalently $j(E) \in \mathbb{R}$) or > 2, it assumes the *square* condition $[E] = [E']^2$, which is independent of whether $j(E)$ is real (e.g. elements of order 4 can be squares). Second, while Theorems 3.7–3.8 determine when $\mathbb{Q}\big(j(E), j(E_1), j(E_2)\big)$ is minimized, Theorem 3.11 etermines when the smaller field $\mathbb{Q}\big(j(E_1), j(E_2)\big)$ has minimal degree $|\mathrm{Cl}(\mathscr{O}')|$.

Proof. Let $\mathrm{End}(E) = \mathscr{O} = \mathbb{Z}[f\alpha] \subset K = \mathbb{Q}[\alpha]$ and‘ let $\mathscr{O}' = \mathbb{Z}[p^n f\,\alpha]$ be the order of conductor $p^n f$. The natural map

$$\phi : \mathrm{Cl}(\mathscr{O}') \longrightarrow \mathrm{Cl}(\mathscr{O}), \qquad [\Gamma] \mapsto [\mathscr{O}\Gamma],$$

is surjective: under the CM isomorphisms $\mathrm{Cl}(\mathscr{O}) \cong \mathrm{Gal}(L_{\mathscr{O}}/K)$ and $\mathrm{Cl}(\mathscr{O}') \cong \mathrm{Gal}(L_{\mathscr{O}'}/K)$ (with $L_{\mathscr{O}} \subset L_{\mathscr{O}'}$ the corresponding ring class fields), this map is the restriction morphism $\mathrm{Gal}(L_{\mathscr{O}'}/K) \twoheadrightarrow \mathrm{Gal}(L_{\mathscr{O}}/K)$, hence surjective (see [4, Prop. 3.2.5]).

Assume now that $[E]$ is a square in $\mathrm{Cl}(\mathscr{O})$, say $[E] = [E']^2$ for some elliptic curve E' with $\mathrm{End}(E') = \mathscr{O}$. By surjectivity of ϕ, choose $[E_2] \in \mathrm{Cl}(\mathscr{O}')$ with $\phi([E_2]) = [E']$, and let E_2

be a CM elliptic curve representing this class. Then $[E'] \cdot \phi([E_2]) = [E'] \cdot [E'] = [E]$, and Lemma 3.3 gives an isomorphism $\mathscr{A}_{p^n,E} \cong E' \times E_2$.

To compute the field of definition, apply [4, Lemma 3.2.6] since $\phi([E_2]) = [E']$ it follows that $j(E') \in \mathbb{Q}(j(E_2))$. Thus $\mathbb{Q}(j(E'), j(E_2)) = \mathbb{Q}(j(E_2))$.

Since E_2 has CM by $\mathscr{O}'$, the minimal polynomial of its j-invariant is the Hilbert class polynomial $H_{\mathscr{O}'}(X) \in \mathbb{Z}[X]$, which is irreducible of degree $|\mathrm{Cl}(\mathscr{O}')|$. Therefore

$$\mathbb{Q}(j(E_1), j(E_2)) : \mathbb{Q}] = [\mathbb{Q}(j(E_2)) : \mathbb{Q}] = |\mathrm{Cl}(\mathscr{O}')|.$$

□

Example 3.13. Let $G = \mathbb{Z}/6\mathbb{Z}$. By the Chinese Remainder Theorem, $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. We compute

$$G^2 = \{0, 2, 4\}, \qquad G[2] = \{0, 3\}.$$

$$G^2 \cdot G[2] = \{0, 2, 4\} + \{0, 3\} = \{0, 1, 2, 3, 4, 5\} = G,$$

while $G^2 \neq G$. In particular, elements such as $3 \in G$ are not squares but lie in $G^2 \cdot G[2]$. This shows that the hypothesis

$$[E] \in \mathrm{Cl}(\mathscr{O})^2 \cdot \mathrm{Cl}(\mathscr{O})[2]$$

in Theorem 3.11 is strictly weaker than requiring $[E]$ to be a square.

Example 3.14 (CM realization)**.** Let $\mathscr{O} = \mathbb{Z}[9i]$. One computes (see Appendix 4)

$$\mathrm{Cl}(\mathscr{O}) \cong \mathbb{Z}/6\mathbb{Z}.$$

Let $\Lambda = \langle 9,\ 1 + i \rangle$, whose class corresponds to $3 \in \mathbb{Z}/6\mathbb{Z}$. Then $[\Lambda]$ is not a square in $\mathrm{Cl}(\mathscr{O})$, but lies in $\mathrm{Cl}(\mathscr{O})^2 \cdot \mathrm{Cl}(\mathscr{O})[2]$.

Let $E = \mathbb{C}/\Lambda$. For any prime power p^n, Theorem 3.11 applies and yields a decomposition

$$\mathscr{A}_{p^n,E} \simeq \mathbb{C}/\mathbb{Z}[p^n \cdot 9\, i] \times \mathbb{C}/\Lambda.$$

Moreover, the field of definition of this decomposition is the real subfield of the ring class field of conductor $p^n \cdot 9$.

3.3 Abelian surfaces with more kinds of decompositions

Remark 3.15. In the prime-power case $d = p^n$, Theorems 3.7 and 3.8 show that the minimal field of definition of $\mathscr{A}_{p^n,E}$ is either the real subfield of the ring class field or the full ring class field of conductor $p^n \cdot \mathrm{cond}(\mathrm{End}(E))$. When d is not a prime power, however (for example, $d = 6 = 2 \cdot 3$), the two prime factors interact to produce minimal fields of definition outside that pattern (see also Example 3.5).

If E is a CM elliptic curve with $\mathrm{End}(E) = \mathscr{O}$, then splitting $\mathscr{A}_{6,E}$ into curves of conductors 2 and 3 can give

$$\mathbb{Q}(j(E_1), j(E_2)) = \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

the compositum of two prime-power subfields. Other decompositions give fourth-root fields such as $\mathbb{Q}(\sqrt[4]{12})$ or $\mathbb{Q}(i\sqrt[4]{12})$, showing that the primes 2 and 3 interact in an essential way. These mixed and hybrid-root extensions cannot occur when d is a prime power.

Example 3.16. Let

$$E = \mathbb{C}/\langle 3, 1-2i\rangle, \qquad \mathrm{End}(E) = \mathbb{Z}[6i].$$

We can find the decomposition

$$\mathscr{A}_{6,E} \simeq \mathbb{C}/\mathbb{Z}[i] \times \mathbb{C}/\langle 3, 2i\rangle,$$

and check that its minimal field of definition is $\mathbb{Q}(\sqrt[4]{12})$. Neither the real subfield nor the full ring class field of conductor 6 contains this extension, so it lies outside the prime-power framework.

4 Field of definition of a singular K3 surface

In this section we discuss the classification of Picard-maximal abelian surfaces and singular K3 surfaces via quadratic forms given by [7] and [8].

4.1 From intersection forms to $\mathscr{A}_{m,E}$ and back

We record a concrete dictionary between the intersection–form description of singular abelian surfaces and our conductor–product description $\mathscr{A}_{m,E}$.

Definition 4.1 (Intersection form and CM parameters)**.** Let

$$Q = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}, \qquad d(Q) = b^2 - 4ac < 0, \qquad K = \mathbb{Q}(\sqrt{d(Q)}).$$

Define

$$\tau_1 = \frac{-b + \sqrt{d(Q)}}{2a}, \qquad \tau_2 = \frac{b + \sqrt{d(Q)}}{2}.$$

We write $E_\tau = \mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})$ where $a, b, c \in \mathbb{Z}$ with $a > 0$ and Q positive definite (so $d(Q) < 0$).

Remark 4.2. Note that $\tau_2 = -a\overline{\tau_1}$. In fact τ_1 (and $\overline{\tau_1}$) have minimal polynomial $ax^2 + bx + c$. Thus we compute

$$\tau_2^2 - b\tau_2 + ac = a^2\overline{\tau_1}^2 + ab\overline{\tau_1} + ac = a(a\overline{\tau_1}^2 + b\overline{\tau_1} + c) = 0.$$

We then see that τ_2 is a root of the polynomial $x^2 - bx + ac$, and so is an algebraic integer. More specifically, this means $\tau_2(\mathbb{Z}+\mathbb{Z}\tau_2) \subseteq \mathbb{Z}+\mathbb{Z}\tau_2$ because $\tau_2^2 \in \mathbb{Z}+\mathbb{Z}\tau_2$; hence $\mathbb{Z}+\mathbb{Z}\tau_2 = \mathrm{End}(E_{\tau_2})$ is an order in K. We can find its conductor by comparing $d(Q)$ and the discriminant of $\mathscr{O}_K$.

Proposition 4.3 (Shioda–Mitani / Schütt [8, Thm. 4.1], [6, Prop. 10, Cor. 12])**.** *With Q and τ_i as above, the product*

$$A = E_{\tau_1} \times E_{\tau_2}$$

is a complex abelian surface of maximal Picard rank whose transcendental lattice $T(A)$ has intersection form Q. The associated Kummer surface $\mathrm{Kum}(A)$ *is a singular K3 surface whose transcendental lattice $T(\mathrm{Kum}(A))$ has intersection form $2Q$.*

Remark 4.4. If an abelian surface A is defined over a field F, then the associated Kummer surface $\mathrm{Kum}(A)$ is also defined over F. Indeed, the blow-up of A along the finite flat group scheme $A[2]$ and the quotient by the involution $x \mapsto -x$ are constructions over F.

In particular, if $A = E_{\tau_1} \times E_{\tau_2}$ is defined over $\mathbb{Q}\big(j(\tau_1), j(\tau_2)\big)$, then $\mathrm{Kum}(A)$ admits a model over the same field. The explicit CM expressions for $j(\tau_1)$ and $j(\tau_2)$ will be used later to determine minimal fields of definition.

Remark 4.5. Note $d(2Q) = (2b)^2 - 4(2a)(2c) = 4\,d(Q)$, so $\sqrt{d(2Q)} = 2\sqrt{d(Q)}$; this gives the identities for ρ_i above.

Proposition 4.6 (Translation to $\mathscr{A}_{m,E}$)**.** *Fix a CM elliptic curve E with* $\mathrm{End}(E) = \mathscr{O} = \mathbb{Z}[f\alpha] \subset K$ *(conductor f). For $m \in \mathbb{Z}_{>0}$ let $\mathscr{O}' = \mathbb{Z}[mf\,\alpha]$. Then if $E' = \mathbb{C}/\mathscr{O}'$ we have*

$$\mathscr{A}_{m,E} \;\cong\; E \times E' \qquad [E] \;=\; [E]\cdot\phi([E']) \;\; in \;\; \mathrm{Cl}(\mathscr{O}),$$

where $\phi : \mathrm{Cl}(\mathscr{O}') \to \mathrm{Cl}(\mathscr{O})$ is the natural map $[\Gamma] \mapsto [\mathscr{O}\Gamma]$. The intersection form Q of $\mathscr{A}_{m,E}$ (see Proposition 4.3) is equal to mQ_E for Q_E the quadratic form associated to the isomorphism class $[E] \in \mathrm{Cl}(\mathscr{O})$ (see Theorem 2.5).

Conversely, given an intersection form Q, one recovers $m = \gcd(a,b,c)$ and $E \cong \mathbb{C}/\langle 1, \tau_1\rangle$ up to isomorphism, and thus $\mathscr{A}_{m,E}$. (Compare [6, §6] and [4, Thm. 4.2.4].)

Proof of Proposition 4.6. Let Q_E be the primitive positive–definite binary quadratic form attached to $[E] \in \mathrm{Cl}(\mathscr{O})$ via Cox's form/ideal dictionary [3, Thm. 7.7].

Consider the product $E \times E'$, where $E' = \mathbb{C}/\mathscr{O}'$. Then $E \cong E_{\tau_1}$ and $E' \cong E_{\tau_2}$ (see Remark 4.2 for the second isomorphism), where τ_1, τ_2 are as in the Shioda–Mitani classification of singular abelian surfaces [8, Thm. 4.1] (cf. [6, §6]). Under this correspondence, the transcendental lattice of $E \times E'$ has intersection form mQ_E.

Hence the intersection form of $\mathscr{A}_{m,E}$ is $Q(\mathscr{A}_{m,E}) = mQ_E$.

Conversely, let A be a singular abelian surface with intersection form

$$Q = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}.$$

Set $m = \gcd(a,b,c)$ and $Q_E = \frac{1}{m}Q$, which is primitive. With $\tau_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}$ one has $E \cong \mathbb{C}/\langle 1, \tau_1\rangle$. By the Shioda–Mitani classification [8, Thm. 4.1], the surface A is isomorphic to

$$E_{\tau_1} \times E_{\tau_2}$$

for a suitable τ_2, and hence $A \cong E \times E'$ with $\mathrm{End}(E') = \mathscr{O}' = \mathbb{Z}[mf\,\alpha]$. Thus $A \cong \mathscr{A}_{m,E}$. □

Proposition 4.7. *[6] For a singular K3 surface X with intersection form Q having degree of primitivity m, X has a model over the field $\mathbb{Q}(j(E), j(\mathbb{Z}+m\mathscr{O}))$ for $E = \mathbb{C}/\Lambda$ an elliptic curve attached to the* primitive *form $\frac{1}{m}Q$ via Cox's form/ideal dictionary [3, Thm. 7.7] and $\mathscr{O} = \mathrm{End}(E)$, so $\mathscr{O}' = \mathbb{Z}+m\mathscr{O}$ is the order with discriminant* $\mathrm{disc}(Q)$.

If $2 \mid m$, then X has a model over the field $\mathbb{Q}(j(E), j(\mathbb{Z}+\frac{m}{2}\mathscr{O}))$.

Proof. This is [6, Prop. 10], restated in terms of $E, \mathscr{O}$ via Proposition 4.6. If $2 \mid m$, then by [7, Theorem 4] $X \cong \mathrm{Kum}(\mathscr{A})$ for the abelian surface $\mathscr{A}$ associated to $\frac{1}{2}Q$ by [8, Theorem 6]. Then $\mathrm{Kum}(\mathscr{A})$ has a model over $\mathbb{Q}(j(E), j(\mathbb{Z}+\frac{m}{2}\mathscr{O}))$ by [6, Cor. 12]. □

Theorem 4.8. *Let X be a singular K3 surface with intersection form Q having degree of primitivity m, and let $E = \mathbb{C}/\Lambda$ an elliptic curve attached to the* primitive *form $\frac{1}{m}Q$ via Cox's form/ideal dictionary [3, Thm. 7.7], with $\mathscr{O} = \mathrm{End}(E)$. If $[E]^2 = 1 \in \mathrm{Cl}(\mathrm{End}(E))$, then X has a model over a field L with degree $|\mathrm{Cl}(\mathbb{Z}+m\mathscr{O})|$ over $\mathbb{Q}$.*

If $2 \mid m$, then if $[E]^2 = 1 \in \mathrm{Cl}(\mathrm{End}(E))$, then X has a model over a field L with degree $|\mathrm{Cl}(\mathbb{Z}+\frac{m}{2}\mathscr{O})|$ over $\mathbb{Q}$.

Proof. Let $\mathscr{O} = \mathrm{End}(E)$, and set $\mathscr{O}' = \mathbb{Z}+m\mathscr{O}$. By Proposition 4.7 (Schutt), the K3 surface X admits a model over $F := \mathbb{Q}\big(j(E),\, j(\mathbb{Z}+m\mathscr{O})\big) = \mathbb{Q}\big(j(E),\, j(\mathbb{C}/\mathscr{O}')\big)$.

Assume now that $[E]^2 = 1 \in \mathrm{Cl}(\mathscr{O})$. Then $[E]$ has order ≤ 2 in $\mathrm{Cl}(\mathscr{O})$. Let $E_0 = \mathbb{C}/\mathscr{O}$ (the identity class in $\mathrm{Cl}(\mathscr{O})$). Since $[E]\,[E_0]^{-1} = [E]$ has order ≤ 2, Lemma 3.2.2 of [4] (equivalently, the argument used in the proof of Theorem 3.7) implies

$$\mathbb{Q}\big(j(E)\big) = \mathbb{Q}\big(j(E_0)\big) = \mathbb{Q}\big(j(\mathbb{C}/\mathscr{O})\big).$$

Next, we apply Lemma 3.2.6 of [4] to the inclusion $\mathscr{O}' \subseteq \mathscr{O}$ and the curve $\mathbb{C}/\mathscr{O}'$: since the natural map $\phi : \mathrm{Cl}(\mathscr{O}') \to \mathrm{Cl}(\mathscr{O})$ sends $[\mathbb{C}/\mathscr{O}']$ to $[\mathbb{C}/\mathscr{O}]$, we obtain $j(\mathbb{C}/\mathscr{O}) \in \mathbb{Q}\big(j(\mathbb{C}/\mathscr{O}')\big)$.

Therefore $j(E) \in \mathbb{Q}\big(j(\mathbb{C}/\mathscr{O})\big) \subseteq \mathbb{Q}\big(j(\mathbb{C}/\mathscr{O}')\big)$, and hence $F = \mathbb{Q}\big(j(\mathbb{C}/\mathscr{O}')\big)$.

Since $\mathbb{C}/\mathscr{O}'$ has CM by $\mathscr{O}'$, the minimal polynomial of the j-invariant $j(\mathbb{C}/\mathscr{O}')$ is the Hilbert class polynomial $H_{\mathscr{O}'}(X) \in \mathbb{Z}[X]$, which has degree $|\mathrm{Cl}(\mathscr{O}')|$. Consequently, $[F : \mathbb{Q}] = \big[\mathbb{Q}\big(j(\mathbb{C}/\mathscr{O}')\big) : \mathbb{Q}\big] = |\mathrm{Cl}(\mathscr{O}')| = |\mathrm{Cl}(\mathbb{Z}+m\mathscr{O})|$. This proves the first claim.

If $2 \mid m$, set $\mathscr{O}'' = \mathbb{Z}+\frac{m}{2}\mathscr{O}$. By Proposition 4.7, X admits a model over $F' = \mathbb{Q}\big(j(E),\, j(\mathbb{Z}+\frac{m}{2}\mathscr{O})\big) = \mathbb{Q}\big(j(E),\, j(\mathbb{C}/\mathscr{O}'')\big)$.

The same argument (using again $[E]^2 = 1$) shows that $j(E) \in \mathbb{Q}(j(\mathbb{C}/\mathscr{O}''))$, so $F' = \mathbb{Q}(j(\mathbb{C}/\mathscr{O}''))$ and therefore $[F' : \mathbb{Q}] = |\mathrm{Cl}(\mathscr{O}'')| = |\mathrm{Cl}(\mathbb{Z}+\frac{m}{2}\mathscr{O})|$. □

Remark 4.9 (Relation to Schütt's results). Schütt's Lemma 20 in [6] identifies, for certain singular K3 surfaces, when the degree of the field of definition attains a minimal value determined by the associated class group, and in that setting the result is essentially optimal.

By contrast, Theorem 4.8 should be viewed as an *existence* statement rather than a classification. Our results do not assert that the K3 surfaces constructed here are the only ones whose fields of definition have degree $|\mathrm{Cl}(\mathbb{Z}+m\,\mathrm{End}(E))|$ (or $|\mathrm{Cl}(\mathbb{Z}+\frac{m}{2}\,\mathrm{End}(E))|$ when $2 \mid m$). Instead, we show that there exist K3 surfaces such that their minimal field of definition having this optimal degree, without restrictions on the discriminant of Q or of m.

5 Appendix: Computations

In this appendix we describe various computations of j-invariants which we use in this paper.

To determine the homothety classes of lattices with complex multiplication by the order of discriminant D and to compute their exact j-invariants, we proceed as follows. First, we invoke Sage's quadratic-form routines to list all primitive, positive-definite binary forms of discriminant D. By the classical bijection between form classes and proper ideal classes in $\mathscr{O}_D$ ([3, Thm. 7.7]), each form $f(x,y) = ax^2 + bxy + cy^2$ yields an explicit proper $\mathscr{O}_D$-ideal and hence a CM-lattice up to homothety.

Next, we retrieve the Hilbert class polynomial $H_D(X)$ from Sage's database ([3, Prop.13.2]), adjoin one of its roots to $\mathbb{Q}$ to realize the ring class field L_D, and factor $H_D(X)$ over L_D to obtain algebraic expressions for all CM-j-invariants.

Finally, to match each algebraic j-value with its corresponding lattice $\Lambda \cong \langle 1, \tau \rangle$, we compute high-precision truncations of the classical q-expansion of $j(\tau)$ ([9, Prop. 9.12]) and compare numerically. This workflow yields a complete and exact description of the homothety classes and their j-invariants.

Consider the order $\mathscr{O} = \mathbb{Z}[\sqrt{-36}] \subset \mathbb{C}$, whose discriminant is $\Delta(\mathscr{O}) = -144$ and whose class number can be shown to be $|\mathrm{Cl}(\Delta)| = 4$. One convenient choice of representatives in terms of primitive, positive-definite binary quadratic forms is

$$Q_1(x,y) = x^2+36y^2, \quad Q_2(x,y) = 5x^2-4xy+8y^2, \quad Q_3(x,y) = 4x^2+9y^2, \quad Q_4(x,y) = 5x^2+4xy+8y^2.$$

Equivalently, the corresponding lattices in $\mathbb{C}$ may be taken as

$$\Lambda_1 = \langle 1, 6i \rangle, \quad \Lambda_2 = \langle 3, 1-2i \rangle, \quad \Lambda_3 = \langle 3, 2i \rangle, \Lambda_4 = \langle 3, 1+2i \rangle,$$

so that their period ratios are

$$\tau_1 = 6i, \quad \tau_2 = \frac{1-2i}{3}, \quad \tau_3 = \frac{2i}{3}, \quad \tau_4 = \frac{1+2i}{3}.$$

By the standard formula for the j-function one obtains Table 1.

We can go through a very similar process for the order $\mathbb{Z}[12i]$ to compute j-invariants and find the fields of definition given in Table 2.

Using Tables 1 and 2 we are able to compute all possible decompositions $\mathscr{A}_{d,E} \cong E_1 \times E_2$ for $d = 2$ and the elliptic curves $\mathbb{C}/\langle 3, 2i\rangle, \mathbb{C}/\langle 3, 1-2i\rangle$. We can then compute the fields of definition, which are given in Table 3.

k	**Lattice** Λ_k **and** $j(\Lambda_k)$
0	$\Lambda_0 = \langle 1, 6i\rangle = \mathbb{Z}6i$, $j(\Lambda_0) = 5894625992142600 + 34032639033336192\sqrt{3} + 3167093925247392\sqrt[4]{12} + 914261265145368(\sqrt[4]{12})^3$.
1	$\Lambda_1 = \langle 3, 1-2i\rangle$, $j(\Lambda_1) = 5894625992142600 - 34032639033336192\sqrt{3} - (3167093925247392\sqrt[4]{12} - 914261265145368(\sqrt[4]{12})^3)i$.
2	$\Lambda_2 = \langle 3, 2i\rangle$, $j(\Lambda_2) = 5894625992142600 + 34032639033336192\sqrt{3} - 3167093925247392\sqrt[4]{12} - 914261265145368(\sqrt[4]{12})^3$.
3	$\Lambda_3 = \langle 3, 1+2i\rangle$, $j(\Lambda_3) = 5894625992142600 - 34032639033336192\sqrt{3} + (3167093925247392\sqrt[4]{12} - 914261265145368(\sqrt[4]{12})^3)i$.

Table 1: The four j-invariants for lattices with CM by $\mathbb{Z}[6i]$.

$[\Lambda] \in \mathrm{Cl}(\mathscr{O})$	Λ	$\mathbb{Q}(j(\Lambda))$
$(0,0)$	$\mathbb{Z}[12i] = \langle 1, 12i\rangle$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$
$(0,1)$	$\langle 3, 1+4i\rangle$	$\mathbb{Q}(\sqrt{2}, i\sqrt[4]{3})$
$(0,2)$	$\langle 3, 4i\rangle$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$
$(0,3)$	$\langle 3, 1-4i\rangle$	$\mathbb{Q}(\sqrt{2}, i\sqrt[4]{3})$
$(1,0)$	$\langle 2, 1+6i\rangle$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$
$(1,1)$	$\langle 6, 1-2i\rangle$	$\mathbb{Q}(\sqrt{2}, i\sqrt[4]{3})$
$(1,2)$	$\langle 6, 3+2i\rangle$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$
$(1,3)$	$\langle 6, 1+2i\rangle$	$\mathbb{Q}(\sqrt{2}, i\sqrt[4]{3})$

Table 2: The fields of definition for the elliptic curves/lattices with CM by $\mathbb{Z}[12i]$

$E = \mathbb{C}/\Lambda$	d	$\mathscr{A}_{d,E} \simeq \mathbb{C}/\Lambda_1 \times \mathbb{C}/\Lambda_2$	$\mathbb{Q}(j(\Lambda_1), j(\Lambda_2))$	$[\mathbb{Q}(j_1, j_2) : \mathbb{Q}]$
$\langle 3, 2i\rangle$	2	$(\langle 1, 6i\rangle, \langle 3, 4i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$	8
		$(\langle 1, 6i\rangle, \langle 6, 3+2i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$	8
		$(\langle 3, 1+2i\rangle, \langle 3, 1-4i\rangle)$	$\mathbb{Q}(\sqrt{2}, i\sqrt[4]{3})$	8
		$(\langle 3, 1+2i\rangle, \langle 6, 1+2i\rangle)$	$\mathbb{Q}(\sqrt{2}, i\sqrt[4]{3})$	8
		$(\langle 3, 2i\rangle, \langle 1, 12i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$	8
		$(\langle 3, 2i\rangle, \langle 2, 1+6i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$	8
		$(\langle 3, 1-2i\rangle, \langle 3, 1+4i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$	8
		$(\langle 3, 1-2i\rangle, \langle 6, 1-2i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3})$	8
$\langle 3, 1-2i\rangle$	2	$(\mathbb{Z}[6i], \langle 3, 1+4i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i)$	16
		$(\mathbb{Z}[6i], \langle 6, 1-2i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i)$	16
		$(\langle 3, 1-2i\rangle, \mathbb{Z}[12i])$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i)$	16
		$(\langle 3, 1-2i\rangle, \langle 2, 1+6i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i)$	16
		$(\langle 3, 2i\rangle, \langle 3, 1-4i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i)$	16
		$(\langle 3, 2i\rangle, \langle 6, 1+2i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i)$	16
		$(\langle 3, 1+2i\rangle, \langle 3, 4i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i)$	16
		$(\langle 3, 1+2i\rangle, \langle 6, 3+2i\rangle)$	$\mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i)$	16

Table 3: Decompositions as a product for the abelian surfaces $\mathscr{A}_{2,\mathbb{C}/\langle 3,2i\rangle}$ and $\mathscr{A}_{2,\mathbb{C}/\langle 3,1-2i\rangle}$

Table 4 lists representatives for $\mathrm{Cl}(\mathbb{Z}[9i]) \simeq \mathbb{Z}/6\mathbb{Z}$ and records whether each class is a square, together with the corresponding field generated by its j-invariant. In particular, the class 3 is not a square but lies in $\mathrm{Cl}(\mathbb{Z}[9i])^2 \cdot \mathrm{Cl}(\mathbb{Z}[9i])[2]$.

Class in $\mathrm{Cl}(\mathbb{Z}[9i])$	Representative lattice Λ	Square?	$\mathbb{Q}(j(\Lambda))$
0	$\langle 1,\, 9i\rangle = \mathbb{Z}[9i]$	yes	real subfield of $L_{\mathbb{Z}[9i]}$
1	$\langle 9,\, 1+3i\rangle$	no	$L_{\mathbb{Z}[9i]}$
2	$\langle 3,\, 1+3i\rangle$	yes	real subfield of $L_{\mathbb{Z}[9i]}$
3	$\langle 9,\, 1+i\rangle$	no	real subfield of $L_{\mathbb{Z}[9i]}$
4	$\langle 3,\, 1-3i\rangle$	yes	real subfield of $L_{\mathbb{Z}[9i]}$
5	$\langle 9,\, 1-3i\rangle$	no	$L_{\mathbb{Z}[9i]}$

Table 4: Representatives for $\mathrm{Cl}(\mathbb{Z}[9i]) \cong \mathbb{Z}/6\mathbb{Z}$.

References

[1] Arnaud Beauville. “Some surfaces with maximal Picard number”. In: *Journal de l’École polytechnique—Mathématiques* 1 (2014), pp. 101–116.

[2] Z. I. Borevic and D. K. Faddeev. “Representations of orders with a cyclic index”. In: *Algebraic number theory and representations.* Trans. by T. S. Bhanu Murthy. Proceedings of the Steklov Institute of Mathematics, no. 80 (1965). American Mathematical Society, 1968, pp. 56–72.

[3] David A Cox. *Primes of the Form x2+ ny2: Fermat, Class Field Theory, and Complex Multiplication. with Solutions.* Vol. 387. American Mathematical Soc., 2022.

[4] Sheela Devadas and Max Lieblich. “Higher-weight Jacobians”. In: *arXiv preprint arXiv:2408.12576* (2024).

[5] Chad Schoen. “Produkte Abelscher Varietäten und Moduln über Ordnungen”. In: *Journal für die reine und angewandte Mathematik* 1992.429 (1992), pp. 115–124. DOI: doi:10.1515/crll.1992.429.115. URL: https://doi.org/10.1515/crll.1992.429.115.

[6] M. Schuett. “Fields of definition of singular K3 surfaces”. In: *Communications in Number Theory and Physics* 1 (2006), pp. 307–321. URL: https://api.semanticscholar.org/CorpusID:55121160.

[7] Tetsuji Shioda and Hiroshi Inose. “On singular K3 surfaces”. In: *Complex analysis and algebraic geometry* (1977), pp. 119–136.

[8] Tetsuji Shioda and Naoki Mitani. “Singular abelian surfaces and binary quadratic forms”. In: *Classification of algebraic varieties and compact complex manifolds.* Springer, 2006, pp. 259–287.

[9] Lawrence C Washington. *Elliptic curves: number theory and cryptography.* Chapman and Hall/CRC, 2008.