Asian J. Math.
Vol. 23, No. 1, pp. 157–172, February 2019

008

DECOMPOSITIONS OF SINGULAR ABELIAN SURFACES*

ROBERTO LAFACE†

Dedicated to my father on the occasion of his 50th birthday

Abstract. Given a singular abelian surface A, we find all possible decompositions of A into a product of two mutually isogenous elliptic curves with complex multiplication. This is done by computing the transcendental lattice of arbitrary such products, and by studying the action of a certain class group on the factors of a given decomposition. We also give an alternative proof of the formula for the number of decompositions of A, which is originally due to Ma.

Key words. Abelian surfaces, complex multiplication, elliptic curves, class field theory, quadratic forms.

Mathematics Subject Classification. 14K12, 14K22.

1. Introduction.

After the groundbreaking work of Shioda and Mitani [10], and of Shioda and Inose [9], singular abelian surfaces, i.e. abelian surfaces of maximum Picard number, have played a central role in the theory of algebraic surfaces. They come equipped with rich arithmetic information, which is encoded in the transcendental lattice, and they are intimately related to K3 surface via the Kummer construction and, more recently, via Shioda-Inose structures [6]. In the latter case, the associated singular K3 surface has the same transcendental lattice by a result of Shioda and Inose [9], so that it inherits the arithmetic structure of the singular abelian surface we started with. This has been employed to show the existence of one-to-one correspondence between singular abelian surfaces and singular K3 surfaces by Shioda and Inose [9], and more recently in the study of the field of definition of singular K3 surfaces by Schütt [7].

In [5], Ma gives a formula for the number of decompositions of an abelian surface into a product of elliptic curves; this expression is in terms of the arithmetic of the transcendental lattice. The proof builds on lattice-theoretical methods, and it works for abelian surfaces of any Picard number. Also, he is able to classify all the decompositions of a given abelian surface of Picard number $\rho \leq 3$. However, there is no mention of the possible decompositions that can appear in the case of singular abelian surfaces. The main purpose of this paper is study the decompositions in this last case. In doing so, we have tried to highlight the connection between the geometry of singular abelian surfaces and the arithmetic of quadratic forms as much as possible.

Our techniques are based on the theory of quadratic forms and the CM theory of elliptic curves. As every singular abelian surface is isomorphic to the product of two mutually isogenous elliptic curves with complex multiplication, we first computed the transcendental lattice of arbitrary such products (Proposition 3.2). A proof of this fact, although not explicitly stated, can be obtained by combining results Hirzebruch and Shioda-Mitani in [10], and it is in the language of ideal classes. However, as our study of the decompositions of a singular abelian surface will use in an essential way the theory of quadratic forms (and numbers represented by them), we give a new and alternative approach to the computation of transcendental lattices, which

*Received October 5, 2016; accepted for publication August 8, 2017.

†Technische Universität München, Zentrum Mathematik – M11, Boltzmannstraße 3, 85748 Garching bei München, Germany (laface@ma.tum.de).

only uses the language of quadratic forms, and which is a natural generalization of the argument of Shioda and Mitani [10, §3.(I)]. Interestingly, this new approach leads to the notion of *generalized Dirichlet composition*: while the usual Dirichlet composition allows to compose two (classes of) quadratic forms of given discriminant, this generalization allows to extend the composition to (classes of) forms of possibly different discriminant. Indeed, this is of interest on its own, as it is a generalization of work of Gauß and Dirichlet in the theory of quadratic forms.

Going back to the study of all the possible decompositions of a given singular abelian surface, we distinguish two cases in our analysis, according to the complex multiplication field K of the singular abelian surface A. If $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, then we are able to explicitly construct enough decompositions of A by using the generalized Dirichlet composition to match Ma's formula (Theorem 4.11). With this method, we are also able to give a new proof of Ma's result: the idea is to consider all singular abelian surfaces of fixed discriminant and index of primitivity at once, and to reduce the statement to a number-theoretical problem of class numbers. The cases $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$ require a little more care to handle, but nevertheless we are able to find all decompositions and to give new formulae for the number of decompositions. These formulae, unlike Ma's, do not depend on the discriminant group of the transcendental lattice of A, but only on its discriminant and its index of primitivity.

Acknowledgement. It is a pleasure to thank Matthias Schütt for fruitful discussions on the topic. Many thanks go to Víctor González Alonso and Daniel Loughran for detailed comments and suggestions on an earlier draft of this manuscript.

2. Preliminaries and notation.

2.1. The period of an abelian surface. We briefly recall the notion of period of an abelian surface A; for details, see [8]. The exponential sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_A \longrightarrow \mathcal{O}_A^\times \longrightarrow 0$$

yields a long exact exact sequence in cohomology, from which we can extract a map

$$p_A : \mathrm{H}^2(X, \mathbb{Z}) \longrightarrow \mathrm{H}^2(A, \mathcal{O}_A) \cong \mathbb{C};$$

this map is called *the period of A*. Let $\{v_1, v_2, v_3, v_4\}$ be a basis of $\mathrm{H}_1(A, \mathbb{Z})$, and let $\{u^1, u^2, u^3, u^4\}$ be the corresponding dual basis of $\mathrm{H}^1(A, \mathbb{Z})$. We can cook up a basis of $\mathrm{H}^2(A, \mathbb{Z})$ by considering

$$\{u^{ij} := u^i \wedge u^j \mid 1 \leq i < j \leq 4\}.$$

As an element of $\mathrm{H}^2(A, \mathbb{C}) \cong \mathrm{Hom}(\mathrm{H}^2(A, \mathbb{Z}), \mathbb{C})$, the period of A has the following explicit description:

$$p_A = \sum_{i<j} \det(v_i|v_j) u^{ij},$$

where the notation $(v_i|v_j)$ indicates the matrix whose columns are v_i and v_j. As $\mathrm{NS}(A) = \ker(p_A)$ and $\mathrm{T}(A) = \mathrm{NS}(A)^\perp$, this formulation of p_A allows us to compute the Néron-Severi lattice and the transcendental lattice explicitly once we are given the period matrix Π of $A = \mathbb{C}^2/\Pi$.

2.2. Class group theory. We recall a few facts on integral binary quadratic forms; for a beautiful account, see [2]. Given an integral binary quadratic form (in the following always referred to as a form)

$$Q \equiv Q(x,y) = ax^2 + bxy + cy^2 = (a,b,c),$$

the quantity $n := \gcd(a,b,c)$ is called *index of primitivity* of Q, and Q is said to be *primitive* if $n = 1$. The (unique) quadratic form Q_0 such that $nQ_0 = Q$ is the *primitive part* of Q. A form Q *represents* an integer $m \in \mathbb{Z}$ if there are integers $x, y \in Z$ such that $Q(x,y) = m$; if moreover $n = 1$, then we say that Q *properly represents* m. Two forms $Q = (a,b,c)$ and $Q' = (a',b',c')$ are *equivalent* (respectively, *properly equivalent*) if there exists a matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ (respectively, $\mathrm{SL}_2(\mathbb{Z})$) such that

$$Q(px+qy, rx+sy) = Q'(x,y).$$

The *discriminant* of a form $Q = (a,b,c)$ is the integer $D := b^2 - 4ac$. The set of proper equivalent classes of primitive forms of discriminant D is called the *(form) class group* of discriminant D: it is denoted by $C(D)$, and its order $h(D)$ is called the *class number* of D. The class group $C(D)$ is a group with respect to the Dirichlet composition, which is described in [2, Lemma 3.2].

2.3. Ideal class group. Fixed a quadratic imaginary field K, an *order* $\mathcal{O}$ is a subring of K containing the unity of K which has also the structure of a rank-two free $\mathbb{Z}$-module. Every order $\mathcal{O}$ can be written in a unique way as

$$\mathcal{O} = \mathbb{Z} + f w_K \mathbb{Z}, \quad w_K := \frac{d_K + \sqrt{d_K}}{2}, \quad d_K := \operatorname{disc} \mathcal{O}_K, \quad f \in \mathbb{Z}^+.$$

The integer f is called the *conductor* of $\mathcal{O}$, and it characterizes $\mathcal{O}$ in a unique way. Therefore, we will denote the order of conductor f in K by $\mathcal{O}_{K,f}$.

Given an order $\mathcal{O}_{K,f}$, one can define the *(ideal) class group* $C(\mathcal{O}_{K,f})$ (see [2, Chapter I, §7]). Letting $I(\mathcal{O}_{K,f})$ be the group of proper fractional ideals, and letting $P(\mathcal{O}_{K,f})$ be the subgroup generated by the principal ones, we set $C(\mathcal{O}_{K,f}) := I(\mathcal{O}_{K,f})/P(\mathcal{O}_{K,f})$. The connection to form class groups is made explicit by the following:

Theorem 2.1 (Theorem 7.7 in [2]). *Let $\mathcal{O}_{K,f}$ be an order in a quadratic imaginary field K, and let $D := f^2 d_K$. Then, there exists a one-to-one correspondence*

$$\begin{aligned} C(D) &\longrightarrow C(\mathcal{O}_{K,f}) \\ Q = (a,b,c) &\longmapsto \Big[a, \frac{-b+\sqrt{D}}{2}\Big]. \end{aligned}$$

2.4. Elliptic curves, quadratic forms and ideal classes. Let E be an elliptic curve over $\mathbb{C}$, $E = \mathbb{C}/\Lambda$, Λ being a rank-two lattice in $\mathbb{C}$. Suppose that E has complex multiplication, that is $\mathrm{End}(E) = \mathrm{End}_{\mathbb{Z}}(\Lambda) = \mathcal{O}_{K,f}$, for some order $\mathcal{O}_{K,f}$. Then, Λ is a proper fractional $\mathcal{O}_{K,f}$-ideal, hence it yields an element $[\Lambda] \in C(\mathcal{O}_{K,f})$. Conversely, every proper fractional $\mathcal{O}_{K,f}$-ideal is a lattice having $\mathcal{O}_{K,f}$ as its ring of endomorphisms. Furthermore, two proper fractional $\mathcal{O}_{K,f}$-ideals are homothetic as lattices if and only if they determine the same class in $C(\mathcal{O}_{K,f})$ (see [2, Exercise 10.15]). This results in the following

Proposition 2.2 (Corollary 10.20 of [2]). *There is a one-to-one correspondence between the ideal class group $C(\mathcal{O}_{K,f})$ and the set $\mathcal{E}ll(\mathcal{O}_{K,f})$ of isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}_{K,f}$.*

As a consequence of Theorem 2.1 and Proposition 2.2, we have the following identifications

$$\mathcal{E}ll(\mathcal{O}_{K,f}) \longleftrightarrow C(\mathcal{O}_{K,f}) \longleftrightarrow C(D),$$

where $D := f^2 d_K$. This means that we can switch between elliptic curves, ideals classes and quadratic forms to our content. In light of this, we will use the following notation: for $Q \in C(D)$, set

$$\tau(Q) := \frac{-b+\sqrt{D}}{2a},$$

and define $E_Q := E_{\tau(Q)}$, where E_τ denotes the elliptic curve $\mathbb{C}/\Lambda_\tau$, Λ_τ being the lattice $\mathbb{Z}+\tau\mathbb{Z}$.

2.5. The space of singular abelian surfaces. Let Σ^{Ab} be the *space* of singular abelian surfaces, i.e. the set of isomorphism classes of singular abelian surfaces. In [10], Shioda and Mitani described Σ^{Ab} by means of the transcendental lattice $\mathrm{T}(A)$ associated to any singular abelian surface A. We say that $\mathrm{T}(A)$ is *positively oriented* if

$$\mathrm{T}(A) = \mathbb{Z}\langle t_1, t_2\rangle \qquad \text{and} \qquad \mathrm{Im}(p_A(t_1)/p_A(t_2)) > 0.$$

Notice that the transcendental lattice $\mathrm{T}(A)$ is an even lattice $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$, and thus we can always associate to it the quadratic form (a,b,c). This describes a 1:1 correspondence between $\mathrm{SL}_2(\mathbb{Z})$-conjugacy classes of binary forms and isomorphism classes of singular abelian surfaces, namely

$$\Sigma^{\mathrm{Ab}} \longleftrightarrow \mathcal{Q}^+/\,\mathrm{SL}_2(\mathbb{Z}),$$

$\mathcal{Q}^+$ being the set of positive definite integral binary quadratic forms. We briefly describe the inverse of this correspondence, meaning how to associate to any quadratic form $Q=(a,b,c)$ an abelian surface A_Q. We set

$$\tau := \tau(Q) = \frac{-b+\sqrt{D}}{2a}, \qquad D := \operatorname{disc} Q = b^2 - 4ac.$$

The abelian surface associated to a form Q is then defined as the product surface

$$A_Q := E_\tau \times E_{a\tau+b}.$$

As a consequence, every singular abelian surface A is isomorphic to the product of two isogenous elliptic curves with complex multiplication [10, Theorem 4.1].

2.6. Decompositions of singular abelian surfaces. Following [5], a *decomposition* of A is a pair (E_1, E_2) such that $A \cong E_1 \times E_2$. Two decompositions (E_1,E_2) and (F_1,F_2) of A are *equivalent* if $E_1 \cong F_1$ and $E_2 \cong F_2$, or $E_1 \cong F_2$ and $E_2 \cong F_1$. Analogously, two decompositions (E_1,E_2) and (F_1,F_2) of A are *strictly equivalent* if $E_1 \cong F_1$ and $E_2 \cong F_2$. Let $\mathrm{Dec}(A)$ be the set of isomorphism classes of decompositions of A, and similarly let $\widetilde{\mathrm{Dec}}(A)$ be the set of strict isomorphism classes of decompositions of A. Also, define $\delta(A) := \#\mathrm{Dec}(A)$ and $\widetilde{\delta}(A) := \#\widetilde{\mathrm{Dec}}(A)$. The quantities $\delta(A)$ and $\widetilde{\delta}(A)$ are obviously related by $\widetilde{\delta}(A) = 2\delta(A) - \delta_0(A)$, where $\delta_0(A)$ is the number of decompositions of A into a self-product. Finally, for $n > 1$, let $\tau(n)$ be the number prime factors of n, and set $\tau(1) = 1$.

Given singular abelian surface A, Ma [5] was able to find formulae for $\widetilde{\delta}(A)$. These formulae depend on the arithmetic of the transcendental lattice $\mathrm{T}(A)$, and in particular on the order of the discriminant group $A_{\mathrm{T}(A)}$. However, in case the primitive part of $\mathrm{T}(A)$ has determinant $D_0 \notin \{3, 4\}$, Ma gives a formula which only depends on $h(\operatorname{disc}\mathrm{T}(A))$ and the index of primitivity of $\mathrm{T}(A)$. For later use, we mention the latter[1]:

Corollary 2.3 (Corollary 5.12 in [5]). *Let A be a singular abelian surface of transcendental lattice $\mathrm{T}(A) = Q = nQ_0$, $Q_0 \in C(D_0)$ (in particular Q_0 is primitive). If $\operatorname{disc} Q_0 \neq -3, -4$, then*

$$\widetilde{\delta}(A) = 2^{\tau(n)} \cdot h(\operatorname{disc} Q).$$

3. A remark on the transcendental lattice of singular abelian surfaces.

3.1. Motivation. In [10], the authors explicitly compute the transcendental lattice of certain product abelian surfaces. As every singular abelian surface is always isomorphic to a product of mutually isogenous elliptic curves, one might want to compute (in an explicit way) the transcendental lattice of arbitrary such products. In principle, this can be done in terms of ideal classes by combining results of Hirzebruch [10, Lemma 4.4], and of Shioda and Mitani [10, Proposition 4.5].

Our approach to the classification of the decompositions of singular abelian surfaces will use quadratic forms (and numbers represented by them) rather than ideal classes. With this motivation in mind, it is worth observing that we can compute transcendental lattices of arbitrary product singular abelian surface just by using quadratic forms, without using the 1:1 correspondence between ideal classes and quadratic forms (Proposition 2.2). This is a new and alternative approach, which only relies on ideas of Shioda and Mitani [10, §3.(I)]. The key step for achieving this is to figure out a way to compose two (classes of) quadratic forms of different discriminant, generalizing the usual Dirichlet compositions of two quadratic forms of given discriminant. This is of independent interest, as it generalizes previous work of Gauß and Dirichlet in the theory of quadratic forms.

3.2. Generalized Dirichlet composition. The idea behind the Dirichlet composition is that two binary quadratic forms Q_1 and Q_2 (having the same discriminant D) give rise to a new form F (again of discriminant D) with the property

$$Q_1(x, y) \cdot Q_2(z, w) = F(B_1(x, y, z, w), B_2(x, y, z, w)),$$

for $B_i(x, y, z, w) \in \mathbb{Z}[xz, xw, yz, yw]$. In particular, the products of numbers represented by Q_1 and Q_2 are represented by F.

[1] This statement constitutes the original motivation of the present paper.

If Q_1 and Q_2 are not of the same discriminant, we can multiply them by positive integers to obtain two new forms (necessarily not primitive) having the same discriminant. Namely, given $[Q_1] \in C(D_1)$ and $[Q_2] \in C(D_2)$, with $D_1 = f_1^2 d_K$ and $D_2 = f_2^2 d_K$, set $f := \operatorname{lcm}(f_1, f_2)$. Then, putting

$$D := f^2 d_K, \qquad d_1 := f/f_1, \qquad d_2 := f/f_2,$$

the forms $d_1 Q_1$ and $d_2 Q_2$ have discriminant D. Therefore, after possibly replacing Q_1 and Q_2 with suitable properly equivalent forms, we can assume that $d_1 Q_1$ and $d_2 Q_2$ have coprime leading coefficients (use [2, Lemma 2.25] and $\gcd(d_1, d_2) = 1$), hence composition is well-defined: indeed, it works exactly as in the case of primitive forms (for an account, see [2, Theorem 3.8]). It is not hard to check the following:

Lemma 3.1. *Assume that $Q = (a, b, c)$ and $Q' = (a', b', c')$ are primitive, and suppose that*

$$n^2 \operatorname{disc} Q = m^2 \operatorname{disc} Q', \qquad \gcd(n, m) = 1.$$

Then, the form $(nQ) * (mQ')$ has primitivity index nm (if the composition exists).

Proof. This follows from repeating the construction of the usual composition of binary quadratic forms in this more general setup; the interested reader will find a detailed account in [2, Ch. 1, Sect. 3]. □

In particular, the above lemma shows that the form $d_1 Q_1 * d_2 Q_2$ has index of primitivity $d_1 d_2$, which is the content of [10, Lemma 4.4] in terms of quadratic forms. Also,

$$D = \operatorname{disc}(d_1 Q_1 * d_2 Q_2) = (d_1 d_2)^2 \gcd(f_1, f_2)^2 d_K,$$

and therefore the primitive part of $d_1 Q_1 * d_2 Q_2$ is a form in $C(\mathcal{O}_{K,f_0})$, where $f_0 := \gcd(f_1, f_2)$. This means that composing forms of discriminants D_1 and D_2 gives forms of discriminant $D := \operatorname{lcm}(D_1, D_2)$, having index of primitivity $d_1 d_2$, where $d_1 = f/f_1$ and $d_2 = f/f_2$. Dropping the primitivity index, we get a *generalized Dirichlet composition*

$$C(D_1) \times C(D_2) \xrightarrow{\circledast} C(D_0),$$

where $D_0 := f_0^2 d_K$. More concretely, given $Q_1 \in C(D_1)$ and $Q_2 \in C(D_2)$, $Q_1 \circledast Q_2$ is the form in $C(D_0)$ with the property that

$$d_1 d_2 [Q_1 \circledast Q_2] = [d_1 Q_1] * [d_2 Q_2].$$

By Theorem 2.1, one sees that the generalized Dirichlet composition corresponds to the usual multiplication between ideal classes

$$C(\mathcal{O}_{K,f_1}) \times C(\mathcal{O}_{K,f_2}) \longrightarrow C(\mathcal{O}_{K,f_0}).$$

3.3. Explicit computation of transcendental lattices. We will now exhibit a formula for the transcendental lattice of a singular abelian surface in terms of quadratic forms. As mentioned earlier, a proof of this can be found in [10] (up to translation into the languange of quadratic forms via Proposition 2.2). However, we provide here an alternative argument, which is inspired by the ideas in [10, §3.(I)].

Proposition 3.2. *Let $D_0 = f_0^2 d_K$ and $D_0' = (f_0')^2 d_K$, where d_K is the fundamental discriminant of a quadratic imaginary field K. Let $Q_0 = (a_0, b_0, c_0) \in C(D_0)$ and $Q_0' = (a_0', b_0', c_0') \in C(D_0')$; moreover, let*

$$f := \operatorname{lcm}(f_0, f_0'), \quad d := f/f_0, \quad d' := f/f_0', \quad D := f^2 d_K.$$

Then,

$$[\mathrm{T}(E_{Q_0} \times E_{Q_0'})] = dd'[Q_0 \circledast Q_0'] = (d[Q_0]) * (d'[Q_0']).$$

Proof. Recall that $E_{Q_0} := E_{\tau(Q_0)}$, and observe that

$$\tau_1 := \tau(Q_0) = \frac{-b_0 + \sqrt{D_0}}{2a_0} = \frac{-b + \sqrt{D}}{2a},$$

where $(a, b, c) = d \cdot (a_0, b_0, c_0)$. Similarly,

$$\tau_2 := \tau(Q_0') = \frac{-b_0' + \sqrt{D_0'}}{2a_0'} = \frac{-b' + \sqrt{D}}{2a'},$$

where $(a', b', c') = d' \cdot (a_0', b_0', c_0')$. Let B be the key element in the Dirichlet composition, which is described in [2, Lemma 3.2]. By $\mathrm{SL}_2(\mathbb{Z})$-invariance of the j-invariant, we can replace b and b' by B without changing the isomorphism classes of E and E'. Therefore, we can assume that

$$\tau_1 = \frac{-B + \sqrt{D}}{2a}, \qquad \tau_2 = \frac{-B + \sqrt{D}}{2a'}.$$

By [10],

$$p_A = u^{12} + \tau_2 u^{14} + \tau_1 u^{23} - \tau_1 \tau_2 u^{34},$$

and $\mathrm{NS}(A) = \ker(p_A)$. Letting

$$v = \sum_{1 \le i < j \le 4} A_{ij} u^{ij} \in \mathrm{NS}(A)_{\mathbb{Q}},$$

from $p_A(v) = 0$, we see that

$$\mathrm{NS}(A)_{\mathbb{Q}} = \mathbb{Q}\Big\langle u^{12} - \frac{B}{a} u^{23} + \frac{D - B^2}{4aa'} u^{34}, u^{14} - \frac{a'}{a} u^{23}, u^{13}, u^{24} \Big\rangle.$$

Similarly, if $v \in \mathrm{T}(A) = \mathrm{NS}(A)^{\perp}$, then

$$A_{24} = A_{13} = 0, \tag{1}$$

$$A_{34} - \frac{B}{a} A_{14} + \frac{D - B^2}{4aa'} A_{12} = 0, \tag{2}$$

$$A_{23} - \frac{a'}{a} A_{14} = 0. \tag{3}$$

Condition (3) gives

$$da_0 A_{23} = d' a_0' A_{14};$$

now we can assume that $(d, a_0') = 1$ and then also that $(a_0, a') = 1$ (use [2, Lemma 2.3] and [2, Lemma 2.25]). Under these assumptions, we see that

$$A_{14} = a_0 A'_{14} = a_0 d A''_{14} \qquad \text{and} \qquad A_{23} = a_0' d' A''_{14};$$

substituting in (2) yields

$$A_{34} = B A''_{14} + C A_{12},$$

where $C = \frac{B^2 - D}{4aa'}$, and therefore we deduce

$$\mathrm{T}(A) = \mathbb{Z}\Big\langle au^{14} + a'u^{23} + Bu^{34}, u^{12} + Cu^{34}\Big\rangle = \begin{pmatrix} 2aa' & B \\ B & 2C \end{pmatrix}.$$

□

4. Decompositions for $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$.

4.1. Cooking up decompositions from a given one. Let A be a singular abelian surface of transcendental lattice $Q = nQ_0$ of discriminant $D = f^2 d_K$, $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$ being a suitable quadratic imaginary field, and let $D_0 := \operatorname{disc} Q_0 = f_0^2 d_K$. We can use Proposition 3.2 to cook up new decompositions starting from a given one. To this end, suppose A decomposes as $A \cong E_{Q_1} \times E_{Q_2}$, with $Q_1 \in C(D_1)$, $Q_2 \in C(D_2)$, $\gcd(D_1, D_2) = D_0$ and $\operatorname{lcm}(D_1, D_2) = D$. Then, as $C(D)$ acts on both $C(D_1)$ and $C(D_2)$ by means of $\circledast$, we get new decompositions of A by considering the following product surfaces

$$E_{Q_1 \circledast R} \times E_{Q_2 \circledast R^{-1}}, \qquad R \in C(D).$$

Remark 4.1. Notice that, given A as above, we can always cook up a decomposition into a product of elliptic curves E_1 and E_2 such that

$$E_1 \in C(D_1),\ E_2 \in C(D_2),\ \operatorname{lcm}(D_1, D_2) = D,\ \gcd(D_1, D_2) = D_0.$$

Indeed, consider a form Q_0 and the principal form P_0, both of discriminant D_0, and let $s, t \in \mathbb{Z}$ be coprime nonnegative integers. Consider the abelian surface given by

$$E_{s\tau(Q_0)} \times E_{t\tau(P_0)}.$$

Then, similar computations to the ones in Theorem 3.2 show that $E_{s\tau(Q_0)} \times E_{t\tau(P_0)}$ gives indeed a decomposition of A. Notice that, if $Q_0 = (a_0, b_0, c_0)$, then $s\tau(Q_0)$ corresponds to the form

$$a_0 x^2 + (b_0 s)xy + (c_0 s^2)y^2,$$

which is primitive, hence it lies in $C(s^2 D_0)$, and similar considerations hold for $t\tau(P_0)$. Therefore, in order to get the desired decomposition, it is enough to set $s := f_1/f_0$ and $t := f_2/f_0$ (or viceversa). □

4.2. Action of a class group on class groups of smaller discriminant. Recall that the class group $C(D)$ acts on $C(D_0)$ by means of $\circledast$ whenever D_0 divides D. Therefore, we might ask whether this action is transitive. We first notice that a form $Q_0 \in C(D_0)$ can be lifted to a primitive form $Q \in C(D)$ in such a way that $Q \circledast P_0 = Q_0$, as stated in the following:

LEMMA 4.2. *For every form $Q_0 \in C(D_0)$ there exists a form $Q \in C(D)$ which is the lift of Q_0 in the following sense: $Q \circledast P_0 = Q_0$.*

Proof. If $Q_0 = [a_0, b_0, c_0]$ is represented by the ideal $[a_0, \frac{-b_0+\sqrt{D_0}}{2}]$, then let Q correspond to the ideal class $[a_0, \frac{-db_0+\sqrt{D}}{2}]$; moreover, let dP_0 correspond to the ideal class $[d, \frac{-dp_0+\sqrt{D}}{2}]$, where $p_0 = 0, 1$ according to the parity of the discriminant D. It follows that

$$\left[a_0, \frac{-db_0+\sqrt{D}}{2}\right] \cdot \left[d, \frac{-dp_0+\sqrt{D}}{2}\right] = [a_0 d, \Delta] = [a_0, \Delta/d],$$

where $\Delta = \frac{-B+\sqrt{D}}{2}$, and B is integer introduced in the Dirichlet composition. Since $[a_0, \Delta/d]$ corresponds exactly to Q_0, we are done. □

As a consequence, we have the following:

COROLLARY 4.3. *The action of $C(D)$ on $C(D_0)$ is transitive.*

This means that the factors of the decompositions

$$E_{Q_1 \circledast R} \times E_{Q_2 \circledast R^{-1}}, \qquad R \in C(D)$$

cover the whole class groups $C(D_1)$ and $C(D_2)$, i.e.

$$\{Q_1 \circledast R \,|\, R \in C(D)\} = C(D_1),$$

and similarly for $C(D_2)$. In the following, we will be investigating whether we get $h(D)$ distinct decompositions under this action, i.e. whether

$$\left(E_{Q_1 \circledast R}, E_{Q_2 \circledast R^{-1}}\right) \neq \left(E_{Q_1 \circledast S}, E_{Q_2 \circledast S^{-1}}\right)$$

for $R \neq S \in C(D)$.

4.3. Distinct decompositions. We now come to the issue of whether the action of $C(D)$ on the factors of a given decomposition delivers $h(D)$ distinct decompositions. Let us assume $Q_1 \in C(D_1)$, $Q_2 \in C(D_2)$ and $R, S \in C(D)$. Moreover, suppose that

$$Q_1 \circledast R = Q_1 \circledast S, \qquad Q_2 \circledast R^{-1} = Q_2 \circledast S^{-1},$$

which is equivalent to assuming that a decomposition be realized by two distinct elements $R, S \in C(D)$. This, in turn, is equivalent to the existence of an element $U \in C(D)$ such that

$$U \circledast Q_1 = Q_1, \qquad U \circledast Q_2 = Q_2.$$

So we are to understand the elements $U \in C(D)$ that fix Q_i, $i = 1, 2$.

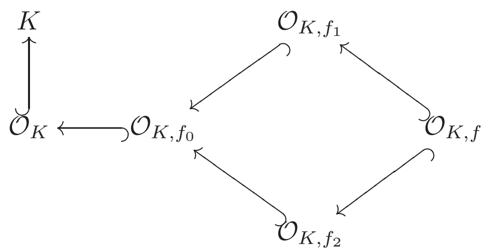
Let $C(D)$ act on $C(D_0)$ (having D_0 divide D), and let U be an element fixing some $Q_0 \in C(D_0)$; notice that U would actually fix the whole class group $C(D_0)$. We call the group of such U's the *stabilizer* of $C(D_0)$ in $C(D)$, and it will be denoted by

$\operatorname{Stab} C(D_0)$; clearly, its order is $h(D)/h(D_0)$. In the situation of interest to us, we want to study $\operatorname{Stab} C(D_1) \cap \operatorname{Stab} C(D_2)$: this intersection describes the elements in $C(D)$ that represent an obstruction to $C(D)$ delivering $h(D)$ distinct decompositions via its action on the factors of a given decomposition. In other words, we would like to answer the following:

QUESTION 4.4. When is $\operatorname{Stab} C(\mathcal{O}_{K,f_1}) \cap \operatorname{Stab} C(\mathcal{O}_{K,f_2})$ trivial?

Whenever the answer is affirmative, the action of $C(D)$ on a given decomposition yields exactly $h(D)$ distinct decompositions.

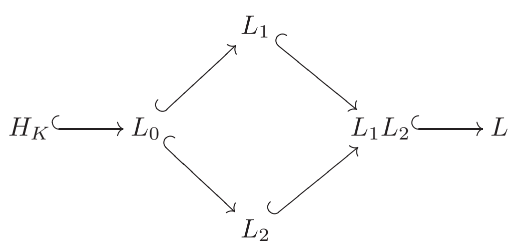
4.4. Interlude: ring class fields and their compositum fields. Suppose we have the diagrams of orders



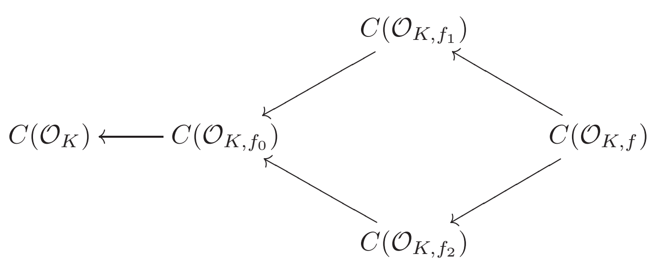
where $f_1, f_2 \geq 1$, $f_0 = \gcd(f_1, f_2)$ and $f = \operatorname{lcm}(f_1, f_2)$. Let $i = 0, 1, 2, \emptyset$; since

$$P_{K,1}(f_i\mathcal{O}_K) \subseteq P_{K,\mathbb{Z}}(f_i) \subseteq I_K(f_i) = I_K(f_i\mathcal{O}_K),$$

by [2, Existence Thm], there exists a unique abelian extension L_i/K all of whose ramified primes divide $f_i\mathcal{O}_K$, such that $\ker(\Phi^{L_i/K}_{f_i\mathcal{O}_k}) = P_{K,\mathbb{Z}}(f_i)$, i.e. $\operatorname{Gal}(L_i/K) \cong C(\mathcal{O}_{K,f_i})$. This extension is the ring class field of $\mathcal{O}_{K,f_i}$, and it is sometimes denoted by $H(\mathcal{O}_{K,f_i})$; at the level of ring class fields, we get induced a diagram of field extensions,



where H_K is the *Hilbert class field* of K, i.e. the ring class field of $\mathcal{O}_K$. By Galois theory, we get the following induced diagram of class groups.



In most cases the field L is precisely the composite of L_1 and L_2, as it is stated in the following[2]

PROPOSITION 4.5 (Proposition 3.1 in [1]). *Assume all conditions above are satisfied.*

(1) *If $d_K \neq -3, -4$, then $L = L_1 L_2$.*
(2) *Assume $d_K \in \{-3, -4\}$.*
  (a) *If f_1 or f_2 is equal to 1, or $f_0 > 1$, then $L = L_1 L_2$.*
  (b) *If $f_1, f_2 > 1$ and $f_0 = 1$, then $L_1 L_2 \subsetneq L$; moreover, the extension $L/L_1 L_2$ has degree 2 if $d_K = -4$, and degree 3 if $d_K = -3$.*

4.5. Interlude: numbers represented by the principal form. For two sets S and T, we say that $S \dot{\subset} T$ if $S \subseteq T \cup \Sigma$, where Σ is a finite set; analogously, $S \doteq T$ means that both $S \dot{\subset} T$ and $T \dot{\subset} S$ hold. Suppose we are now given a quadratic form Q; then, we can ask about the primes represented by Q, i.e. about the set

$$\mathcal{P}_Q := \{p \text{ prime} \,|\, p \text{ is represented by } Q\}.$$

It turns out that

$$\mathcal{P}_Q \doteq \left\{ p \text{ prime} \,\middle|\, p \text{ unramified in } K, \left(\frac{L/K}{p}\right) = \langle\sigma\rangle \right\} =: \hat{\mathcal{P}}_Q,$$

where $\langle\sigma\rangle$ is the conjugacy class of the element $\sigma \in \mathrm{Gal}(L/K)$ corresponding to the ideal associated to the form Q, K is the quadratic imaginary field of discriminant $\operatorname{disc} Q$, and L is the ring class field of the order $\mathcal{O}$ of discriminant $\operatorname{disc} Q$. Notice that in case $Q = P$, the principal form, then $\hat{\mathcal{P}}_P = \mathrm{Spl}(L/\mathbb{Q})$, $\mathrm{Spl}(L/\mathbb{Q})$ being the set of primes in $\mathbb{Q}$ that split completely in L. For later reference, we mention the following

LEMMA 4.6 (Exercise 8.14 in [2]). *Let L and M be two finite extension of K, and let $\mathcal{P}$ be a prime in K that splits completely in both L and M; then $\mathcal{P}$ splits completely in the composite LM. Consequently,* $\mathrm{Spl}(LM/K) = \mathrm{Spl}(L/K) \cap \mathrm{Spl}(M/K)$.

4.6. Answer to Question 4.4. Let P_i be the principal form of the order $\mathcal{O}_{K,f_i}$, $i = 1, 2, \emptyset$. Also, let L_i be the ring class field of the order $\mathcal{O}_{K,f_i}$, $i = 1, 2, \emptyset$. The key tool we will use is the fact that the principal form represents all but finitely many unramified primes which split completely in the ring class field.

LEMMA 4.7. *Let $\mathcal{P}_{P_i}$ be the set of primes of represented by P_i, for $i = 1, 2,$. Then, $\mathcal{P}_P \doteq \mathcal{P}_{P_1} \cap \mathcal{P}_{P_2}$.*

Proof. By using Lemma 4.6, we see that

$$\mathcal{P}_P \doteq \mathrm{Spl}(L/K) = \mathrm{Spl}(L_1/K) \cap \mathrm{Spl}(L_2/K) \doteq \mathcal{P}_{P_1} \cap \mathcal{P}_{P_2}.$$

□

By the Čebotarev Density Theorem, we can reason with the set $\mathcal{P}_{P_i}$ rather than $\mathrm{Spl}(L_i/K)$, for $i = 1, 2, \emptyset$: in fact, they both have positive Dirichlet density (thus they are infinite), and they are the same up to a finite set (which has Dirichlet density 0).

[2]This result is the reason why we have to distinguish two cases, according to whether $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})\}$ or not.

Proposition 4.8. *The principal form is characterized by representing almost all primes that split completely in the ring class field.*

Proof. Suppose Q is a form such that $\mathcal{P}_Q \doteq \mathrm{Spl}(L/K)$. Then, we would have

$$\left\{p \text{ prime} \,\middle|\, p \text{ unramified}, \left(\frac{L/K}{p}\right) = \langle\sigma\rangle\right\} \doteq \left\{p \text{ prime} \,\middle|\, \left(\frac{L/K}{p}\right) = \langle 1\rangle\right\},$$

and since both sets have infinitely many elements it must necessarily be $\sigma = 1 \in \mathrm{Gal}(L/K)$, which corresponds to the class of the principal form. Since equivalent forms represent the same numbers, we are done. □

We can now answer Question 4.4:

Proposition 4.9. *Unless $d_K \in \{-3, -4\}$, $f_1, f_2 > 1$ and $f_0 = 1$, we have*

$$\mathrm{Stab}\, C(\mathcal{O}_{K,f_1}) \cap \mathrm{Stab}\, C(\mathcal{O}_{K,f_2}) = (0).$$

Proof. Let $Q \in \mathrm{Stab}\, C(D_1) \cap \mathrm{Stab}\, C(D_2)$, i.e. Q is such that

$$Q \circledast P_1 = P_1, \qquad Q \circledast P_2 = P_2.$$

Now, for $i = 1, 2$, the primes represented by P_i are, up to a finite set, those p that split completely in the ring class field L_i. In the same fashion, the primes represented by Q are, up to a finite set, the ones splitting completely in the ring class field L. Notice that, by the assumption, it follows that all primes represented by Q are also represented by P_1 and P_2. Moreover, by [1, Proposition 3.1], $L = L_1L_2$, and Lemma 4.7 and Proposition 4.8 imply that Q is in fact the principal form. □

Remark 4.10. With the aid of a computer program, it is not difficult to find examples of $\mathrm{Stab}\, C(\mathcal{O}_{K,f_1}) \cap \mathrm{Stab}\, C(\mathcal{O}_{K,f_2})$ being non-trivial, if $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$. □

4.7. Classification result for $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. As an immediate consequence of Proposition 4.9, we have constructed all possible decompositions of a given singular abelian surface in case $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. More precisely,

Theorem 4.11. *Let A be a singular abelian surface having transcendental lattice $Q = nQ_0$, and let $D = f^2 d_K = \mathrm{disc}\, Q$, $D_0 = f_0^2 d_K = \mathrm{disc}\, Q_0$, $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. Then, all decompositions of A into a product of two mutually isogenous elliptic curves with complex multiplication are obtained as follows: choose a pair (f_1, f_2) of positive integers such that*

$$\gcd(f_1, f_2) = f_0 \qquad \text{and} \qquad f_1 f_2 = n f_0^2,$$

and pick an arbitrary decomposition $A = E_{Q_1} \times E_{Q_2}$, with $Q_1 \in C(D_1)$ and $Q_2 \in C(D_2)$. Then, $A \cong E_{Q_1 \circledast R} \times E_{Q_2 \circledast R^{-1}}$, for all $R \in C(D)$.

Proof. Choose a pair (f_1, f_2) as in the statement, and use Remark 4.1 to obtain a decomposition $A \cong E_1 \times E_2$ with $E_i \in C(D_i)$, $D_i = f_i^2 d_K$ $(i = 1, 2)$. Then, the action of $C(D)$ on the factors of $E_1 \times E_2$ gives us $h(D)$ distinct decompositions (by means of Theorem 4.9). As there are $2^{\tau(n)}$ choices of pairs (f_1, f_2) as above, we find that

$$\tilde{\delta}(A) = 2^{\tau(n)} h(D) = 2^{\tau(n)} h(\mathcal{O}_{K,f}),$$

matching Ma's formula (Corollary 2.3) for the number of decompositions in case $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. Therefore, we have indeed found all possible decompositions of A. □

5. Alternative proof of Ma's formula for $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. The classification of decompositions of singular abelian surfaces has been obtained by producing enough distinct decompositions to match Ma's formula. However, our construction incidentally provides the reader with an alternative and simpler proof of Ma's formula for the number of decompositions in the case $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$.

Let $\Sigma^{\mathrm{Ab}}(D, n)$ be the space of singular abelian surfaces of discriminant D and primitivity index n, i.e. the space of surfaces A such that $\mathrm{T}(A) = nQ_0$, for a primitive form Q_0, and $\operatorname{disc}\mathrm{T}(A) = D$. If we consider all the elements of $\Sigma^{\mathrm{Ab}}(D, n)$ at once, Proposition 4.9 says that we have constructed a total of

$$2^{\tau(n)} h(\mathcal{O}_{K,f_0}) h(\mathcal{O}_{K,f})$$

distinct product surfaces. However, the number of distinct product surfaces within $\Sigma^{\mathrm{Ab}}(D, n)$ is

$$\sum_{A \in \Sigma^{\mathrm{Ab}}(D,n)} \widetilde{\delta(A)} = \sum_{\substack{(f_1,f_2)=f_0 \\ f_1 f_2 = n f_0^2}} h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2}).$$

The following result will allow us to give a new proof of Ma's formula for the number of decompositions of a singular abelian surface (Corollary 2.3).

Proposition 5.1. *Unless $d_K \in \{-3, -4\}$ and $f_0 = 1$, we have*

$$2^{\tau(n)} h(\mathcal{O}_{K,f}) h(\mathcal{O}_{K,f_0}) = \sum_{\substack{(f_1,f_2)=f_0 \\ f_1 f_2 = n f_0^2}} h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2}).$$

Proof. We notice that

$$\begin{aligned} \sum_{\substack{(f_1,f_2)=f_0 \\ f_1 f_2 = n f_0^2}} h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2}) &= 2 \sum_{\substack{(f_1,f_2)=f_0 \\ f_1 f_2 = n f_0^2 \\ f_1 < f_2}} h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2}) \\ &= 2 \sum_{\substack{(f_1,f_2)=f_0 \\ f_1 f_2 = n f_0^2 \\ f_0 \neq f_1 < f_2}} h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2}) + 2h(\mathcal{O}_{K,f_0}) h(\mathcal{O}_{K,f}), \end{aligned}$$

and so it is enough to prove that

$$(2^{\tau(n)-1} - 1) h(\mathcal{O}_{K,f}) = \sum_{\substack{(f_1,f_2)=f_0 \\ f_1 f_2 = n f_0^2 \\ 1 \neq f_1 < f_2}} \frac{h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2})}{h(\mathcal{O}_{K,f_0})};$$

since the number of summands on the right-hand side is precisely $2^{\tau(n)-1} - 1$, we are left to prove that

$$\frac{h(\mathcal{O}_{K,f_1}) h(\mathcal{O}_{K,f_2})}{h(\mathcal{O}_{K,f_0})} = h(\mathcal{O}_{K,f}).$$

But this comes as a consequence of class field theory: by the assumptions, one has

$$[\mathcal{O}_K^\times : \mathcal{O}_{K,f_i}^\times] = \frac{1}{2} \# \mathcal{O}_K^\times, \qquad i = 0, 1, 2, \emptyset.$$

Setting

$$\Pi_i := \prod_{p \mid f_i} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right), \qquad i = 0, 1, 2, \emptyset$$

[2, Theorem 7.24] yields

$$\frac{h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2})}{h(\mathcal{O}_{K,f_0})} = \frac{h(\mathcal{O}_K)f}{\#\mathcal{O}_K^\times/2} \cdot \frac{\Pi_1\Pi_2}{\Pi_0},$$

since $f = nf_0$ and $f_1f_2 = nf_0^2 = ff_0$. However, it is not hard to see that

$$\frac{\Pi_1\Pi_2}{\Pi_0} = \Pi,$$

and therefore the proof is complete. □

Proof of [5, Corollary 5.12]. Our construction of decompositions of a given singular abelian surface A shows that $\tilde{\delta}(A) \geq 2^{\tau(n)}h(\mathcal{O}_{K,f})$. Summing over all $A \in \Sigma^{\mathrm{Ab}}(D,n)$, we get

$$\sum_{A \in \Sigma^{\mathrm{Ab}}(D,n)} \tilde{\delta}(A) \geq 2^{\tau(n)}h(\mathcal{O}_{K,f})h(\mathcal{O}_{K,f_0})$$

$$= \sum_{\substack{(f_1,f_2)=f_0 \\ f_1f_2=nf_0^2}} h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2}) = \sum_{A \in \Sigma^{\mathrm{Ab}}(D,n)} \tilde{\delta}(A).$$

Therefore, $\sum_{A\in\Sigma^{\mathrm{Ab}}(D,n)} \tilde{\delta}(A) = 2^{\tau(n)}h(\mathcal{O}_{K,f})h(\mathcal{O}_{K,f_0})$, and all $A \in \Sigma^{\mathrm{Ab}}(D,n)$ have the same number of decompositions, in particular $\tilde{\delta}(A) = 2^{\tau(n)}h(\mathcal{O}_{K,f})$. □

6. Decompositions in the remaining cases. The techniques employed thus far cannot be employed when $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$. However, we are still able to completely solve the classification problem, and also to give an alternative formula for the number of decompositions of a singular abelian surface. Let A be a singular abelian surface with transcendental lattice $Q = nQ_0$, and let $D = f^2d_K = \operatorname{disc} Q$, $D_0 = f_0^2 d_K = \operatorname{disc} Q_0$, $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})\}$. We will divide the analysis into two cases, depending on f_0.

6.1. Case $f_0 > 1$. Under these hypotheses, we can still use Proposition 4.9 to get $h(D)$ distinct decomposition starting from a given one. By combining this with Proposition 5.1, and reasoning as in the alternative proof of [5, Corollary 5.12] given above, we find that the number of decompositions of A is again $\tilde{\delta}(A) = 2^{\tau(n)}h(D)$. Moreover, all decompositions are obtained exactly as in the proof of Theorem 4.11.

6.2. Case $f_0 = 1$. In this case, we will proceed with a direct analysis case by case. We will consider pairs (f_1, f_2) as above, which now will have the additional property that f_1 and f_2 are relatively prime (because $f_0 = 1$), and thus we will also have $f = n$.

THEOREM 6.1. *In the above setting, the number of decompositions of A into the product of two mutually isogenous elliptic curves with complex multiplication (up to isomorphism of the factors) is*

$$\tilde{\delta}(A) = (1 + 2^{\tau(n)-1})h(\mathcal{O}_{K,n}),$$

if $n > 1$*, and* $\tilde{\delta}(A) = 1$ *otherwise. The surface* A *is isomorphic to any of the products* (E_1, E_2)*, where* $[E_i] \in \mathcal{E}ll(\mathcal{O}_{K,f_i})$ $(i = 1, 2)$*,* $\gcd(f_1, f_2) = 1$ *and* $f_1 f_2 = n$*.*

Proof. If $n = 1$, there is nothing to prove; therefore, we can assume $n > 1$. Since $h(\mathcal{O}_K) = 1$, a formula for the number of decompositions of A can be obtained just by a counting argument, and thus we see that

$$\begin{aligned}\tilde{\delta}(A) &= \sum_{\substack{(f_1,f_2)=1\\ f_1 f_2 = n}} h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2}) = 2 \sum_{\substack{(f_1,f_2)=1\\ f_1 f_2 = n\\ f_1<f_2}} h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2})\\ &= 2 \sum_{\substack{(f_1,f_2)=1\\ f_1 f_2 = n\\ 1\neq f_1<f_2}} h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2}) + 2h(\mathcal{O}_{K,n}).\end{aligned}$$

Following the notation from earlier, since $\#\mathcal{O}_K^\times = 4$, [2, Theorem 7.24] implies that $h(\mathcal{O}_{K,f_i}) = f_i \Pi_i/2$. Therefore, $h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2}) = n\Pi/4$, and thus

$$\begin{aligned}\tilde{\delta}(A) &= (2^{\tau(n)-1} - 1)n\Pi/2 + n\Pi\\ &= \frac{1}{2}n\Pi(1 + 2^{\tau(n)-1}) = (1 + 2^{\tau(n)-1})h(\mathcal{O}_{K,n}).\end{aligned}$$

So we are able to exhibit a formula for the number of decompositions of such a singular abelian surface. Also, the classification problem is solved, as we can just take all pairs (E_1, E_2) (since $h(\mathcal{O}_K) = 1$). ☐

The case $K = \mathbb{Q}(\sqrt{-3})$ is analogous, and thus the proof of Theorem 6.2 is the same, except for the fact that $\#\mathcal{O}_K^\times = 6$. We omit the proof for sake of brevity.

THEOREM 6.2. *Let* A *be a singular abelian surface having transcendental lattice* $Q = nQ_0$*, and let* $D = f^2 d_K = \operatorname{disc} Q$*,* $D_0 = f_0^2 d_K = \operatorname{disc} Q_0$*,* $K = \mathbb{Q}(\sqrt{-3})$*. The number of decompositions of* A *into the product of two mutually isogenous elliptic curves with complex multiplication (up to isomorphism of the factors) is*

$$\tilde{\delta}(A) = \frac{2}{3}(2 + 2^{\tau(n)-1})h(\mathcal{O}_{K,n}),$$

if $n > 1$*, and* $\tilde{\delta}(A) = 1$ *otherwise. The surface* A *is isomorphic to any of the products* (E_1, E_2)*, where* $[E_i] \in \mathcal{E}ll(\mathcal{O}_{K,f_i})$ $(i = 1, 2)$*,* $\gcd(f_1, f_2) = 1$ *and* $f_1 f_2 = n$*.*

6.3. Application: Shioda-Inose models of singular K3 surfaces. Let X be a singular K3 surface, i.e. a K3 surface of maximum Picard number, and let $\mathrm{T}(X)$ denote its transcendental lattice. By results of Shioda and Inose [9], there exists a singular abelian surface $A = E_1 \times E_2$ such that $\mathrm{T}(A) = \mathrm{T}(X)$. Moreover, there is a model of X which is given in terms of the j-invariants of E_1 and E_2. In his work, Inose [3] provides explicit equations for a Shioda-Inose model in terms of the j-invariants of the factors of a singular abelian surface. More recently, Schütt [7] has improved Inose's result, by showing that X has the following model as an elliptic fibration

$$X: \qquad y^2 = x^3 - 3\alpha\beta t^4 x + \alpha\beta t^5(\beta t^2 - 2\beta t + 1),$$

where $\alpha = j_1 j_2$ and $\beta = (1 - j_1)(1 - j_2)$, j_k being the j-invariant of E_k, and the j-invariant being normalized to $j(i) = 1$. It follows that our classification of the decompositions of a singular abelian surface gives all the possible Shioda-Inose models of X, i.e. all the possible models of X which are realizable via a Shioda-Inose structure.

6.4. Open problems. The present treatment has dealt with decompositions of singular abelian surfaces, but one might want to investigate the possible decompositions in the case of singular abelian varieties of higher dimension. It was proven by Katsura [4] that such a variety is isomorphic to the product of mutually isogenous elliptic curves with complex multiplication.

PROBLEM 6.3. Given a singular abelian variety A,

(1) find a formula for the number of decompositions of A into a product of mutually isogenous elliptic curves with complex multiplication;
(2) classify all such decompositions explicitly.

It is our intention to pursue these problems in the near future.

REFERENCES

[1] B. Allombert, Y. Bilu, and A. Pizarro-Madariaga, *CM-Points on Straight Lines*, arXiv:1406.1274, June 2014.

[2] D. A. Cox, *Primes of the form $x^2 + ny^2$*, Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[3] H. Inose, *Defining equations of singular $K3$ surfaces and a notion of isogeny*, in "Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977)", pp. 495–502. Kinokuniya Book Store, Tokyo, 1978.

[4] T. Katsura, *On the structure of singular abelian varieties*, Proc. Japan Acad., 51:4 (1975), pp. 224–228.

[5] S. Ma, *Decompositions of an Abelian surface and quadratic forms*, Ann. Inst. Fourier (Grenoble), 61:2 (2011), pp. 717–743.

[6] D. R. Morrison, *On K3 surfaces with large Picard number*, Inventiones mathematicae, 75:1 (1984), pp. 105–121.

[7] M. Schütt, *Fields of definition of singular $K3$ surfaces*, Commun. Number Theory Phys., 1:2 (2007), pp. 307–321.

[8] T. Shioda, *The period map of Abelian surfaces*, J. Fac. Sci. Univ. Tokyo Sect. IA Math., 25:1 (1978), pp. 47–59.

[9] T. Shioda and H. Inose, *On singular $K3$ surfaces*, in "Complex analysis and algebraic geometry", pp. 119–136. Iwanami Shoten, Tokyo, 1977.

[10] T. Shioda and N. Mitani, *Singular abelian surfaces and binary quadratic forms*, in "Classification of algebraic varieties and compact complex manifolds", pp. 259–287. Lecture Notes in Math., Vol. 412. Springer, Berlin, 1974.