Picard numbers of abelian varieties and related arithmetic

Von der Fakultät für Mathematik und Physik
der Gottfried Wilhelm Leibniz Universität Hannover
zur Erlangung des Grades

Doktor der Naturwissenschaften
Dr. rer. nat.

genehmigte Dissertation

von

Roberto Laface
geboren am 11. Juni 1990 in Reggio Calabria, Italien

— 2016 —

Referent:

Prof. Dr. Matthias Schütt (Leibniz Universität Hannover)

Korreferenten:

Prof. Dr. François Charles (Université Paris-Sud, Paris, Frankreich)
Prof. Dr. Lambertus van Geemen (Universitá degli Studi di Milano, Italien)

Tag der Promotion:

28. Oktober 2016

Zusammenfassung

Die vorliegende Arbeit befasst sich mit Picard-Zahlen von abelschen Varietäten und einigen verwandten arithmetischen Phänomenen. Eine Motivation hierfür bildet die Tatsache, dass singuläre abelsche Flächen, das heißt abelsche Flächen mit maximaler Picard-Zahl, mit einer zusätzlichen arithmetischen Struktur ausgestattet sind. Diese Struktur ist in dem transzendentalen Gitter kodiert und überträgt sich auf singuläre K3 Flächen mittels der Shioda-Inose Strukturen.

Zuerst konzentrieren wir uns darauf, alle möglichen Zerlegungen einer singulären abelschen Fläche in ein Produkt von zueinander isogenen elliptischen Kurven mit komplexer Multiplikation zu finden. Hierbei nutzen wir eine Verallgemeinerung der Dirichlet Komposition, welche die Komposition von quadratischen Formen verschiedener Diskriminante ermöglicht. Unser Resultat ist eine Verallgemeinerung einer vorangegangenen Arbeit von Ma, der eine Formel für die Anzahl solcher Zerlegungen gefunden hat. Gleichzeitig liefert unser Ansatz einen alternativen Beweis für die Formel von Ma.

Darauf aufbauend untersuchen wir den (relativen und absoluten) Körper der Moduli von singulären K3 Flächen. Wir verwenden eine Idee von Šafarevič, um unser Problem auf das entsprechende Problem über singuläre abelsche Flächen zu reduzieren. Dies ermöglicht uns die CM-Theorie von elliptischen Kurven anzuwenden, denn nach der Arbeit von Shioda und Mitani ist jede singuläre abelsche Fläche das Produkt von zwei solchen Kurven. Abgesehen von der abstrakten Charakterisierung sind wir in der Lage, eine explizite Beschreibung des Körpers der Moduli zu geben, wodurch diese mittels eines Computeralgebrasystems berechnet werden können.

Schließlich untersuchen wir die möglichen Picard-Zahlen einer komplexen abelschen Varietät einer fixierten Dimension. Für Dimension g ist eine Einschränkung der Picard-Zahl durch das Lefschetz Theorem von $(1,1)$-Klassen gegeben. Es stellt sich die Frage, ob alle ganzen Zahlen ρ mit $1 \leq \rho \leq h^{1,1}$ als Picard-Zahl einer g-dimensionalen abelschen Varietät auftreten können. Wir zeigen, dass dies überraschenderweise nicht zutrifft für $g \geq 3$, und berechnen die ersten zwei Folgen von Lücken in der Menge der Picard-Zahlen für jede Dimension g.

Schlüsselwörter: Picard-Zahl, abelsche Fläche, K3 Fläche, Klassenkörper Theorie, komplexe Multiplikation, quadratische Formen, abelsche Varietäten

Abstract

This dissertation focuses on the Picard numbers of abelian varieties and some related arithmetic phenomena. The motivation lies in the fact that singular abelian surfaces, i.e. abelian surfaces attaining the maximum Picard number, are equipped with extra arithmetic structure. This structure is encoded in the transcendental lattice, and it carries over to singular K3 surfaces by means of Shioda-Inose structures.

A first problem we were interested in was finding all possible decompositions of a singular abelian surface into a product of mutually isogenous elliptic curves with complex multiplication. A key tool is a generalization of the Dirichlet composition, which allows one to compose quadratic forms of different discriminant. Our result is a generalization of previous work of Ma, who found a formula for the number of such decompositions. Incidentally, our approach also yields a new proof of Ma's formula.

Building on this, we studied the (relative and absolute) field of moduli of singular K3 surfaces. By using an idea of Šafarevič, we reduce our problem to the corresponding one on singular abelian surfaces. This technique enables us to use the CM theory of elliptic curves, as every singular abelian surface is always the product of two such curves, by results of Shioda and Mitani. Besides the abstract characterization, we were able to give an explicit description of the field of moduli, which allows to compute it by means of a computer algebra system.

Finally, we investigated the possible Picard numbers of a complex abelian variety of a fixed dimension. In dimension g, a restriction on the Picard number is given by the Lefschetz theorem of $(1,1)$-classes, and the question is actually asking whether all integers in the range $1 \leq \rho \leq h^{1,1}$ can appear as the Picard number of a g-dimensional abelian variety. To our surprise, we show that this is not the case for every $g \geq 3$, and we computed the first two sequences of gaps in the set of Picard numbers in any dimension.

Keywords: Picard number, abelian surface, K3 surface, class field theory, complex multiplication, quadratic forms, abelian varieties.

Contents

Acknowledgements

I would like to thank my supervisor Matthias Schütt for his constant encouragement during the past three years, for always agreeing to my many travelling plans, and for his advice on my future plans as a post-doc.

It is my pleasure to express my gratitude to Klaus Hulek, from whom I learnt and I keep learning a lot, for our many mathematical discussions, for listening to my problems and ideas, and for his invaluable opinion.

I would like to warmly thank François Charles for having me as a guest at the *IHÉS* during Spring 2016, time where I had the chance to learn a lot and the pleasure to enjoy our many conversations.

Parts of this work have grown out of discussions with Bert van Geemen, whose keen interest in my questions has motivated me in pursuing some of the results in this dissertation. I wish to thank him for dedicating time to me and for his crystal clear explanations.

Both the *Institut für Algebraische Geometrie* and the *GRK 1463 "Analysis, Geometry and String Theory"* have contributed to my education because of their lively environment and the generous fundings, which are here gratefully acknowledged. I also wish to thank all members of these research groups for the many beautiful experiences during the past three years and their memories, which I will always cherish.

Last but certainly not least, my deepest thanks go to my family, which keep supporting me everyday of my life with their love, and to whom I dedicate this work.

Introduction

> Thinking of you, wherever you are. We pray for our sorrows to end, and hope that our hearts will blend. Now I will step forward to realize this wish. And who knows: Starting a new journey may not be so hard, or maybe it has already begun. There are many worlds, but they share the same sky. One sky, one destiny.
>
> Kairi, *Kingdom Hearts II*

Motivation

This dissertation grew out of the investigation of certain aspects of the geometry and the arithmetic of singular K3 surfaces, i.e. K3 surfaces with maximum Picard number over $\mathbb{C}$. The reason for this somewhat confusing name is explained, to the best of the author's knowledge, in a paper of Ulf Persson [26]: in Russian, the word особый (*osobyi*) is used in the precise sense of non-smooth (e.g. a singular point), and сингулярный (*singulyarnyi*), is instead used in the vaguer sense of exceptional, peculiar (singular). Unfortunately, both terms translate into "singular" in English, and, at the same time, the word "extremal" already described a different notion in the theory of elliptic surfaces (see [27], [2], [22]).

Among the reasons why one should be interested in studying singular K3 surfaces, the most natural is that they represent a possible two-dimensional analog of elliptic curves with complex multiplication (CM). A classical result, proofs of which were given (for instance) by Serre [32] and Serre-Tate [33], states that every elliptic curve with CM is defined over a number field. Also, if one fixes a positive integer $n \in \mathbb{N}$, one can show that the set

$$\left\{\text{CM elliptic curves defined over } K,\ [K:\mathbb{Q}] \leq n\right\} / \cong_{\mathbb{C}}$$

is finite, i.e. that the set of isomorphism classes of CM elliptic curves with bounded field of definition is finite.

These results (and many others) carry over to singular K3 surfaces in a natural way. For example, work of Shioda and Inose [38] has revealed that singular K3 surfaces have a model over a number field, a result later refined by Inose [13] and Schütt [28]. Moreover, Šafarevič [34] proved a finiteness result for singular K3 surfaces with bounded field of definition, i.e. that the set

$$\left\{\text{singular K3 surfaces defined over } K,\, [K:\mathbb{Q}] \leq n\right\} / \cong_{\mathbb{C}}$$

is finite. A feature of this latter result is that the proof uses a reduction to the case of singular abelian surfaces, which in turn uses results from the theory of CM elliptic curves. Reduction to abelian varieties and elliptic curves is a technique we will make use of extensively in this thesis.

Having described some aspects of the arithmetic of singular K3 surfaces, we would like to say something about their geometry, and in particular about their connection to singular abelian surfaces. Both in the case of singular abelian and K3 surfaces, their large Néron-Severi lattice allows one to construct arithmetically interesting moduli[1]. This was first explored by Shioda and Mitani [39], who described the set Σ_{Ab} of moduli of singular abelian surfaces in terms of quadratic forms. To any singular abelian surface, one can associate its oriented transcendental lattice, which in this case acquires the structure of a positive definite lattice, and thus it can be interpreted as a positive definite integral binary quadratic form. If $\mathcal{Q}^+$ denotes the set of positive definite integral binary quadratic forms, then the association above yields a one-to-one correspondence

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

which, for us, is the bridge between the arithmetic of quadratic forms (based on class group theory) and the geometry of singular abelian surfaces.

One can analogously build the set Σ^{K3} of moduli of singular K3 surfaces, and ask for its structure. In their paper, Shioda and Mitani [39] showed that by taking the Kummer surface of a singular abelian surface, one is able to recover all singular K3 surfaces whose transcendental lattice has primitivity index which is divisible by 2. Later, Shioda and Inose [38] proved the surjectivity of the period map for singular K3 surfaces by means of *Shioda-Inose* structures (as Morrison later called them in [23]): if A is an abelian surface, a Shioda-Inose structure associated to A is a K3 surface $X = SI(A)$, which is a 2:1 cover of $\operatorname{Km}(A)$ and has the property that $\mathrm{T}(X) = \mathrm{T}(A)$.

$$\begin{tikzcd} A \arrow[r, dashed, "2:1"] & \operatorname{Km}(A) & X \arrow[l, dashed, "2:1"'] \end{tikzcd}$$

It turns out that also (isomorphism classes of) singular K3 surfaces are uniquely characterized by their transcendental lattice, and thus there exists a one-to-one correspondence between Σ_{Ab} and Σ_{K3} given by Shioda-Inose structures; in particular, this implies that two singular abelian surfaces are isomorphic if and only if the corresponding

[1] By moduli we mean $\mathbb{C}$-isomorphism classes.

K3 surfaces via a Shioda-Inose structure are. In the following, we will be using this fact to reduce a problem on singular K3 surfaces to one on the conrresponding singular abelian surfaces via a Shioda-Inose structure.

At this point it should be clear to the reader that the Picard number, if large enough, may equip a variety with extra (arithmetic) structure, and thus it is an interesting numerical invariant to study. In general, computing the Picard number of a given variety is a very hard task; sometimes, this can be accomplished if one adds, for instance, (many) automorphisms, (elliptic) fibrations, etc. A somewhat easier question may be: given a class of varieties (for instance, with specified numerical invariants), what are the possible Picard number that can appear? However, already in relatively easy cases, this question remains still difficult to answer. For example, a full answer is not known in the case of smooth quintic surfaces in $\mathbb{P}^3$, while it is if one allows quintic surfaces to have ADE-singularities (see [29], [30]).

Problems and results

Chapters 2 and 3 of this work are devoted to the study of certain aspects of the geometry and the arithmetic of singular abelian and K3 surface. The techniques we use exploit the deep connections to class field theory, the theory of quadratic forms and the CM theory of elliptic curves that we have presented above. In Chapter 2, we study the problem of classifying all decompositions of a singular abelian surface into a product of mutually isogenous CM elliptic curves. Let us notice that this question perfectly makes sense in light of the results of Shioda and Mitani [39] that we have mentioned earlier. A formula for the number of decompositions of an abelian surface of arbitrary Picard number was found by Ma [19]; therein, he also classified the possible decompositions for abelian surfaces of Picard number $\rho \leq 3$, leaving open the case of singular abelian surfaces, which is the main object of our studies. Indeed, we successfully classify such decompositions, by developing a tool called *generalized Dirichlet composition*: it is a generalization of the usual Dirichlet composition of quadratic forms of given discriminant to pairs of forms with possibly different discriminants. This allows to exploit the reduction maps between class groups of different discriminant, as well as results from class field theory, to explicitly compute the transcendental lattice of an arbitrary product of mutually isogenous CM curves (Proposition 2.2.4), hence generalizing previous work of Shioda and Mitani [39]. Afterwards, we apply this technique to study the possible decompositions of a singular abelian surface. Our analysis distinguishes two cases, according to the CM field K of our abelian surface: if $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, then we are able to build enough decompositions to match Ma's formula (Theorem 2.3.11). On the other hand, if $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$, then we have to proceed with a case-by-case argument (Theorems 2.5.1 and 2.5.2). Incidentally, our approach turns out to be completely independent of Ma's work [19] and, in fact, it yields an alternative proof of the formula for the number of decompositions.

The results accomplished in Chapter 2 allow us to study the field of moduli of singular K3 surfaces, which is the main topic of Chapter 3. Our interest stems from the fact that the field of moduli of a singular K3 surface (and in general, of an arbitrary variety) is contained in every field of definition. A result of Schütt, who generalized previous work of Shimada [35], states the following: letting K be the CM field of a singular K3 surface X, i.e. $K = \mathbb{Q}(\sqrt{\operatorname{disc} \mathrm{T}(X)})$, the set of $\mathbb{C}$-isomorphism classes of Galois conjugates of X under $\mathrm{Gal}(\mathbb{C}/K)$ is in one-to-one correspondence with the genus of $\mathrm{T}(X)$ seen as a quadratic form, i.e.

$$\{[X^\sigma] \mid \sigma \in \mathrm{Gal}(\mathbb{C}/K)\} \longleftrightarrow \big(\text{genus of } \mathrm{T}(X)\big).$$

In particular, this suggests that the field of K-moduli M_K might be a degree $g := \#\big(\text{genus of } \mathrm{T}(X)\big)$ extension of K. Indeed, this is the case, as we are able to prove; moreover, M_K/K is always a Galois extension (Theorem 3.4.4). The proof of this result is divided into two steps: first, we solve the case where the transcendental lattice is primitive, and then we use results for the theory of CM to prove some compatibility conditions, that allow to extend the proof the general case. Our methods also enable us to explicitly compute the field of K-moduli as a finite extension of K, in a way that unlocks the computational side of the problem: it turns out that the field of K-moduli is always the subfield of the ring class field H of the order of discriminant $\operatorname{disc} \mathrm{T}(X)$ in K that is fixed by the 2-torsion elements of $\mathrm{Gal}(H/K)$ (Proposition 3.6.5), i.e.

$$M_K = H^{\mathrm{Gal}(H/K)[2]}.$$

We also study the dependence of the field of K-moduli on the index of primitivity of the transcendental lattice, and we prove, among other things, that in fact the field of K-moduli is independent of it (Proposition 3.6.2). Afterwards, we turn our focus to the study of the field of $\mathbb{Q}$-moduli, which is indeed a degree g extension of $\mathbb{Q}$, but, contrary to the field of K-moduli, it is not Galois in general (Theorem 3.5.3), and we extend other results valid for the field of K-moduli to the field of $\mathbb{Q}$-moduli.

The last chapter of this dissertation reports on a joint work (partly in progress) with Klaus Hulek [10]. We focus our attention on the problem of which Picard number can appear within a given class of varieties, and, in particular, we study the case of varieties with (numerically) trivial canonical bundle. Let us begin with the case of surfaces, where an answer to this problem is already known. For abelian surfaces all possible Picard numbers between 1 (or 0 if one includes the non-algebraic case) and 4 occur. For the other surfaces with trivial canonical bundle the situation is similar: for K3 surfaces all possibilities between 1 (respectively 0) and 20 can occur as can be seen by the Torelli theorem for K3 surfaces and the Lefschetz $(1,1)$-theorem. Enriques surfaces and bi-elliptic surfaces have $p_g = 0$ and their Picard number is 10 and 2 respectively. Moving to higher dimension, by the Beauville-Bogomolov decomposition theorem [4], every Kähler manifold with trivial first Chern class admits a finite cover which is a product of tori, Calabi-Yau varieties and irreducible holomorphic symplectic manifolds (IHSM), also know as hyperkähler manifolds. For higher dimensional

Calabi-Yau varieties Y we always have $\rho(Y) = b_2(Y)$ as $h^{2,0}(Y) = h^{0,2}(Y) = 0$. For IHSM one can use Huybrechts' surjectivity of the period map [11] to conclude, as in the case of K3 surfaces, that all values $1 \leq \rho(X) \leq b_2(X) - 2$ can be obtained. This leaves us with the case of abelian varieties which is the main topic of Chapter 4. For a g-dimensional abelian variety, the Picard number must satisfy the following restriction:

$$1 \leq \rho \leq h^{1,1} = g^2.$$

Very little seems to be know about the set R_g of realizable Picard numbers of g-dimensional abelian varieties. Our aim is to take a first step in the analysis of the set R_g. In particular, we show that there are series of gaps for the possible Picard numbers of abelian varieties, and we explicitly compute the first two of them. In particular, we prove that for dimension $g \geq 7$, the three largest values of the Picard number are $(g-2)^2 + 4$, $(g-1)^2 + 1$ and g^2 (Main Theorem of Chapter 4).

Structure of the dissertation

The present thesis is divided into four chapters.

Chapter 1 is merely meant for later reference, and contains some of the main ideas and results to be used later on.

Chapter 2 is an adaption of [16], and deals with the problem of classifying the decompositions of a singular abelian surface into a product of elliptic curves.

Chapter 3 discusses the results obtained in [17] about the field of moduli of singular K3 surfaces.

Chapter 4 contains a study of the possible Picard numbers for abelian varieties of arbitrary dimension, which is part of the forthcoming paper [10] joint with Klaus Hulek.

Chapter 1

Preliminaries

> And I've been telling Yuna "Let's go to Zanarkand together", "Let's beat Sin". I told her all the things...we could...we could...and all along the whole time, I didn't know anything! But Yuna, she'd...just smile.
>
> Tidus, *Final Fantasy X*

The aim of this chapter, mainly meant for later reference, is to recall the basic properties of the main objects of the present treatment, together with some of the techniques we will employ later. Unless otherwise specified, all fields are of characteristic zero.

1.1 Quadratic forms, class groups and elliptic curves

We introduce the classical class group of quadratic forms of given discriminant and the ideal class group from algebraic number theory; also, we discuss their mutual interplay, as well as their relation to elliptic curves. For a beautiful account on the subject, see [8].

1.1.1 Form class group

The theory of integral binary quadratic forms began with Lagrange [18], and it was later continued by Gauß [9], who introduced new ideas into the theory, in particular the notion of proper equivalence of forms.

An *(integral binary) quadratic form* is an expression of the form

$$Q(x,y) = ax^2 + bxy + cy^2, \qquad a,b,c \in \mathbb{Z}.$$

the quantity $\gcd(a,b,c)$ is called *index of primitivity* and Q is said *primitive* if $\gcd(a,b,c) = 1$. Sometimes, it is convenient to extract the *primitive part* of a form Q: this is the quadratic form Q_0 such that $mQ_0 = Q$, m being the index of primitivity of Q. A form Q *represents* $m \in \mathbb{Z}$ if $m = Q(x,y)$ for some $x, y \in \mathbb{Z}$; if moreover $\gcd(x,y) = 1$, then we say that Q *properly represents* $m \in \mathbb{Z}$. A quadratic form Q as above will be denoted in short by $Q = (a,b,c)$. Two forms $Q = (a,b,c)$ and $Q' = (a',b',c')$ are equivalent (properly equivalent, respectively) if there exists $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ ($\mathrm{SL}_2(\mathbb{Z})$, respectively) such that

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

The following basic results give a hint on why it is important to know which numbers a form represents.

Lemma 1.1.1 (Lemma 2.3 in [8]). *A form Q properly represents $m \in \mathbb{Z}$ if and only if Q is properly equivalent to the form (m, B, C), for some $B, C \in \mathbb{Z}$.*

Lemma 1.1.2 (Lemma 2.25 in [8]). *Given a form Q and an integer M, Q represents infinitely many numbers prime to M.*

The *discriminant* of a form $Q = (a,b,c)$ is the integer $D := b^2 - 4ac$. The set of proper equivalence classes of primitive forms of discriminant D is called the *(form) class group of discriminant D*, and it is denoted by $C(D)$; we will denote the class of a form Q by $[Q]$, or simply by Q if there is no risk of confusion arising.

1.1.2 Dirichlet composition

The class group is equipped with the *Dirichlet composition* of forms: by [8, Lemma 3.2], if $Q = (a,b,c)$ and $Q' = (a',b',c')$ are primitive forms of discriminant D such that

$$\gcd\left(a, a', \frac{b+b'}{2}\right) = 1, \tag{$\star$}$$

then the composition $Q * Q'$ is the form (aa', B, C), where $C = \frac{B^2-D}{4aa'}$ and B is the integer, unique modulo $2aa'$, such that

$$\begin{cases} B \equiv b \mod 2a, \\ B \equiv b' \mod 2a', \\ B^2 \equiv D \mod 4aa'. \end{cases}$$

Naturally, we put $[Q] * [Q'] := [Q * Q']$. Notice that two arbitrary primitive forms of the same discriminant are not always composable, as they might not satisfy the condition ($\star$). However, by considering their classes, we can use Lemma 1.1.2 to change the representative and ensure that condition ($\star$) be fulfilled.

1.1.3 Elliptic curves

An *elliptic curve* E over a field k is a complete smooth genus 1 curve with the choice of a k-rational point $O \in E(k)$. One readily sees that the canonical sheaf of E is trivial, i.e. $\omega_E \cong \mathcal{O}_E$. Moreover, E comes equipped with a group law on its k-rational points for which O is the neutral element (see, for example, [41, Ch. 3]). Among other features, elliptic curves are always projective, as one can use Riemann-Roch theorem to embed them into $\mathbb{P}^2$ as smooth cubics. Their equation in $\mathbb{P}^2$ is called the *Weierstraß model* of E, and it can be written in the form

$$y^2 = x^3 + Ax + B,$$

for $A, B \in k$ such that the discriminant

$$\Delta_E := -16(4A^3 + 27B^2)$$

is non-zero. Over an algebraically closed field k, elliptic curves are classified by the j-invariant

$$j_E := -1728\frac{(4A)^3}{\Delta},$$

and their moduli space $\mathcal{M}_{1,1}$ is isomorphic to $\mathbb{A}^1_k$. An elliptic curve has many automorphisms, due to the presence of translations by a point. However, if we are interested in the group $\mathrm{Aut}_0(E)$ of those automorphisms preserving the group structure (i.e. those sending $O \longmapsto O$), then there are very few:

(i) $\mathrm{Aut}_0(E) = \mathbb{Z}/2\mathbb{Z}$, for $j \neq 0, 1728$;

(ii) $\mathrm{Aut}_0(E) = \mathbb{Z}/4\mathbb{Z}$, for $j = 1728$;

(iii) $\mathrm{Aut}_0(E) = \mathbb{Z}/6\mathbb{Z}$, for $j = 0$.

Turning to endomorphism (as a group variety), the situation is much richer. Recall that, 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. There are two cases:

(i) $\mathrm{End}(E) = \mathbb{Z}$, generated by the multiplication-by-n maps $[n] : E \longrightarrow E$, for $n \in \mathbb{Z}$;

(ii) $\mathrm{End}(E) = \mathcal{O}$, where $\mathcal{O}$ is an order in a quadratic imaginary field K.

In the second case, we will say that E has *complex multiplication* (CM) by $\mathcal{O}$. This terminology stems from the fact that all elements in $\mathcal{O} \setminus \mathbb{Z}$ are genuinely complex, and it is best understood by looking at an elliptic curve as a complex torus of dimension one. We will see that, for us, the most arithmetically interesting elliptic curves are those having CM. For example, the j-invariant of a CM elliptic curve is always an algebraic integer (see [40, Ch. 2]).

1.1.4 Ideal class group

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; we will denote the order of conductor f in $\mathcal{O}_K$ by $\mathcal{O}_{K,f}$. Similarly, a *module* M in K is a rank-two $\mathbb{Z}$-submodule of K (no condition on the unity). Two modules M_1 and M_2 are equivalent ($M_1 \sim M_2$) if they are homothetic, i.e. there exists $\lambda \in K$ such that $\lambda M_1 = M_2$. To any module M, we can associate its *complex multiplication* (CM) *ring*[1]

$$\mathcal{O}_M := \{x \in K \mid xM \subseteq M\}.$$

Notice that $\mathcal{O}_M$ is an order in K, and that equivalent modules in K have the same CM ring. The product module M_1M_2 is defined in a natural way, and if f_i is the conductor of M_i ($i = 1, 2$), then $\mathcal{O}_{M_1M_2} = \mathcal{O}_{K,(f_1,f_2)}$, the latter being the order of conductor (f_1, f_2) in K.

Given an order $\mathcal{O}_{K,f}$, one can define the *(ideal) class group* $C(\mathcal{O}_{K,f})$ (see [8, 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 1.1.3 (Theorem 7.7 in [8]). *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*

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

The order of the class group $C(\mathcal{O}_{K,f})$ is called the *class number* of $\mathcal{O}_{K,f}$, and it is denoted by $h(\mathcal{O}_{K,f})$ or $h(D)$, by virtue of Theorem 1.1.3. There is a beautiful formula that describes the order of the class group of an order in terms of its conductor and the maximal order that contains it.

Theorem 1.1.4 (Theorem 7.24 in [8]). *Let $\mathcal{O}_{K,f}$ be the order of conductor f in $\mathcal{O}_K$. Then*

$$h(\mathcal{O}_{K,f}) = \frac{h(\mathcal{O}_K) \cdot f}{[\mathcal{O}_K^\times : \mathcal{O}_{K,f}^\times]} \prod_{p \mid f} \left(1 - \left(\frac{d_K}{p}\right)\frac{1}{p}\right),$$

where p runs over the primes dividing the conductor f.

1.1.5 Elliptic curves vs. quadratic forms vs. ideal classes

Over $\mathbb{C}$, an elliptic curve E can be seen as $E = \mathbb{C}/\Lambda$, 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 homotetic as lattices if and only if they determine the same class in $C(\mathcal{O}_{K,f})$ (see [8, Exercise 10.15]). This results in the following

[1] The name CM ring refers to the property $\mathcal{O}_M = \mathrm{End}(\mathbb{C}/M)$.

Proposition 1.1.5 (Corollary 10.20 of [8])**.** *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 1.1.3 and Proposition 1.1.5, 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 $\mathbb{Z} + \tau\mathbb{Z}$.

1.2 Singular abelian surfaces and singular K3 surfaces

1.2.1 Higher dimensional analogs of elliptic curves

If one wishes to generalize elliptic curves to dimension two, there are at least three ways to do so: K3 surfaces, abelian surfaces and elliptic surfaces. We briefly recall their definitions and properties, and we also point out some useful references.

K3 surfaces

One way to generalize elliptic curves to dimension two is to require (at least) that the canonical sheaf be trivial. This being said, one defines a *K3 surface* as a complex or algebraic smooth minimal complete surface that is simply connected and has trivial canonical bundle. K3 surfaces have been extensively studied both from a geometric and an arithmetic point of view: for a beautiful account, see [12]. Over the complex numbers, lattice polarized K3 surfaces and their moduli spaces are still a very active research areas: for an introduction, see [3].

Abelian surfaces

If it is the group law that we wish to preserve when passing to dimension two, then we obtain the so-called *abelian surfaces*. An abelian surface A over k is a two-dimensional complete connected group variety over k. Notice that abelian surfaces have trivial canonical bundle. Abelian surfaces, and in general *abelian varieties*, over $\mathbb{C}$ have a richer structure as they can be seen as *complex tori*. In particular, this allows one to study them by means of linear algebra and lattice theory. These approaches have been exploited particularly in the study of their moduli spaces. For a classical reference on the general theory, see [24]; for the theory over the complex numbers, an excellent reference is [7].

Elliptic surfaces

One further way to proceed in generalizing elliptic curves is to consider them in families: this leads to the notion of *elliptic surface*. An elliptic surface is a flat morphism $f : S \longrightarrow C$ such that the general fiber is a smooth curve of genus 1 (not necessarily an elliptic curve, as there is no choice of a point), and no fiber contains (-1)-curves (so it is *relatively minimal*). If we want to require that the general fiber of f be an elliptic curve, we need to coherently choose a point in each fiber: this amounts to giving a *section* of f, i.e. a morphism $\sigma : C \longrightarrow S$ such that $f \circ \sigma = \mathrm{id}_C$. A basic but fundamental fact is that the existence of a section equips an elliptic fibration with a (local) Weierstraß model, thanks to which one is able to see such a surface as an elliptic curve over the function field $k(C)$, k being the ground field. According to the Enriques-Kodaira classification, elliptic surfaces can have Kodaira dimension $\kappa \in \{-\infty, 0, 1\}$; in particular, some of them will be K3 surfaces, and these are usually called *elliptic K3 surfaces*. For a reference see [22], or the more recent [31].

1.2.2 Singular surfaces in general

We now recall some basics on singular surfaces, and, to this end, let us work over the field $\mathbb{C}$ of complex numbers. If X is a smooth algebraic surface, we can define the Néron-Severi lattice of X: it is the group of divisors on X, modulo algebraic equivalence, namely

$$\mathrm{NS}(X) := \mathrm{Div}(X) / \sim_{\mathrm{alg}},$$

together with the restriction of the intersection form on $\mathrm{H}^2(X, \mathbb{Z})$. Its rank $\rho(X) := \operatorname{rank} \mathrm{NS}(X)$ is called *Picard number* of X; the Picard number measures how many different curves lie on a surface. By the Lefschetz theorem on $(1,1)$-classes, we have the bound

$$\rho(X) \leq h^{1,1}(X) = b_2(X) - 2p_g(X),$$

where $b_2(X) := \operatorname{rank} \mathrm{H}^2(X, \mathbb{Z})$ and $p_g(X) := \dim_{\mathbb{C}} \mathrm{H}^0(X, \omega_X)$. We can consider the lattice

$$\mathrm{H}^2(X, \mathbb{Z})_{\mathrm{free}} := \mathrm{H}^2(X, \mathbb{Z}) / (\mathrm{torsion}),$$

and since $\mathrm{NS}(X) \subset \mathrm{H}^2(X, \mathbb{Z})$, also $\mathrm{NS}(X)_{\mathrm{free}} \subset \mathrm{H}^2(X, \mathbb{Z})_{\mathrm{free}}$. The lattice $\mathrm{NS}(X)_{\mathrm{free}}$ has signature $(1, \rho(X) - 1)$; its orthogonal complement $\mathrm{T}(X) \subset \mathrm{H}^2(X, \mathbb{Z})_{\mathrm{free}}$ is called the *transcendental lattice* of X, and it has signature

$$(2p_g(X), h^{1,1}(X) - \rho(X)).$$

A smooth algebraic surface with maximum Picard number, i.e. $\rho(X) = h^{1,1}(X)$, is called a *singular surface*. In this case, the transcendental lattice acquires the structure of a positive definite lattice of rank $2p_g(X)$. Both in the case of singular abelian surfaces and singular K3 surfaces, $\mathrm{T}(X)$ is a positive definite rank-two lattice. For further interesting properties of singular surfaces and their generalizations, we refer the reader to [5].

1.2.3 Periods of abelian surfaces

We now recall the notion of period of an abelian surface A (not necessarily singular); details can be found in [37]. The morphism $\mathbb{Z} \longrightarrow \mathcal{O}_A$ yields in cohomology a map

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

since $p_g(A) = 1$; the map p_A is called *the period of A*. By using the structure of complex torus of $A = \mathbb{C}^2/\Lambda$ ($\Lambda \in M_{2\times 4}(\mathbb{C})$), we make this more explicit: since

$$\mathrm{H}^2(A, \mathbb{Z}) \cong \bigwedge^2 \mathrm{H}^1(A, \mathbb{Z}) \qquad \text{and} \qquad \mathrm{H}^1(A, \mathbb{Z}) = \mathrm{H}_1(A, \mathbb{Z})^\vee,$$

we can take a basis $\{v_1, v_2, v_3, v_4\}$ of $\Lambda \cong \mathrm{H}_1(A, \mathbb{Z})$ (typically, the columns of the period matrix Λ of A) and the corresponding dual basis $\{u^1, u^2, u^3, u^4\}$ of $\mathrm{H}^1(A, \mathbb{Z})$. Then, setting $u^{ij} := u^i \wedge u^j$, we get a basis of $\mathrm{H}^2(A, \mathbb{Z})$ by considering

$$\{u^{ij} \,|\, 1 \leq i < j \leq 4\},$$

which also gives a basis of $\mathrm{H}^2(A, \mathbb{C})$. As an element of $\mathrm{H}^2(A, \mathbb{C}) \cong \mathrm{Hom}(\mathrm{H}_2(A, \mathbb{Z}), \mathbb{C})$, the period has the following description:

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

where the notation $(v_i|v_j) \in M_{2\times 2}(\mathbb{C})$ indicates the matrix whose columns are v_i and v_j (seen as vectors). Upon using Poincaré duality, p_A can be seen as

$$p_A : \mathrm{H}^2(A, \mathbb{Z}) \longrightarrow \mathbb{C}.$$

Notice that, since $\mathrm{NS}(A) = \ker(p_A)$ and $\mathrm{T}(A) = (\ker(p_A))^\perp$, this allows us to explicit compute the Néron-Severi and the transcendental lattices. Also, the period satisfies the period relations

$$(p_A, p_A) = 0 \qquad \text{and} \qquad (p_A, \overline{p_A}) > 0.$$

1.2.4 Two interesting spaces of singular surfaces

Let Σ^{Ab} be the set moduli of singular abelian surfaces, i.e. the set of isomorphism classes of singular abelian surfaces; in [39], 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 an ordered basis $\{t_1, t_2\}$ of $\mathrm{T}(A)$ is *positive* if

$$\mathrm{Im}(p_A(t_1)/p_A(t_2)) > 0,$$

and $\mathrm{T}(A)$ with a choice of a positive basis is said to be *positively oriented*. Notice that the transcendental lattice $\mathrm{T}(A)$ is an even lattice, and after choosing a basis one has that

$$\mathrm{T}(A) \cong \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}, \qquad a, c > 0, \qquad b^2 - 4ac < 0.$$

Thus we can always associate to it the quadratic form (a, b, c), and therefore we can naturally see the transcendental lattice as a integral binary quadratic form (after choosing a basis). We can associate to any quadratic form $Q = (a, b, c)$ an abelian surface A_Q. In order to describe the correspondence, we set

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

and we will denote by E_τ the elliptic curve $\mathbb{C}/\Lambda_\tau$, Λ_τ being the lattice $\mathbb{Z} + \tau\mathbb{Z}$. The abelian surface associated to a form Q is then defined as the product surface

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

where $\tau = \tau(Q)$. The mapping $Q \mapsto A_Q$ realizes 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. By forgetting the orientation, we get a 2:1 map $\Sigma^{\mathrm{Ab}} \longrightarrow \mathcal{Q}^+ / \mathrm{GL}_2(\mathbb{Z})$, which is just taking the transcendental lattice of an abelian surface:

$$\Sigma^{\mathrm{Ab}} \ni [A] \longmapsto [\mathrm{T}(A)] \in \mathrm{GL}_2(\mathbb{Z}).$$

As a consequence, we get that every singular abelian surface A is isomorphic to the product of two isogenous elliptic curves with complex multiplication.

Via the Kummer construction, a singular abelian surface naturally gives rise to a singular K3 surface. If Σ_{K3} denotes the moduli space of singular K3 surfaces, Shioda and Mitani [39] proved that there exists a natural map

$$\mathrm{Km} : \Sigma^{\mathrm{Ab}} \longrightarrow \Sigma^{\mathrm{K3}}, \quad [A] \longmapsto [\mathrm{Km}(A)].$$

Unfortunately, this map is not surjective, and in fact the image of Km consists of the isomorphism classes of singular K3 surfaces with 2-divisible transcendental lattice. More precisely, if

$$\mathrm{T} : \Sigma_{\mathrm{Ab}} \longrightarrow \mathcal{Q}^+ / \mathrm{SL}_2(\mathbb{Z}) \quad \text{and} \quad \mathrm{T} : \Sigma_{\mathrm{K3}} \longrightarrow \mathcal{Q}^+ / \mathrm{SL}_2(\mathbb{Z})$$

are the *period maps* associating to a singular abelian or K3 surface its transcendental lattice seen as a quadratic form, one has the following commutative diagram

$$\begin{tikzcd}
\Sigma^{\mathrm{Ab}} \arrow[r, "T"] \arrow[d, "\mathrm{Km}"'] & \mathcal{Q}^+ / \mathrm{SL}_2(\mathbb{Z}) \arrow[d, "{[2]}"] \\
\Sigma^{\mathrm{K3}} \arrow[r, "T"] & \mathcal{Q}^+ / \mathrm{SL}_2(\mathbb{Z})
\end{tikzcd}$$

where $[2] : \mathcal{Q}^+ / \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathcal{Q}^+ / \mathrm{SL}_2(\mathbb{Z})$ is the map that multiplies a quadratic form by 2. In other words, $\mathrm{T}(\mathrm{Km}(A)) = \mathrm{T}(A)[2]$ (lattice-theoretical notation), or equivalently $\mathrm{T}(\mathrm{Km}(A)) = 2 \cdot \mathrm{T}(A)$ (number-theoretic notation).

In order to recover the whole Σ^{K3}, and thus prove the surjectivity of the period map for singular K3 surfaces, Shioda and Inose [38] came up with a new construction that later acquired the name of *Shioda-Inose structure* (following the notation of Morrison [23]). A Shioda-Inose structure for A is a K3 surface X with a Nikulin involution $\sigma : X \longrightarrow X$ (i.e. an involution that preserves the 2-form on X) such that the quotient X/σ is birationally equivalent to $\mathrm{Km}(A)$. One has a diagram

$$\begin{tikzcd}
A \arrow[dr, dashed, "2:1"'] & & X \arrow[dl, dashed, "2:1"] \\
& \mathrm{Km}(A) \cong X/\sigma &
\end{tikzcd}$$

where the map on the left-hand side comes from the classical Kummer construction, and the one on the right-hand side is an explicit (rational) 2:1 covering of $\mathrm{Km}(A)$, with the additional property that $\mathrm{T}(A) = \mathrm{T}(X)$. As a consequence, $\Sigma^{\mathrm{Ab}} \cong \Sigma\mathrm{K3}$, so that, in particular, this implies that two singular abelian surfaces are isomorphic if and only if the corresponding K3 surfaces via a Shioda-Inose structure are. Therefore, Shioda-Inose structures allow to reduce certain problems on K3 surfaces to the analogous ones on abelian surfaces.

1.3 Class field theory and complex multiplication

1.3.1 The Artin map

For later reference, we need to state a couple of facts from class field theory; see [8] for an account on the subject. Let K be a number field, and let $\mathfrak{m}$ be a *modulus* in K, i.e. a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$$

over all primes $\mathfrak{p}$ of K, finite or infinite, where the exponents satisfy

1. $n_{\mathfrak{p}} \geq 0$, and at most finitely many are nonzero;
2. $n_{\mathfrak{p}} = 0$, for $\mathfrak{p}$ a complex infinite prime;
3. $n_{\mathfrak{p}} \leq 1$, for $\mathfrak{p}$ a real infinite prime.

Consequently, any modulus $\mathfrak{m}$ can be written as $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an $\mathcal{O}_K$-ideal and $\mathfrak{m}_\infty$ is a product of distinct real infinite primes of K. We define $I_K(\mathfrak{m})$ to be the group of fractional ideals of K that are coprime to $\mathfrak{m}$, and we let $P_{K,1}(\mathfrak{m})$ be the subgroup of $I_K(\mathfrak{m})$ generated by the principal ideals $\alpha\mathcal{O}_K$, where $\alpha \in \mathcal{O}_K$ satisfies

$$\alpha \equiv 1 \mod \mathfrak{m}_0, \quad \sigma(\alpha) > 0 \text{ for every real infinite prime } \sigma | \mathfrak{m}_\infty.$$

One sees that $P_{K,1}(\mathfrak{m})$ is of finite index in $I_K(\mathfrak{m})$. A subgroup $H \subseteq I_K(\mathfrak{m})$ is called a *congruence subgroup* for $\mathfrak{m}$ if

$$P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m}),$$

and the quotient $I_k(\mathfrak{m})/H$ is called a *generalized class group* of $\mathfrak{m}$. Let now L be an abelian extension of K, and assume that $\mathfrak{m}$ is divisible by all primes of K that ramify in L. Then, for a given prime $\mathfrak{p}$ in K, one can define the Frobenius element associated to $\mathfrak{p}$ by means of the Artin symbol $\left(\frac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$, thus defining a map

$$\Phi_{\mathfrak{m}}^{L/K} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K),$$

called the *Artin map* for L/K and $\mathfrak{m}$.

1.3.2 Main theorems of class field theory

We now recall some of the main theorems of class field theory. The first result we would like to mention tells us that $\mathrm{Gal}(L/K)$ is a generalized ideal class group for some modulus $\mathfrak{m}$:

Theorem 1.3.1 (Artin reciprocity theorem)**.** *Let $K \subset L$ be an abelian extension, and let $\mathfrak{m}$ be a modulus divisible by all primes, finite or infinite, of K that ramify in L. Then,*

(i) the Artin map $\Phi_{\mathfrak{m}}^{L/K}$ is surjective;

(ii) if the exponents of the finite primes $\mathfrak{m}$ are sufficiently large, then $\ker \Phi_{\mathfrak{m}}^{L/K}$ is a congruence subgroup for $\mathfrak{m}$.

The modulus $\mathfrak{m}$ for which $\mathrm{Gal}(L/K)$ is a generalized class group is not unique. In fact, if $\mathfrak{n}$ is any modulus divisible by $\mathfrak{m}$, then $\mathrm{Gal}(L/K)$ is also a generalized class group for $\mathfrak{n}$. This shows that $\mathrm{Gal}(L/K)$ is a generalized class group for infinitely many moduli. However, there is one that is better that the others:

Theorem 1.3.2 (Conductor theorem)**.** *Let $K \subset L$ be an abelian extension. There exists a unique modulus $\mathfrak{f}$, called the conductor, such that*

(i) a prime of K, finite or infinite, ramifies in L if and only if it divides $\mathfrak{f}$;

(ii) if $\mathfrak{m}$ is modulus divisible by all primes of K that ramify in L, then $\ker \Phi_{\mathfrak{m}}^{L/K}$ is a congruence subgroup for $\mathfrak{m}$ if and only if $\mathfrak{f}|\mathfrak{m}$.

Finally, we want to mention one further result in class field theory, known as the *Existence theorem*, saying that every generalized class group is the Galois group of some abelian extension $K \subset L$.

Theorem 1.3.3 (Existence theorem)**.** *Let $\mathfrak{m}$ be a modulus of K, and let H be a congruence subgroup for $\mathfrak{m}$,* i.e.

$$P_{K,1} \subset H \subset I_K(\mathfrak{m}).$$

Then, there exists a unique abelian extension L/K, all of whose ramified primes (finite or infinite) divide $\mathfrak{m}$, such that if $\ker \Phi_{\mathfrak{m}}^{L/K} = H$.

This latter result is a powerful tool that allows one to construct abelian extensions of K with specified Galois group and restricted ramification. The field L constructed in the Existence Theorem above is called the *ring class field* of $\mathfrak{m}$ over K.

1.3.3 CM theory of elliptic curves

We recall a couple of elementary facts about the CM theory of elliptic curves; for a reference, see [41, Ch. 2] or [36]. Let $\mathcal{E}ll(\mathcal{O})$ be the set of isomorphism classes of elliptic curves with CM by the order $\mathcal{O} \subset K$. Since a proper $\mathcal{O}$-ideal is also a lattice, quotienting by $\mathcal{O}$-ideals induces a map

$$C(\mathcal{O}) \longrightarrow \mathcal{E}ll(\mathcal{O}), \qquad [\mathfrak{a}] \longmapsto [\mathbb{C}/\mathfrak{a}],$$

which is an isomorphism. Multiplication of ideal classes and lattices gives an action

$$* : C(\mathcal{O}) \times \mathcal{E}ll(\mathcal{O}) \longrightarrow \mathcal{E}ll(\mathcal{O}), \qquad ([\mathfrak{a}], [\mathbb{C}/\Lambda]) \longmapsto [\mathfrak{a}] * [\mathbb{C}/\Lambda] := [\mathbb{C}/\mathfrak{a}^{-1}\Lambda].$$

This action is simply transitive. Another action on $\mathcal{E}ll(\mathcal{O})$ is given by conjugation by elements of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$:

$$\mathrm{conj} : \mathrm{Gal}(\bar{K}/K) \times \mathcal{E}ll(\mathcal{O}) \longrightarrow \mathcal{E}ll(\mathcal{O}), \qquad (\sigma, [E]) \longmapsto [E^{\sigma}].$$

Now, let us fix $[E] \in \mathcal{E}ll(\mathcal{O})$; given $\sigma \in \mathrm{Gal}(\bar{K}/K)$, we can form $[E^{\sigma}]$, and, by using the action of $C(\mathcal{O})$, there exists a unique $[\mathfrak{a}] \in C(\mathcal{O})$ such that $[\mathfrak{a}] * [E] = [E^{\sigma}]$. This correspondence defines a surjective homomorphism

$$F : \mathrm{Gal}(\bar{K}/K) \longrightarrow C(\mathcal{O}), \qquad \sigma \longmapsto F(\sigma) \, : \, F(\sigma) * [E] = [E^{\sigma}].$$

The map F is independent of the curve $[E]$ chosen to define it, and thus we have that $F(\sigma) * [E] = [E^{\sigma}]$, $\forall \sigma \in \mathrm{Gal}(\bar{K}/K)$ and $\forall [E] \in \mathcal{E}ll(\mathcal{O})$.

1.3.4 The Main Theorem of CM

Given a number field K, we denote by $I_K = I(\mathcal{O}_K)$ the group of fractional ideals in K. We can define the so-called *group of idéles* by setting

$$\mathbb{I}_K := \left\{ (a_v) \in \prod_v K_v^{\times} \,\middle|\, a_v \in \mathcal{O}_v^{\times} \text{ for all but finitely many } v \right\},$$

where K_v denote the completion of K at the place v. There is a canonical surjective homomorphism associating to every idéle an element of I_K, namely

$$\mathrm{id} : \mathbb{I}_K \longrightarrow I_K, \qquad (a_v) \longmapsto \prod_{v \text{ finite}} p_v^{\mathrm{ord}_{p_v}(a_v)},$$

where p_v is the prime corresponding to the finite place v, and $\mathrm{ord}_{p_v}(a_v)$ is the valuation of a_v at the place v. There is also a canonical injective (diagonal) homomorphism

$$K^{\times} \longrightarrow \mathbb{I}_K, \qquad a \longmapsto (a, a, a, \dots),$$

with discrete image. The statement of the main theorems of class field theory in terms of ideals is very explicit. However, it has the big disadvantage of working for a fixed modulus $\mathfrak{m}$ at the time, and so it describes only the abelian extensions whose conductor divides $\mathfrak{m}$. On the other hand, the statements in terms of idéles allow one to consider infinite abelian extensions, or equivalently all finite abelian extensions simultaneously. It also relates local and global class field theory, namely the global Artin map to its local components.

Proposition 1.3.4. *There exists a unique continuous surjective homomorphism*

$$\phi_K : \mathbb{I}_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

with the following property: for any $L \subset K^{\mathrm{ab}}$ finite over K and any prime w of L lying over a prime v of K, the diagram

$$\begin{tikzcd}
K_v^\times \arrow[r, "\phi_v"] \arrow[d] & \mathrm{Gal}(L_w/K_v) \arrow[d] \\
\mathbb{I}_K \arrow[r, "\phi_{L/K}"] & \mathrm{Gal}(L/K)
\end{tikzcd}$$

where the bottom map sends $a \in \mathbb{I}_K$ to $\phi_K(a)|_L$. Here, ϕ_v is the local component of the Artin map at the place v.

In particular, for any finite extension L of K which is contained in K^{ab}, ϕ_K gives rise to a commutative diagram

$$\begin{tikzcd}
\mathbb{I}_K \arrow[r, "\phi_K"] \arrow[dr, "\phi_{L/K}"'] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[d, "|_L"] \\
 & \mathrm{Gal}(L/K)
\end{tikzcd}$$

We recall that the Main Theorem of Complex Multiplication makes use of the group of idéles $\mathbb{I}_K$ to control the Galois conjugates of an elliptic curve with CM in K. Let K be an imaginary quadratic field and E an elliptic curve with CM in K; then, there exist an order $\mathcal{O} \subset K$ and a fractional ideal $\mathfrak{a} \subset \mathcal{O}$ such that $E \cong \mathbb{C}/\mathfrak{a}$, and thus E has CM in the order $\mathcal{O}$.

Theorem 1.3.5 (Main Theorem of Complex Multiplication, Theorem 5.4 of [36]). *Let $E = \mathbb{C}/\Lambda$ be an elliptic curve with CM by an order in K. Let $\sigma \in \mathrm{Gal}(\bar{K}/K)$ and $s \in \mathbb{I}_K$ such that $\sigma = \phi_K(s)$ on K^{ab}. Then, there exists an isomorphism*

$$E^\sigma \cong \mathbb{C}/s^{-1}\Lambda.$$

Chapter 2

Decompositions of singular abelian surfaces

> Right and wrong are not what separate us and our enemies. It's our different standpoints, our perspectives that separate us. Both sides blame one another. There's no good or bad side. Just two sides holding different views.
>
> Squall, *Final Fantasy VIII*

2.1 Introduction

2.1.1 Decompositions of abelian surfaces

A *decomposition* of an abelian surface A is a pair of elliptic curves (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 a singular abelian surface A, Ma [19] 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:

Corollary 2.1.1 (Corollary 5.12 in [19]). *Let A be a singular abelian surface of transcendental lattice $\mathrm{T}(A) = Q = nQ_0$, $Q_0 \in \mathcal{C}(D_0)$ (in particular Q_0 is primitive). If $\operatorname{disc} Q_0 \neq -3, -4$, then*

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

The proof given by Ma builds on lattice theoretical methods, and it works for abelian surfaces of arbitrary 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, which is the main topic of this chapter.

2.1.2 Results and organization the chapter

The present chapter consists of two parts: in the first one, we develop the *generalized Dirichlet composition*, a notion that generalizes the usual Dirichlet composition of quadratic forms. This notion is crucial for fully understanding how to compute the transcendental lattice of an arbitrary product of two elliptic curves which are mutually isogenous and have complex multiplication (Proposition 2.2.4). We would like to stress that the results of this part are of interest on their own, as they provide generalizations of previous results of Shioda and Mitani [39] about the geometry of abelian surfaces, and also of Gauß and Dirichlet in the theory of quadratic forms.

The second part of this chapter is concerned with the problem of classifying all the possible decompositions of a given singular abelian surface, and it is the real motivation behind our studies. 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. In our analysis, we distinguish two cases, 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 2.3.11). 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.

2.2 Transcendental lattices of arbitrary singular abelian surfaces

2.2.1 Generalized Dirichlet composition

The idea behind Dirichlet composition is that two binary quadratic forms Q_1 and Q_2, of the same discriminant D, give rise to a new form F, itself 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. We would like to generalize this technique in a way that allows one to compose form of (possibly) different discriminants.

This can be done as follows: 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, suppose we are given $[Q_1] \in C(D_1)$ and $[Q_2] \in C(D_2)$, with $D_1 = f_1^2 d_K$ and $D_2 = f_2^2 d_K$ (d_K here denotes the fundamental discriminant of a quadratic imaginary field K), set $f := \operatorname{lcm}(f_1, f_2)$. Then, putting

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

one readily sees that the forms d_1Q_1 and d_2Q_2 have discriminant D. Therefore, after possibly replacing Q_1 and Q_2 with suitable properly equivalent forms, we can assume that d_1Q_1 and d_2Q_2 have coprime leading coefficients (here, we use [8, 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 [8, Theorem 3.8]). It is not hard to check the following:

Lemma 2.2.1. *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 [8, Ch. 1, Sect. 3]. □

In particular, the above lemma shows that the form $d_1Q_1 * d_2Q_2$ has index of primitivity d_1d_2. Also,

$$D = \operatorname{disc}(d_1Q_1 * d_2Q_2) = (d_1d_2)^2 \gcd(f_1, f_2)^2 d_K,$$

and therefore the primitive part of $d_1Q_1 * d_2Q_2$ 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_1d_2, where $d_1 = f/f_1$ and $d_2 = f/f_2$. Dropping the primitivity index, we get a new form, denoted by

$Q_1 \circledast Q_2$, which we call the *generalized Dirichlet composition* of Q_1 and Q_2. At the level of equivalence classes, we get a map of class groups

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

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 of discriminant D_0 with the property that

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

Remark 2.2.2. By using the 1:1 correspondence between ideal class group and form class group, one sees that the generalized Dirichlet composition corresponds to the usual multiplication between ideal classes

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

□

We now establish some elementary properties of $\circledast$.

Proposition 2.2.3. *Let $Q_i \in C(D_i)$ ($i = 0, 1, 2$), $R \in C(D)$, and let P be the principal form of discriminant D. The composition $\circledast$ satisfies:*

(i) $Q_0 \circledast P = Q_0$*;*

(ii) $(Q_0 \circledast R) \circledast R^{-1} = Q_0$*;*

(iii) $(Q_1 \circledast R) \circledast (R^{-1} \circledast Q_2) = Q_1 \circledast Q_2$*;*

Proof. Making use of the isomorphism between form class group and ideal class group, the proof follows easily from the corresponding properties for fractional ideals. □

2.2.2 Explicit computation of transcendental lattices

We will now explicitly compute the transcendental lattice of a singular abelian surface.

Proposition 2.2.4. *Let $D_0 = f_0^2 d_K$ and $D_0' = (f_0')^2 d_K$, where K is 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 [8, 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 [39],

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

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

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

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

$$A_{24} = A_{13} = 0, \tag{2.1}$$

$$A_{34} - \frac{B}{a} A_{14} + \frac{D - B^2}{4aa'} A_{12} = 0, \tag{2.2}$$

$$A_{23} - \frac{a'}{a} A_{14} = 0. \tag{2.3}$$

Condition (7) gives

$$d a_0 A_{23} = d' a'_0 A_{14};$$

now we can assume that $(d, a'_0) = 1$ and then also that $(a_0, a') = 1$ (use [8, Lemma 2.3] and [8, 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 (6) yields

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

and therefore we deduce

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

□

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

2.3.1 Cooking up decompositions from a given one

Let K be a quadratic imaginary field, $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. Let A be a singular abelian surface of transcendental lattice $Q = nQ_0$ of discriminant $D = f^2 d_K$, and let $D_0 := \operatorname{disc} Q_0 = f_0^2 d_K$. We can use Proposition 2.2.4 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 2.3.1. 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 2.2.4 show that $E_{s\tau(Q_0)} \times E_{t\tau(P_0)}$ gives indeed a decomposition of A, for a suitable choice of s and t. 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). □

2.3.2 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 2.3.2. *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 2.3.3. *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 $R \neq S \in C(D)$.

2.3.3 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 $D = f^2 d_K$, and consider $D_1 := f_1^2 d_K$ and $D_2 := f_2^2 d_K$ such that $\gcd(f_1, f_2) = f_0$ and $\mathrm{lcm}(f_1, f_2) = f$. 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 groups $C(D_0)$. 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 2.3.4. 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.

2.3.4 Interlude: ring class fields and their compositum fields

Suppose we have the diagrams of orders

$$\begin{tikzcd}
K & & \mathcal{O}_{K,f_1} \arrow[dl, hook'] & \\
\mathcal{O}_K \arrow[u, hook] & \mathcal{O}_{K,f_0} \arrow[l, hook'] & & \mathcal{O}_{K,f} \arrow[ul, hook'] \arrow[dl, hook] \\
& & \mathcal{O}_{K,f_2} \arrow[ul, hook] &
\end{tikzcd}$$

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 Theorem 1.3.3, 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 an induced diagram of field extensions,

$$\begin{tikzcd}
& & L_1 \arrow[dr, hook] & & \\
H_K \arrow[r, hook] & L_0 \arrow[ur, hook] \arrow[dr, hook] & & L_1L_2 \arrow[r, hook] & L \\
& & L_2 \arrow[ur, hook] & &
\end{tikzcd}$$

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.

$$\begin{tikzcd}
& & C(\mathcal{O}_{K,f_1}) \arrow[dl] & \\
C(\mathcal{O}_K) & C(\mathcal{O}_{K,f_0}) \arrow[l] & & C(\mathcal{O}_{K,f}) \arrow[ul] \arrow[dl] \\
& & C(\mathcal{O}_{K,f_2}) \arrow[ul] &
\end{tikzcd}$$

In most cases the field L is precisely the compositum of L_1 and L_2, as it is stated in the following

Proposition 2.3.5 (Proposition 3.1 in [1])**.** *Assume all conditions above are satisfied.*

1. *If $d_K \neq -3, -4$, then $L = L_1L_2$.*
2. *Assume $d_K \in \{-3, -4\}$.*
   (a) *If f_1 or f_2 is equal to 1, or $f_0 > 1$, then $L = L_1L_2$.*
   (b) *If $f_1, f_2 > 1$ and $f_0 = 1$, then $L_1L_2 \subsetneq L$; moreover, the extension L/L_1L_2 has degree 2 if $d_K = -4$, and degree 3 if $d_K = -3$.*

2.3.5 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

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

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 2.3.6 (Exercise 8.14 in [8])**.** *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, $\mathrm{Spl}(LM/K) = \mathrm{Spl}(L/K) \cap \mathrm{Spl}(M/K)$.*

2.3.6 Answer to Question 2.3.4

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 2.3.7. *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 2.3.6, 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 $\mathrm{Spl}(L_i/\mathbb{Q})$, for $i = 1, 2, \varnothing$: 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).

Proposition 2.3.8. *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 $\mathcal{P}_Q \doteq \mathrm{Spl}(L/\mathbb{Q})$. Then, we would have

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

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 2.3.4:

Proposition 2.3.9. *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 Proposition 2.3.5, $L = L_1L_2$, and Lemma 2.3.7 and Proposition 2.3.8 imply that Q is in fact the principal form. □

Remark 2.3.10. With the aid of a computer algebra system, 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 $K = \mathbb{Q}(\sqrt{-3})$. □

2.3.7 Classification result for $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$

As an immediate consequence of Proposition 2.3.9, 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 2.3.11. *Let A be a singular abelian surface having transcendental lattice $Q = nQ_0$, and let $D = f^2 d_K = \mathrm{disc}\, Q$, $D_0 = f_0^2 d_K = \mathrm{disc}\, Q_0$, $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$ (in particular, $n = f/f_0$). 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*

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

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 2.3.1 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 Proposition 2.3.9). As there are $2^{\tau(n)}$ choices of pairs (f_1, f_2) as above, we have found

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

distinct decompositions of A. This matches Ma's formula (Proposition 2.1.1) 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. □

2.4 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 2.3.9 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 (Proposition 2.1.1).

Proposition 2.4.1. *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

$$\begin{aligned}\sum_{\substack{(f_1,f_2)=f_0\\ f_1f_2=nf_0^2}} h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2}) &= 2\sum_{\substack{(f_1,f_2)=f_0\\ f_1f_2=nf_0^2\\ f_1<f_2}} h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2})\\ &= 2\sum_{\substack{(f_1,f_2)=f_0\\ f_1f_2=nf_0^2\\ f_0\neq f_1<f_2}} h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2}) + 2h(\mathcal{O}_{K,f_0})h(\mathcal{O}_{K,f}),\end{aligned}$$

and so it is enough to prove that

$$(2^{\tau(n)-1}-1)h(\mathcal{O}_{K,f}) = \sum_{\substack{(f_1,f_2)=f_0\\ f_1f_2=nf_0^2\\ 1\neq f_1<f_2}} \frac{h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2})}{h(\mathcal{O}_{K,f_0})};$$

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

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

Setting

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

[8, 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 Corollary 2.1.1. 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

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

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

2.5 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 $D = f^2 d_K = \operatorname{disc} Q$, $D_0 = f_0^2 d_K = \operatorname{disc} Q_0$, $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})\}$. We will divide the analysis into two cases, depending on f_0.

2.5.1 Case $f_0 > 1$

Under these hypotheses, we can still use Proposition 2.3.9 to get $h(D)$ distinct decompositions starting from a given one. By combining this with Proposition 2.4.1, and reasoning as in the alternative proof of [19, 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 2.3.11.

2.5.2 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 2.5.1. *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

$$\begin{aligned}\tilde{\delta}(A) &= \sum_{\substack{(f_1,f_2)=1\\ f_1f_2=n}} h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2})\\ &= 2\sum_{\substack{(f_1,f_2)=1\\ f_1f_2=n\\ f_1<f_2}} h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2})\\ &= 2\sum_{\substack{(f_1,f_2)=1\\ f_1f_2=n\\ 1\neq f_1<f_2}} h(\mathcal{O}_{K,f_1})h(\mathcal{O}_{K,f_2}) + 2h(\mathcal{O}_{K,n}).\end{aligned}$$

Following the notation from earlier, since $\#\mathcal{O}_K^\times = 4$, [8, 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 2.5.2 is the same, except for the fact that $\#\mathcal{O}_K^\times = 6$. We omit the proof for sake of brevity.

Theorem 2.5.2. *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 $f_1 f_2 = n$.

2.5.3 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 [38], 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. Inose first found a model for it [13], and later Schütt exhibited a finer model for such a K3 surface as an elliptic fibration defined over $\mathbb{Q}(j_1, j_2)$, namely

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

where $\alpha = j_1 j_2$ and $\beta = (1 - j_1)(1 - j_2)$, j_k being the j-invariant of E_k ($k = 1, 2$). 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.

2.5.4 Open problems

In this chapter, we have 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 [14] that such a variety is isomorphic to the product of mutually isogenous elliptic curves with complex multiplication.

Problem 2.5.3. 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.

Chapter 3

The field of moduli of singular K3 surfaces

> Why do people insist on creating things that will inevitably be destroyed? Why do people cling to life, knowing that they must someday die? Knowing that none of it will have meant anything once they do?
>
> Kefka, *Final Fantasy VI*

3.1 Introduction

3.1.1 Field of definition vs. field of moduli

The arithmetic data of a singular abelian surface is encoded in its transcendental lattice, and a Shioda-Inose structure associates to it a singular K3 surface with the same transcendental lattice, thus preserving the arithmetic information. This has been employed, for instance, by Schütt in the study of the field of definition of singular K3 surfaces [28]: he proved that a singular K3 surface X always admits a model over a ring class field H/K, K being the field $K = \mathbb{Q}(\operatorname{disc} \mathrm{T}(X))$, generalizing previous results of Inose [13]. Morever, Schütt [28], generalizing previous work of Shimada [35], describes the conjugate varieties of X (modulo $\mathbb{C}$-isomorphism) under the action of $\mathrm{Gal}(\mathbb{C}/K)$: this is done by looking at the corresponding transcendental lattices, and it is best understood in the language of genus theory of quadratic forms. As a by-product, given a good notion of field of moduli, one should expect its degree to be exactly the number of Galois conjugates of X. However, apart from the aforementioned result, nothing is known in general for the field of moduli of singular K3 surfaces, which is indeed a good candidate for an object to be studied, as every field of definition must contain the field of moduli itself. This chapter aims at describing the field of moduli of singular K3 surfaces. This is achieved by using tools such as Galois theory, CM theory of elliptic curves, the theory of quadratic forms and the results in Chapter 2.

3.1.2 Results and organization of the chapter

We first give a new notion of *relative field of moduli*, a notion that was first introduced by Matsusaka in [20], and later refined by Koizumi [15]. Then, we study the relative field of moduli with respect to the CM field of our singular K3 surface; in the following, this will also be called the *field of K-moduli*, K being the CM field. Using an idea of Šafarevič [34], we reduce the problem of studying the field of moduli of a singular K3 surface X to the study of the analogous field for a singular abelian surface A with transcendental lattice $\mathrm{T}(A) = \mathrm{T}(X)$ (this condition can always be achieved by means of a Shioda-Inose structure). We obtain that the field of moduli of a singular K3 surface X is a Galois extension of K, of degree the order of the genus of the (primitive part of the) transcendental lattice of X seen as a quadratic form, and we characterize it as the subfield of $\bar{K}$ which is fixed by a certain subgroup of $\mathrm{Gal}(\bar{K}/K)$ (Theorem 3.4.4). Having this result as a starting point, we are able to study the *absolute field of moduli*, i.e. the field of $\mathbb{Q}$-moduli. Here the analysis is slightly more subtle, as we have to distinguish two cases, according to whether the primitive part of the transcendental lattice is 2-torsion or not: in fact, this condition reflects the behaviour of the modulus $[X]$ under the Galois action of the complex conjugation automorphism. Finally we are able to recover almost the same result as in the case of the relative field of moduli (Theorem 3.5.3). The exception lies in the fact that this field is not a Galois extension of $\mathbb{Q}$ in general: as a counterexample, it is enough to consider a certain singular K3 surface of class number three (Example 3.5.4). One last section is devoted to further questions on singular K3 surfaces and their field of moduli: we study non-finiteness with respect to the degree of the field of moduli, we provide an explicit description of the field of K-moduli that can be implemented on a computer algebra system, and finally we investigate how the field of moduli varies within the moduli space of singular K3 surfaces.

3.2 The field of K-moduli

3.2.1 A new definition

We define the *field of K-moduli* M_K of a variety X, where K is a given field. This field was first introduced by Matsusaka [20] as the *relative field of moduli* (or *field of moduli over K*), and it was defined to be the intersection of all fields of definition of X which contain K, in other words

$$M_K := \bigcap_{\substack{X \text{ defined over } L \\ L \supset K}} L.$$

Later, Koizumi [15] adjusted the definition to positive characteristic geometry by adding the extra condition that for an automorphism $\sigma \in \mathrm{Aut}(\Omega/K)$, where Ω is a fixed universal domain[1],

$$\sigma \in G := \{\sigma \in \mathrm{Aut}(\Omega/K) \mid X^\sigma \in [X]\} \iff \sigma_{|M_K} = \mathrm{id}_{M_K},$$

where by $[X]$ we denote the isomorphism class of X. For our purposes, it is best to introduce the following

Definition 3.2.1. The *field of K-moduli* of X is the subfield of $\mathbb{C}$ fixed by the group

$$G := \{\sigma \in \mathrm{Aut}(\mathbb{C}/K) \mid X^\sigma \in [X]\}.$$

In practice, we are dropping Matsusaka's condition and keeping the one Koizumi introduced. Notice that, unlike in the case of Koizumi's definition [15], our field of moduli always exists and it is unique by Galois theory. Following [15], if the characteristic of the ground field is zero, then M_K is contained in any field of definition for X which contains K, and thus we have the following extension

$$M_K \subset \bigcap_{\substack{X \text{ defined over } L \\ L \supset K}} L,$$

which in fact is algebraic and Galois. We remark that the right-hand side of this inclusion is quite a mysterious object in general.

If X is a variety, by the *absolute field of moduli* of X we will mean the field of $\mathbb{Q}$-moduli, i.e. the field $M_{\mathbb{Q}}$ such that for all automorphisms $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$,

$$X^\sigma \in [X] \iff \sigma \text{ acts trivially on } M_{\mathbb{Q}};$$

equivalently, it is defined as the fixed field of the group

$$G := \{\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q}) \mid X^\sigma \in [X]\}.$$

Galois theory once again guarantees that this field is unique for a given variety X.

If X is a variety and $\tau \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$, let X^τ denote the variety obtained by conjugating X by τ. Suppose we want to study the field of L-moduli, for some number field L, and denote by $G(X)$ (respectively, $G(X^\tau)$) the group fixing the modulus of X (respectively, X^τ) and by $M(X)$ (respectively, $M(X^\tau)$) the field of L-moduli. Then, one can show that:

1. $G(X)$ only depends on the isomorphism class of X;
2. $G(X^\tau) = \tau \cdot G(X) \cdot \tau^{-1}$;
3. $M(X^\tau) = \tau(M(X))$.

[1] Given a field K, a universal domain Ω is an extension of K with infinite transcendence degree over K. Universal domains were the fundamental object algebraic geometry was based on before the advent of Grothendieck. More details can be found in the fundational book of Weil [42]; this uses notions very much different from the modern language of schemes and it is quite hard to read at times.

3.2.2 A little motivation

Let X be a singular K3 surface, and let

$$\mathrm{T}(X) \cong \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} = (a, b, c)$$

be its transcendental lattice, where the right-hand side equality identifies $\mathrm{T}(X)$ with the corresponding quadratic form. To $\mathrm{T}(X)$, one can associate two gadgets: the first one is $\det \mathrm{T}(X)$, and the second one is $\operatorname{disc} \mathrm{T}(X)$, when $\mathrm{T}(X)$ is regarded as a quadratic form. Clearly,

$$\det \mathrm{T}(X) = -\operatorname{disc} \mathrm{T}(X) < 0,$$

and thus $K := \mathbb{Q}(\sqrt{\det \mathrm{T}(X)})$ is a quadratic imaginary field. We will call K the *CM field*[2] of X. If X is the K3 surface associated to a singular abelian surface A via a Shioda-Inose structure (so that, in particular, $\mathrm{T}(A) = \mathrm{T}(X)$), we will say that K is the CM field of A as well. Generalizing a previous result of Shimada [35], Schütt was able to prove the following result

Theorem 3.2.2 (Theorem 5.2 in [28]). *Let X be a singular K3 surface, and let $\mathrm{T}(X)$ be its transcendental lattice. Assume that X is defined over a Galois extension L/K. Then, the action of the Galois group $\mathrm{Gal}(L/K)$ spans the genus of $\mathrm{T}(X)$, i.e.*

$$\big(\text{genus of } \mathrm{T}(X)\big) = \big\{[\mathrm{T}(X^\sigma)] \,:\, \sigma \in \mathrm{Gal}(L/K)\big\}.$$

Here, as the genus is defined for primitive quadratic forms only, we mean the following: consider the primitive part of $\mathrm{T}(X)$, so that $\mathrm{T}(X) = m\mathrm{T}(X)_0$, m being the index of primitivity of $\mathrm{T}(X)$. Then,

$$\big(\text{genus of } \mathrm{T}(X)\big) = \big\{m[T] \,:\, [T] \text{ lies in the genus of } \mathrm{T}(X)_0\big\}.$$

Set $L := H(\operatorname{disc} \mathrm{T}(X))$ in Theorem 3.2.2, where $H(D)$ denotes the ring class field of the order in K of discriminant D, for $D < 0$. Galois theory tells tells us that

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L/K) \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

where $\mathrm{Gal}(K/\mathbb{Q})$ accounts for the complex conjugation (for a reference, see [8, Ch. 9]). But complex conjugation has the effect of sending a singular K3 surface of transcendental lattice (a, b, c) to the singular K3 surface with transcendental lattice $(a, -b, c)$, so it acts as inversion on the corresponding class group (see [39] and [28]). By observing that a form and its inverse lie in the same genus, we conclude that

$$\begin{aligned}(\text{genus of } T(X)) =& \{[T(X^\sigma)] \,|\, \sigma \in \mathrm{Gal}(L/K)\} = \\ =& \{[T(X^\sigma)] \,|\, \sigma \in \mathrm{Gal}(L/\mathbb{Q})\}.\end{aligned}$$

[2] There are other notions of CM field currently in use. For example, a number field K is a CM field if it is a totally imaginary quadratic extension of a totally real field. In fact, the CM field of a singular K3 surface is also a CM field in the latter sense.

This observation suggests a connection between the field of moduli of a singular K3 surface and the genus of its transcendental lattice, even in the case of the field of $\mathbb{Q}$-moduli.

The classification of decompositions of a singular abelian surface (Chapter 2) allows us to tell something more about the field of moduli of X containing K. Recall that M_K is contained in the intersection of all possible fields of definition for X. Then, by means of Shioda-Inose structures, we can study X by means of those abelian surfaces A whose transcendental lattice equals $\mathrm{T}(X)$. Let A be such a surface, and consider all product surfaces $E_1 \times E_2$ isomorphic to A (which we know explicitly by Chapter 2); if $j_k := j(E_k)$, by work of Schütt [28], X admits a model over $\mathbb{Q}(j_1 j_2, j_1 + j_2)$. Therefore, considering all admissible pairs (E_1, E_2) as above, we see that

$$M_K \subseteq \bigcap_{X \text{ defined over } L} L \subseteq \bigcap_{j_1, j_2 \text{ as above}} \mathbb{Q}(j_1 j_2, j_1 + j_2).$$

We deduce a slightly clearer picture of what M_K looks like, as we know where it has to sit as an extension of $\mathbb{Q}$. Namely, M_K lies in right-hand side above, which is theoretically clear. In practice, describing it is a hard task, as this involves the computation of j-invariants.

3.2.3 The case of elliptic curves

Our toy example is the case of an elliptic curve E, for which one always has a Weierstraß model

$$y^2 = x^3 + Ax + B,$$

for some $A, B \in \mathbb{C}$. It can be proven (see [40, Ch. 1]) that an elliptic curve E can be defined over the field $\mathbb{Q}(j_E)$; moreover, the field of $\mathbb{Q}$-moduli of E is again $\mathbb{Q}(j_E)$. Let now E be a CM elliptic curve. The theory of complex multiplication tells us (see [40, Ch. 2]) that $j_E \in \overline{\mathbb{Q}}$, i.e. the j-invariant of a CM elliptic curve is always an algebraic number. Suppose that E has CM by an order $\mathcal{O}$ in $K = \mathbb{Q}(\sqrt{D})$. Then, by means of class field theory, one can show that there exists a commutative diagram of field extensions,

$$\begin{tikzcd}
& H = K(j_E) \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \mathbb{Q}(j_E) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

where $H := H(D)$ is the ring class field corresponding to the order $\mathcal{O}$ (for details, consult [36]). We would like to let the reader notice that $K(j_E)$ is indeed the field of K-moduli of E. Our study of the field of moduli in the rest of the chapter will reveal that this very picture carries over to singular K3 surfaces (and singular abelian surfaces). This provides more evidence to the fact that singular K3 surfaces can be regarded as a two-dimensional analog of CM elliptic curves.

3.2.4 An alternative definition of M_K

As a singular K3 surface is defined over a number field by a result of Inose [13], when studying the field of moduli one would like to consider the field

$$\bar{K}^{G'}, \qquad G' := \{\sigma \in \mathrm{Aut}(\bar{K}/K) \mid X^\sigma \in [X]\},$$

rather than $\mathbb{C}^G$, as we defined it above. In fact, one has that $\mathbb{C}^G = \bar{K}^{G'}$; also this is independent of the fact that we are working on a singular K3 surface, as the following more general result shows.

Proposition 3.2.3. *Let X be a variety defined over a number field K. Then the fields $\mathbb{C}^G$ and $\bar{K}^{G'}$ coincide.*

Proof. Suppose X is defined over a number field L containing K. As L is a number field, $\bar{K} \supset L \supseteq K$; therefore $\mathrm{Gal}(\mathbb{C}/\bar{K}) \subseteq G$, and thus $\mathbb{C}^G \subseteq \mathbb{C}^{\mathrm{Gal}(\mathbb{C}/\bar{K})} = \bar{K}$ (see [21, Theorem 9.29]). We have a diagram of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Gal}(\mathbb{C}/\bar{K}) \arrow[r] \arrow[d, equal] & G \arrow[r, "{|_K}"'] \arrow[d, hook] & G' \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \mathrm{Gal}(\mathbb{C}/\bar{K}) \arrow[r] & \mathrm{Gal}(\mathbb{C}/K) \arrow[r, "{|_K}"'] & \mathrm{Gal}(\bar{K}/K) \arrow[r] & 0
\end{tikzcd}$$

and by surjectivity of the map $G \longrightarrow G'$ plus the fact that $\mathbb{C}^G \subseteq \bar{K}$, one sees that $\mathbb{C}^G = \bar{K}^{G'}$. □

As every singular K3 surface can be defined over a number field, we can define the field of K-moduli of a singular K3 surface to be the field

$$M_K := \bar{K}^{G_K}, \qquad G_K := \{\sigma \in \mathrm{Aut}(\bar{K}/K) \mid X^\sigma \in [X]\}.$$

In the following, we will be concerned with finding explicitly the group G_K, as it characterizes uniquely, thanks to Galois theory, the field of moduli.

3.3 Characterization in the primitive case

3.3.1 Statement of the result

Let X be a singular K3 surface, with transcendental lattice $\mathrm{T}(X) = Q = mQ_0$ (Q_0 being the primitive part of $\mathrm{T}(X)$), and discriminant $\operatorname{disc}\mathrm{T}(X) = D = m^2 D_0$ (D_0 being the discriminant of Q_0). Recall that we can always find a singular abelian surface A such that X is obtained from A by means of the Shioda-Inose structure, and in particular such that $\mathrm{T}(A) = \mathrm{T}(X)$. In light of this, notice that determining the field of moduli of X is equivalent to determining the field of moduli of any such A, so that we can reduce to considering the problem for singular abelian surfaces.

We will now proceed in giving a different characterization of G_K. In what follows, let us assume additionally that $m = 1$, which is to say that the transcendental lattice $\mathrm{T}(X)$ is primitive. Under this assumption, for any decomposition $A \cong E_1 \times E_2$, the quadratic forms Q_1 and Q_2 corresponding to the elliptic curves E_1 and E_2 both lie in $C(D) \cong C(\mathcal{O})$, $\mathcal{O}$ being the order of discriminant D. Observe that, if we fix a decomposition of $A \cong E_1 \times E_2$, then

$$X^\sigma \in [X] \Longleftrightarrow A^\sigma \in [A] \Longleftrightarrow E_1^\sigma \times E_2^\sigma \cong E_1 \times E_2.$$

We will prove the following

Theorem 3.3.1. *Let X be a singular K3 surface with primitive transcendental lattice, and let H be the ring class field of $\mathcal{O}$, the order of discriminant* $\operatorname{disc}\mathrm{T}(X)$. *Then the field of K-moduli is*

$$M_K = \bar{K}^{G_K}, \qquad G_K = (|_H)^{-1}\,\mathrm{Gal}(H/K)[2];$$

it is a Galois extension of K of degree g, g being the order of the genus of the transcendental lattice of X.

The proof is divided into two steps. First, we will prove that G_K restricts to the subgroup of 2-torsion elements of $\mathrm{Gal}(H/K)$, and thus it is a closed and normal subgroup of $\mathrm{Gal}(\bar{K}/K)$ with respect to the Krull topology. Afterwards, we will use these facts to study the field extension M_K/K, hence to prove Theorem 3.3.1.

3.3.2 Interlude: CM elliptic curves vs. quadratic forms

Let us recall the reader of the action

$$*: C(\mathcal{O}) \times \mathcal{E}ll(\mathcal{O}) \longrightarrow \mathcal{E}ll(\mathcal{O}), \qquad ([\mathfrak{a}], [\mathbb{C}/\Lambda]) \longmapsto [\mathfrak{a}] * [\mathbb{C}/\Lambda] := [\mathbb{C}/\mathfrak{a}^{-1}\Lambda],$$

which can be interpreted in terms of ideal classes, as we will now show. Indeed, to any $[E] \in \mathcal{E}ll(\mathcal{O})$, one can associate a quadratic form Q such that $j(\tau(Q)) = j(E)$. Therefore, by Proposition 1.1.5, the action $*$ is isomorphic to the action

$$C(\mathcal{O}) \times C(\mathcal{O}) \longrightarrow C(\mathcal{O}), \qquad ([\mathfrak{a}], [\mathfrak{b}]) \longmapsto [\mathfrak{a}]^{-1}[\mathfrak{b}],$$

which we again denote by $*$. Also, by Theorem 1.1.3, we can phrase everything in terms of the corresponding classes of quadratic forms, where now multiplication of ideal classes corresponds to the Dirichlet composition. Indeed, let $[Q] \in C(\mathcal{O})$ correspond to $[E] \in \mathcal{E}ll(\mathcal{O})$; then, the map

$$F : \mathrm{Gal}(\bar{K}/K) \longrightarrow C(\mathcal{O}), \qquad \sigma \longmapsto F(\sigma),$$

associates to σ the element $F(\sigma)$ such that

$$[E^\sigma] = F(\sigma) * [E] = F(\sigma) * [\mathbb{C}/\mathfrak{a}] = [\mathbb{C}/F(\sigma)^{-1}\mathfrak{a}] = [F(\sigma)]^{-1} * [Q].$$

Furthermore, if $[Q^\sigma]$ corresponds to $[E^\sigma]$, then $F(\sigma)$ has the property

$$[Q^\sigma] = F(\sigma)^{-1} * [Q].$$

We will make use of this formula extensively in the rest of this chapter.

3.3.3 The group G_K

By the previous discussions, it follows that

$$\begin{aligned} G_K &= \{\sigma \in \mathrm{Gal}(\bar{K}/K) \mid X^\sigma \in [X]\} \\ &= \{\sigma \in \mathrm{Gal}(\bar{K}/K) \mid E_1^\sigma \times E_2^\sigma \cong E_1 \times E_2\}. \end{aligned}$$

We will now proceed in giving a different characterization of G_K.

Proposition 3.3.2. $G_K = F^{-1}(C(\mathcal{O})[2])$.

Proof. Let Q_i be the form corresponding to E_i $(i = 1, 2)$, and let Q_i^σ be the one corresponding to E_i^σ $(i = 1, 2)$. By use of the map

$$F : \mathrm{Gal}(\bar{K}/K) \longrightarrow C(\mathcal{O}),$$

we get that

$$[Q_1^\sigma] = [F(\sigma)]^{-1} * [Q_1] \qquad \text{and} \qquad [Q_2^\sigma] = [F(\sigma)]^{-1} * [Q_2],$$

where here we make use of the fact that F is independent of the elliptic curve (and thus of the quadratic form) we use to define it. By Proposition 2.2.4, we see that

$$\begin{aligned} E_1^\sigma \times E_2^\sigma \cong E_1 \times E_2 &\iff Q_1^\sigma * Q_2^\sigma = Q_1 * Q_2 \\ &\iff F(\sigma)^2 = 1. \end{aligned}$$

□

There is a commutative diagram

$$\begin{tikzcd} \mathrm{Gal}(\bar{K}/K) \arrow[r, two heads, "F"] \arrow[d, two heads, "|_H"'] & C(\mathcal{O}) \\ \mathrm{Gal}(H/K) \arrow[ur, "\cong"'] & \end{tikzcd} \tag{†}$$

where $H := H(\mathcal{O})$, which follows from class group theory and says that F is an isomorphism on the restriction of the elements of $\mathrm{Gal}(\bar{K}/K)$ to H. In particular, $C(\mathcal{O})[2] \cong \mathrm{Gal}(H/K)[2]$, and thus

$$G_K = \{\sigma \in \mathrm{Gal}(\bar{K}/K) \; : \; (\sigma|_H)^2 = \mathrm{id}_H\}.$$

This implies the following

Corollary 3.3.3. $G_K = (|_H)^{-1}(\mathrm{Gal}(H/K)[2])$.

We now turn to describing G_K as a topological subgroup of $\mathrm{Gal}(\bar{K}/K)$.

Proposition 3.3.4. *G_K is a closed normal subgroup of $\mathrm{Gal}(\bar{K}/K)$ with respect to the Krull topology.*

Proof. As G_K maps onto $\mathrm{Gal}(H/K)[2]$, and[3]

$$G_K \cap \mathrm{Gal}(\bar{K}/H) = \mathrm{Gal}(\bar{K}/H),$$

we get the following diagram,

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Gal}(\bar{K}/H) \arrow[r] \arrow[d, equal] & G_K \arrow[r] \arrow[d, hook] & \mathrm{Gal}(H/K)[2] \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \mathrm{Gal}(\bar{K}/H) \arrow[r] & \mathrm{Gal}(\bar{K}/K) \arrow[r, "|_H"] & \mathrm{Gal}(H/K) \arrow[r] & 0
\end{tikzcd}$$

from which we extract the short exact sequence

$$0 \to G_K \to \mathrm{Gal}(\bar{K}/K) \to C(\mathcal{O})/C(\mathcal{O})[2] \to 0.$$

The group inclusions

$$\mathrm{Gal}(\bar{K}/H) \subseteq G_K \subseteq \mathrm{Gal}(\bar{K}/K)$$

yield the reversed inclusions of fields

$$K \subseteq M_K \subseteq H.$$

Notice that for $\sigma \in G_K$ and $\tau \in \mathrm{Gal}(\bar{K}/K)$, the element $(\tau\sigma\tau^{-1})^2$ restricts to id_H, which amounts to saying that G_K is normal in $\mathrm{Gal}(\bar{K}/K)$. Indeed, as H/K is Galois, σ and τ restrict to automorphisms of H, and therefore:

$$(\tau\sigma\tau^{-1})^2 = (\tau|_H)(\sigma^2|_H)(\tau^{-1}|_H) = \mathrm{id}_H\,.$$

As $G_K = (|_H)^{-1}(\mathrm{Gal}(H/K)[2])$, and the restriction map

$$|_H : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Gal}(H/K)$$

is a continuous surjection by Galois theory, G_K is closed and we are done. □

[3] This is independent of the fact that every singular K3 surface has a model over the ring class field.

3.3.4 The extension M_K/K

We can now use our knowledge of G_K to give a proof of Theorem 3.3.1.

Proof of Theorem 3.3.1. As G_K is closed and normal in $\mathrm{Gal}(\bar{K}/K)$, we have that

$$\mathrm{Gal}(\bar{K}/M_K) = \mathrm{Gal}(\bar{K}/\bar{K}^{G_K}) = G_K$$

and M_K/K is a (finite) Galois extension. The exact sequence

$$0 \to G_K \to \mathrm{Gal}(\bar{K}/K) \to C(\mathcal{O})/C(\mathcal{O})[2] \to 0$$

tells us that $\mathrm{Gal}(M_K/K) \cong C(\mathcal{O})/C(\mathcal{O})[2]$, from which we can now cook up the following short exact sequence.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Gal}(H/K)[2] \arrow[r] \arrow[d, equal, "\mathrm{iso}"'] & \mathrm{Gal}(H/K) \arrow[r] & \mathrm{Gal}(M_K/K) \arrow[r] & 0 \\
& \mathrm{Gal}(H/M_K) \arrow[ur, hook] & & &
\end{tikzcd}$$

By genus theory (see [8]), there is a short exact sequence

$$0 \to C(D)[2] \to C(D) \to C(D)^2 \to 0,$$

where $C(D)^2$ is the group of squares in the class group $C(D)$ (in fact, it is the principal genus). As $\mathrm{Gal}(H/K) \cong C(D)$, we deduce that

$$\mathrm{Gal}(M_K/K) \cong C(D)^2,$$

and in particular that $\#\mathrm{Gal}(M_K/K) = g$, where $g = \#C(D)^2$ is the order of the genus of the transcendental lattice. □

Example 3.3.5. Let $D = -23$ and $K = \mathbb{Q}(\sqrt{D})$. The class group of discriminant D is

$$C(D) = \left\{ \begin{pmatrix} 2 & 1 \\ 1 & 12 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ 1 & 6 \end{pmatrix}, \begin{pmatrix} 4 & -1 \\ -1 & 6 \end{pmatrix} \right\}.$$

There is only one genus in $C(D)$ (of order 3), thus we expect a field of moduli of degree 3 over K. Let X be the singular K3 surface whose transcendental lattice is

$$P = \begin{pmatrix} 2 & 1 \\ 1 & 12 \end{pmatrix}.$$

A Shioda-Inose structure starting from the self-product of E, E being the elliptic curve corresponding to the principal form P in $C(D)$, reveals that X has a model over $\mathbb{Q}(j(P))$. We now show that the field of K-moduli is $M_K = K(j(P)) = H(\mathcal{O}_K)$, which is a degree 3 extension of K by class field theory. Indeed, as X is realized starting from the self-product of E, where E corresponds to the principal form P, then the transcendental lattice of the conjugate surface by $\sigma \in \mathrm{Gal}(\bar{K}/K)$ is given by

$$P^\sigma * P^\sigma = F(\sigma)^{-2},$$

and this is trivial if and only if $F(\sigma)$ is 2-torsion. However, as $\#\mathrm{Gal}(H/K) = 3$, it follows that $F(\sigma)$ is necessarily trivial, and thus $G_K = \ker F = \mathrm{Gal}(\bar{K}/H)$. Therefore, we have proven that $M_K = H$.

We can also look at the K3 surface Y whose transcendental lattice is

$$Q := \begin{pmatrix} 4 & 1 \\ 1 & 6 \end{pmatrix}.$$

By means of a Shioda-Inose structure, Y has a model over $\mathbb{Q}(j_1, j_2)$, where $j_1 := j(P)$ and $j_2 := j(Q)$; notice that

$$\mathbb{Q}(j_1, j_2) = K(j_1, j_2) = K(j_2),$$

as we have considered the Shioda-Mitani model of Y (plus some class field theory considerations). It follows that $H = K(j_2)$, which is a degree 3 extension of K, and thus we have that $M_K = H = K(j_2)$. □

3.4 Generalization to the imprimitive case

3.4.1 A first look at G_K

We will now treat the case of a singular K3 surface X with imprimitive transcendental lattice $\mathrm{T}(X) = Q = mQ_0$ ($m > 1$). As in the primitive case, we see that it is enough to choose a decomposition of A, and to compute the field of moduli in that case. Thus, we now fix a decomposition $A \cong E_1 \times E_2$.

We would like to mimic the techniques used in the primitive case to give an analogous characterization of the field of moduli. The issue at hand is that given a decomposition $A \cong E_1 \times E_2$, the quadratic forms Q_1 and Q_2 corresponding to E_1 and E_2 must necessarily lie in class groups with different discriminant by Proposition 2.2.4. Therefore, we need to use the Dirichlet composition in its generalized sense, as introduced in Chapter 2, in order to compute transcendental lattices.

When dealing with decompositions, it is always useful to keep in mind the diagram of orders,

$$\begin{tikzcd}
K & & \mathcal{O}_{K,f_1} \arrow[dl, hook] & \\
\mathcal{O}_K \arrow[u, hook] & \mathcal{O}_{K,f_0} \arrow[l, hook'] & & \mathcal{O}_{K,f} \arrow[ul, hook'] \arrow[dl, hook] \\
& & \mathcal{O}_{K,f_2} \arrow[ul, hook] &
\end{tikzcd}$$

and the corresponding one of class groups,

$$\begin{tikzcd}
& & C(\mathcal{O}_{K,f_1}) \arrow[dl] & \\
C(\mathcal{O}_K) & C(\mathcal{O}_{K,f_0}) \arrow[l] & & C(\mathcal{O}_{K,f}) \arrow[ul] \arrow[dl] \\
& & C(\mathcal{O}_{K,f_2}) \arrow[ul] &
\end{tikzcd}$$

where f_0, f_1, f_2, f are such that

$$\operatorname{lcm}(f_1, f_2) = f, \qquad \gcd(f_1, f_2) = f_0, \qquad f^2 d_K = \operatorname{disc} \mathrm{T}(A),$$

and also $[E_1] \in C(\mathcal{O}_{K,f_1})$ and $[E_2] \in C(\mathcal{O}_{K,f_2})$. The maps between the above class group are the one induced by extension of ideals; in terms of quadratic forms, these correspond to multiplication by the principal form of the target order: for instance, the reduction map

$$\mathrm{red}_0 : C(\mathcal{O}_{K,f}) \longrightarrow C(\mathcal{O}_{K,f_0})$$

sends $[Q]$ to $[Q] \circledast [P_0]$, where $\circledast$ is the generalized Dirichlet composition (see Chapter 2 for details), and P_0 is the principal form in $C(\mathcal{O}_{K,f_0})$. As before, there are maps

$$F_i : \mathrm{Gal}(\bar{K}/K) \longrightarrow C(\mathcal{O}_{K,f_i}) \qquad (i = 0, 1, 2),$$

such that

$$[Q_i^\sigma] = [F_i(\sigma)]^{-1} \circledast [Q_i] \qquad (i = 0, 1, 2).$$

By use of the generalized Dirichlet composition $\circledast$ and the maps F_i ($i = 1, 2$), we see that

$$E_1^\sigma \times E_2^\sigma \cong E_1 \times E_2 \Longleftrightarrow Q_1^\sigma \circledast Q_2^\sigma = Q_1 \circledast Q_2 \Longleftrightarrow F_1(\sigma) \circledast F_2(\sigma) = P_0.$$

The discussion above can be rephrased as follows:

Lemma 3.4.1. $G_K = \{\sigma \in \mathrm{Gal}(\bar{K}/K) \mid F_1(\sigma) \circledast F_2(\sigma) = P_0\}$.

In order to go any further, we need to understand the interaction of the maps F_i ($i = 0, 1, 2$). As the class groups are abelian groups, these maps factor through the Galois group of K^{ab}, the maximal abelian extension of K. We get maps (again called F_i by abuse of notation)

$$F_i : \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow C(\mathcal{O}_{K,f_i}).$$

Here is where the theory of idéles comes into play, picturing the behaviour of these maps in their totality.

3.4.2 Compatibility condition for the maps F_i

The idea is inspired by a paper of Schütt [28]: given a singular abelian surface A, among all decompositions that we can choose, there is one that behaves better that the others, namely the decomposition that Shioda and Mitani used to prove the surjectivity of the period map for singular abelian surfaces [39]. To the reader's convenience, we briefly recall this construction. Letting A be a singular abelian surface of transcendental lattice $\mathrm{T}(A) \cong (a, b, c)$, Shioda and Mitani showed that $A \cong E_\tau \times E_{a\tau+b}$, where

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

In particular, $E_{a\tau+b}$ always corresponds to the principal form in the class group of discriminant $D = \operatorname{disc} \mathrm{T}(A)$, and E_τ instead corresponds to the quadratic form $\mathrm{T}(A)_0$, the primitive part of $\mathrm{T}(A)$.

Let us assume $A \cong E_1 \times E_2$ is the Shioda-Mitani decomposition: if $\mathrm{T}(A) = Q = mQ_0$, then E_1 corresponds to the quadratic form $Q_0 \in C(D_0)$ and E_2 corresponds to the principal form $P \in C(D)$. Notice that we also have $A \cong \mathbb{C}/\mathfrak{a} \times \mathbb{C}/\mathcal{O}_{K,f}$, for $\mathfrak{a} \in C(\mathcal{O}_{K,f_0})$, and thus the proof of [28, Theorem 5.4] shows in particular that, for $\sigma \in \mathrm{Gal}(\bar{K}/K)$

$$A^\sigma \cong E_1^\sigma \times E_2^\sigma \cong \mathbb{C}/s^{-1}\mathfrak{a} \times \mathbb{C}/s^{-1}\mathcal{O}_{K,f} \cong \mathbb{C}/s^{-2}\mathfrak{a} \times \mathbb{C}/\mathcal{O}_{K,f},$$

where, as s varies in $\mathbb{I}_K$, $(s^{-1}\mathfrak{a})^2 = (s^{-1}Q_0)^2$ spans the whole genus of Q_0 in $C(D_0)$. This ultimately suggests that we look at elements of the form $s^{-1}\mathcal{O}$, as their squares span the principal genus of a class group, and characterize the transcendental lattice as it moves in its genus.

To do so, suppose we are given an order $\mathcal{O} \subset K$, the map

$$F : \mathrm{Gal}(\bar{K}/K) \longrightarrow C(\mathcal{O})$$

factorizes through a map

$$F : \mathrm{Gal}(K^{\mathrm{ab}}/K) \longrightarrow C(\mathcal{O}).$$

For $\sigma \in \mathrm{Gal}(K^{\mathrm{ab}}/K)$, $F(\sigma)$ has the property $[E^\sigma] = [\mathbb{C}/F(\sigma)^{-1} \cdot \mathfrak{a}]$ independently of the chosen $E = \mathbb{C}/\mathfrak{a} \in \mathcal{E}ll(\mathcal{O})$. By the Main Theorem of CM, there exists an idéle $s \in \mathbb{I}_K$ such that $\phi_K(s) = \sigma$ and

$$[E^\sigma] = [\mathbb{C}/F(\sigma)^{-1} \cdot \mathfrak{a}] = [\mathbb{C}/s^{-1}\mathfrak{a}].$$

As $s^{-1}\mathfrak{a} = (s^{-1}\mathcal{O}) \cdot \mathfrak{a}$, we can identify $[s\mathcal{O}] = [F(\sigma)]$. Now let $\mathcal{O}_0$ be another order in K, $\mathcal{O} \subset \mathcal{O}_0 \subset K$, and consider the following diagram;

$$\begin{tikzcd}
 & & C(\mathcal{O}) \arrow[dd, "\mathrm{red}_0"] \\
\mathbb{I}_K \arrow[r, "\phi_K"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[ur, "F"] \arrow[dr, "F_0"'] & \\
 & & C(\mathcal{O}_0)
\end{tikzcd}$$

we would like to show that the triangle on the right-hand side is indeed commutative. For $\sigma \in K^{\mathrm{ab}}$, we have the identifications

$$[F(\sigma)] = [s\mathcal{O}] \qquad \text{and} \qquad [F_0(\sigma)] = [s\mathcal{O}_0],$$

which are a consequence of the Main Theorem of CM. Notice that this uses the fact that the Main Theorem of CM holds for all elliptic curves with CM in any order in K at once. By looking at every rational prime p, one checks that $(s\Lambda) \cdot \Lambda' = s(\Lambda \cdot \Lambda')$, for two lattices Λ and Λ' in K (see [36]). In particular, after noticing that Λ and $s\Lambda$ have the same endomorphism ring, we get $[s\mathcal{O}] \circledast [\mathcal{O}_0] = [s\mathcal{O}_0]$. We have proven the following compatibily condition

Lemma 3.4.2. *Under the assumptions above,*

$$[F_0(\sigma)] = [F(\sigma)] \circledast [P_0],$$

or equivalently $\mathrm{red}_0 \circ F = F_0$.

This proves the commutativity of the triangle in the diagram above, and thus we are now ready to prove a characterization theorem for the field of K-moduli also in the imprimitive case.

3.4.3 Completion of the proof

In Lemma 3.4.1, we showed that

$$E_1^\sigma \times E_2^\sigma \cong E_1 \times E_2 \iff F_1(\sigma) \circledast F_2(\sigma) = P_0.$$

Now, $F_1(\sigma) \circledast F_2(\sigma)$ lives in $C(\mathcal{O}_{K,f_0})$ so we can multiply by the principal form P_0, and, by commutativity and Lemma 3.4.2, the last condition above is equivalent to $F_0(\sigma)^2 = P_0$, i.e. $F_0(\sigma) \in C(\mathcal{O}_{K,f_0})[2]$. Therefore we get, in analogy to the primitive case:

Proposition 3.4.3. $G_K = F_0^{-1}(C(\mathcal{O}_{K,f_0})[2])$.

Now, the same argument used in the primitive case (replacing every occurrence of H with H_0, the ring class field of $\mathcal{O}_{K,f_0}$), yields the following result, which extends Theorem 3.3.1 to the imprimitive case.

Theorem 3.4.4. *Let X be a singular K3 surface with transcendental lattice $T(X) = Q = mQ_0$, and let H_0 be the ring class field of $\mathcal{O}_{K,f_0}$, the order of discriminant* $\operatorname{disc} Q_0$*. Then the field of K-moduli is*

$$M_K = \bar{K}^{G_K}, \qquad G_K = (|_{H_0})^{-1}\operatorname{Gal}(H_0/K)[2];$$

it is a Galois extension of K of degree g, g being the order of the genus of the transcendental lattice of X.

3.5 The absolute field of moduli

So far, we have studied the field of K-moduli of a singular K3 surface X, K being the CM field of X. Now, we want to move our attention to the *absolute field of moduli* $M_{\mathbb{Q}}$, by which we mean the field of $\mathbb{Q}$-moduli.

We will proceed as in the case of M_K. Let us recall that the absolute field of moduli of X is the field $M_{\mathbb{Q}} := \mathbb{C}^{G_{\mathbb{Q}}}$, where

$$G_{\mathbb{Q}} = \{\sigma \in \operatorname{Gal}(\mathbb{C}/\mathbb{Q}) \mid X^\sigma \in [X]\}.$$

The proof of Lemma 3.2.3 shows that we can equivalently define the field of moduli $M_{\mathbb{Q}}$ to be the subfield of $\bar{\mathbb{Q}}$ which is fixed by the group

$$G_{\mathbb{Q}} = \{\sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \mid X^\sigma \in [X]\}.$$

As G_K is the subgroup of elements of $G_{\mathbb{Q}}$ whose restriction to K is trivial, we have the following commutative diagram,

$$\begin{tikzcd}
0 \arrow[r] & G_K \arrow[r] \arrow[d, hook] & G_{\mathbb{Q}} \arrow[r] \arrow[d, hook] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \operatorname{Gal}(\bar{\mathbb{Q}}/K) \arrow[r] & \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \arrow[r, "|_K"] & \operatorname{Gal}(K/\mathbb{Q}) \arrow[r] & 0
\end{tikzcd}$$

where C is simply the quotient group $G_{\mathbb{Q}}/G_K$ (notice that G_K is normal in $G_{\mathbb{Q}}$). We have the following:

Proposition 3.5.1. $C \cong \operatorname{Gal}(K/\mathbb{Q})$.

Proof. As complex conjugation acts as the inverse in the corresponding class group, we need to distinguish two cases, according to whether the transcendental lattice of X is 2-torsion or not. Let us consider the case of $\mathrm{T}(X)$ being 2-torsion first. This is equivalent to the condition that $X^{\iota} \cong X$, ι being the complex conjugation automorphism. Under this assumption, a nontrivial element $\sigma \in G_{\mathbb{Q}}$ is either contained in G_K or $\iota\sigma$ lies in G_K; this implies that $C \cong \mathrm{Gal}(K/\mathbb{Q})$. We are left to deal with the case when $\mathrm{T}(X)$ is not 2-torsion. This condition is equivalent to $X^{\iota} \ncong X$. Assume there exists an element $\sigma \in G_{\mathbb{Q}} \setminus G_K$, thus $X^{\sigma} \cong X$ and $\sigma|_K \neq \mathrm{id}_K$. Notice that

$$X \cong X^{\sigma^{-1}\sigma} \cong (X^{\sigma})^{\sigma^{-1}} \cong X^{\sigma^{-1}},$$

so that also $\sigma^{-1} \in G_{\mathbb{Q}} \setminus G_K$. If $\tau \in G_{\mathbb{Q}} \setminus G_K$ is another such element, then $\sigma\tau^{-1} \in G_K$, which means $\bar{\sigma} = \bar{\tau} \in C$. This implies that $C \cong \mathbb{Z}/2\mathbb{Z}$, and thus we can identify the quotient group C with $\mathrm{Gal}(K/\mathbb{Q})$. □

As a consequence, we have the diagram of field extensions in Figure 3.1,

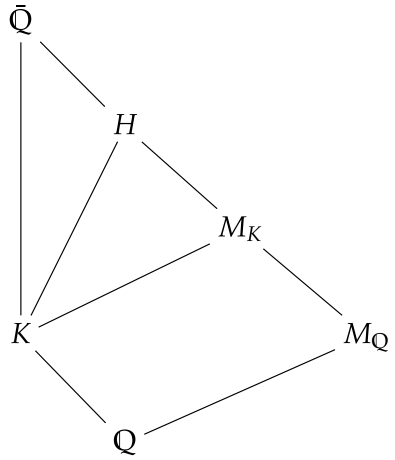

Figure 3.1: Relative and absolute field of moduli

where all extensions are Galois, except possibly for $M_{\mathbb{Q}}/\mathbb{Q}$. We see that $M_K/M_{\mathbb{Q}}$ is Galois with group $C \cong \mathrm{Gal}(K/\mathbb{Q})$, thus $M_K \supsetneq M_{\mathbb{Q}}$. By multiplicativity of degrees, the extensions M_K/K and $M_{\mathbb{Q}}/\mathbb{Q}$ have the same degree.

Remark 3.5.2. We would like to point out that Figure 3.1 recovers the picture of the case of elliptic curves with CM in K. For an elliptic curve E with CM in an imaginary quadratic field K, $M_{\mathbb{Q}} = \mathbb{Q}(j(E))$ and $M_K = K(j(E)) = H$, H being the ring class field of the elliptic curve E (we are implicitly using the fact that elliptic curves correspond to quadratic forms). The equality $M_K = H$ is explained by the fact that the field of K-moduli coincides with the minimal field of definition, for every elliptic curve with CM in K.

As a consequence of the discussion above, we have the following:

Theorem 3.5.3. *Let X be a singular K3 surface. Its absolute field of moduli $M_{\mathbb{Q}}$ is a degree-two subfield of the field of K-moduli M_K. Moreover, $M_{\mathbb{Q}}$ is an extension of $\mathbb{Q}$ of degree*

$$[M_{\mathbb{Q}} : \mathbb{Q}] = [M_K : K] = g,$$

g being the genus of $T(X)$. In general, it is not a Galois extension of $\mathbb{Q}$.

We remark that K is not contained in $M_{\mathbb{Q}}$, and thus $M_{\mathbb{Q}} \cap K = \mathbb{Q}$. Indeed, if this were the case, then we would have $G_{\mathbb{Q}} \subset \mathrm{Gal}(\bar{\mathbb{Q}}/K)$. If $\mathrm{T}(X)$ is 2-torsion, then $\iota \in G_{\mathbb{Q}} \setminus \mathrm{Gal}(\bar{\mathbb{Q}}/K)$, and so we get a contradiction. If $\mathrm{T}(X)$ is not 2-torsion, then any $\tau \in G_{\mathbb{Q}} \setminus G_K$ yields the same contradiction.
The final statement of Theorem 3.5.3 is that the extension $M_{\mathbb{Q}}/\mathbb{Q}$ is not Galois in general; the following example shows an occurrence of this phenomenon.

Example 3.5.4 (Example 3.3.5 reloaded). We compute the absolute field of moduli for the K3 surface X. Our results tell us that $M_{\mathbb{Q}}$ must be an extension of degree 3 of $\mathbb{Q}$. In this case, X has a model over $\mathbb{Q}(j(P))$, which is a degree 3 extension of $\mathbb{Q}$, so it follows that the absolute field of moduli $M_{\mathbb{Q}}$ is indeed $\mathbb{Q}(j(P))$ itself, which agrees with Theorem 3.5.3. Now, the class polynomial $H_{\mathcal{O}_K}(T)$ of the order $\mathcal{O}_K$ has $j(P)$, $j(Q)$ and $j(Q^{-1})$ as roots; $j(P)$ is real, while $j(Q) = \overline{j(Q^{-1})}$. It follows that the extension $\mathbb{Q}(j(P))/\mathbb{Q}$ cannot be Galois.

For a more interesting example, we look at the K3 surface Y, and we recall that

$$\mathbb{Q}(j_1, j_2) = K(j_1, j_2) = K(j_2), \qquad [\mathbb{Q}(j_1, j_2) : \mathbb{Q}] = 6,$$

if we consider a Shioda-Inose model for Y. As the field of moduli $M_{\mathbb{Q}}$ in contained in every field of definition for Y, and must have degree 3 by Theorem 3.5.3, we must find an element $\alpha \in \mathrm{Gal}(H/\mathbb{Q})$ which leaves the modulus invariant. If ι denotes the (restriction of the) complex conjugation automorphism and $\sigma \in \mathrm{Gal}(\bar{K}/K)$ is an element such that $F(\sigma) = Q^{-1}$, then $\alpha := \sigma\iota$ satisfies this condition. Therefore $M_{\mathbb{Q}}$ is the subfield of H which is fixed by the group generated by α: this group has order 2, and thus we get that $M_{\mathbb{Q}}$ is an extension of $\mathbb{Q}$ of degree 3, as expected. □

3.6 Further questions

3.6.1 Non-finiteness of singular K3 surfaces

The following discussion is inspired by the following striking result of Šafarevič on the finiteness of singular K3 surfaces with bounded field of definition:

Theorem 3.6.1 (Theorem 1 of [34])**.** *Let n be a positive integer. There exist finitely many singular K3 surfaces with a model over a number field K of degree $[K : \mathbb{Q}] \leq n$.*

This result says that we can use the degree of the field of definition to stratify Σ^{K3}, and that each stratum contains finitely many elements only: the n^{th} stratum is defined as

$$\Sigma^{\mathrm{K3}}(n) := \{[X] \in \Sigma^{K3} \,:\, X \text{ has a model over } K,\, [K : \mathbb{Q}] \leq n\}.$$

One might wonder whether a similar result holds for the field of moduli in place of the field of definition. We will now see that this is not the case.

Proposition 3.6.2. *Let X and Y be two singular K3 surfaces such that $\mathrm{T}(X)$ is primitive (as a quadratic form) and $\mathrm{T}(Y) = n\mathrm{T}(X)$, for some $n \in \mathbb{N}$. Then, X and Y have the same field of K-moduli, K being the CM field of X and Y.*

Proof. The argument used in proving Theorem 3.4.4 shows, in particular, that the ring class field H_0 only depends on the discriminant of the primitive part of the transcendental lattice. In the situation at hand, X and Y would both lead to the same ring class field, and the result is then a consequence of Theorem 3.4.4. □

Proposition 3.6.3. *Let X and Y be two singular K3 surfaces whose transcendental lattices are primitive and lie in the same class group (as quadratic forms). Then, X and Y have the same field of K-moduli, K being the CM field of X and Y.*

Proof. Same as for Proposition 3.6.2. □

As a corollary, we get that

Corollary 3.6.4. *Let X and Y be two singular K3 surfaces such that the primitive parts of $\mathrm{T}(X)$ and $\mathrm{T}(Y)$ lie in the same class group (as quadratic forms). Then, X and Y have the same field of K-moduli, K being the CM field of X and Y.*

In particular, this shows that bounding the degree of the (relative) field of moduli is not enough to have a stratification of Σ^{K3} in strata containing finitely many elements only. In fact, we have shown that for each possible field of K-moduli, there exist infinitely many singular K3 surfaces with that field of K-moduli. This non-finiteness result holds true also if we replace the relative field of moduli with the absolute one: in fact, it is enough to fix a primitive quadratic form Q such that $h(\operatorname{disc} Q) = 1$; then

$$\#\{[X] \in \Sigma^{\mathrm{K3}} \,:\, \mathrm{T}(X) = mQ,\ m \in \mathbb{N}\} = +\infty,$$

and all K3 surfaces in the set above have clearly $\mathbb{Q}$ as absolute field of moduli.

3.6.2 Explicit fields of K-moduli

We can still ask questions such as: which fields can appear as the field of K-moduli of a singular K3 surface? To answer such a question, Theorem 3.4.4 and its description of the field of moduli does not help us. The ideal situation would be to describe M_K as the subfield of a finite extension of K fixed by a (finite) group. This would also allow us to explicitly describe this field with the aid of a computer algebra system.

In consequence of Proposition 3.6.2, we can restrict ourselves to working with singular K3 surfaces whose transcendental lattice is primitive as a quadratic form; thus, let X be such a singular K3 surface. Consider X as obtained by a singular abelian surface A in its Shioda-Mitani model $A \cong E_Q \times E_P$. Let us remind the reader that Q and P

belong to the same class group, exactly because the transcendental lattice is primitive. Then, a result of Schütt [28] implies that X has a model[4] over the ring class field

$$H := K(j_1, j_2) = K(j_2), \qquad j_k := j(E_k) \quad (k = 1, 2).$$

This model is particularly nice as the extension H/K is Galois by class field theory. It is clear that $\mathrm{Gal}(\bar{K}/H) \subseteq G_K$, because of the existence of a model over H. Also, the arguments in Section 3.3 yield a proof of the following result:

Proposition 3.6.5. $M_K = H^{\mathrm{Gal}(H/K)[2]}$.

Proof. Let us consider the restriction map

$$|_H : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Gal}(H/K).$$

By the existence of a model over H, G_K maps onto the following subgroup of $\mathrm{Gal}(H/K)$:

$$G_K|_H := \{\sigma \in \mathrm{Gal}(H/K) \mid X^\sigma \cong X\}.$$

The proof of Proposition 3.3.2 shows in particular that $G_K|_H = \mathrm{Gal}(H/K)[2]$. Therefore, one has the following commutative diagram of groups,

$$\begin{tikzcd}
G_K \arrow[r, hook] \arrow[d, two heads, "|_H"'] & \mathrm{Gal}(\bar{K}/K) \arrow[d, two heads, "|_H"] \\
\mathrm{Gal}(H/K)[2] \arrow[r, hook] & \mathrm{Gal}(H/K)
\end{tikzcd}$$

from which the proof follows after a direct check. □

This last result allows us to explicitly compute the field of moduli of a given singular K3 surface. We can have a computer algebra system run this sort of computations for us, but in order to do so, we have to reduce to isolate a finite number of cases at the time. To this end, Proposition 3.6.2 enables us to project Σ^{K3} onto

$$\Sigma^{\mathrm{K3}}_{\mathrm{prim}} := \{[X] \in \Sigma^{\mathrm{K3}} \, : \, \mathrm{T}(X) \text{ is primitive}\},$$

by forgetting the index of primitivity of the transcendental lattice. Analogously to the situation of [39], there is a 1:1 correspondence

$$\Sigma^{\mathrm{K3}}_{\mathrm{prim}} \longleftrightarrow \mathcal{Q}_0^+ \,/\, \mathrm{SL}_2(\mathbb{Z}),$$

where $\mathcal{Q}_0^+$ is the subset of $\mathcal{Q}^+$ containing primitive quadratic forms only. Class group theory implies that

$$\mathcal{Q}_0^+ \,/\, \mathrm{SL}_2(\mathbb{Z}) \cong \bigsqcup_{\substack{K \text{ quadratic imaginary field} \\ f \in \mathbb{N}}} C(\mathcal{O}_{K,f}),$$

[4] More generally it has a model over the field $\mathbb{Q}(j_1, j_2)$, which does not always coincide with the ring class field H.

and thus we can bound $\Sigma^{\mathrm{K3}}_{\mathrm{prim}}$ by bounding the orders in the quadratic imaginary fields. This can be achieved, for instance, by bounding the discriminant or the class number. Such constraint gives a stratification of $\Sigma^{\mathrm{K3}}_{\mathrm{prim}}$ whose strata contain finitely many elements only, and we can therefore run the computations in a finite, perhaps long, time.

3.6.3 More on the field of $\mathbb{Q}$-moduli

Let X be a singular K3 surface, and let us assume that its transcendental lattice $\mathrm{T}(X) = Q_0$ is primitive. Let Y be another singular K3 surface, such that $\mathrm{T}(Y) = m\mathrm{T}(X)$, for some $m > 0$. From previous discussions, we know that X and Y will have the same field of K-moduli, with $K = \mathbb{Q}(\sqrt{\operatorname{disc}\mathrm{T}(X)})$. We would like to study the analogous question for the field of $\mathbb{Q}$-moduli. We are able to prove the following:

Proposition 3.6.6. *If* $\mathrm{T}(X)$ *is 2-torsion in its class group, then* $M_{\mathbb{Q}}(X) = M_{\mathbb{Q}}(Y)$.

Proof. As $\mathrm{T}(X)$ is 2-torsion in its class group, $\mathrm{T}(Y)$ is 2-torsion as well. Otherwise said, if ι denotes the complex conjugation automorphism, $\iota \in G_{\mathbb{Q}}(X)$ if and only if $\iota \in G_{\mathbb{Q}}(Y)$. For X and Y as above, let us consider their Shioda-Mitani models:

$$X \cong \mathrm{SI}(A), \qquad A = E_{Q_0} \times E_{P_0} \in \Sigma^{\mathrm{K3}},$$
$$Y \cong \mathrm{SI}(B), \qquad B = E_{Q_0} \times E_{P} \in \Sigma^{\mathrm{K3}}.$$

We have that

$$\sigma \in G_K(X) \iff F_0(\sigma)^2 = P_0, \qquad F_0 : \mathrm{Gal}(\bar{K}/K) \longrightarrow C(D_0),$$
$$\sigma \in G_K(Y) \iff F_0(\sigma) \circledast F(\sigma) = P_0, \qquad F : \mathrm{Gal}(\bar{K}/K) \longrightarrow C(D).$$

We would like to prove that the field of $\mathbb{Q}$-moduli is independent of the index of primitivity of a singular K3 surface, namely, in the notation above, that $M_{\mathbb{Q}}(X) = M_{\mathbb{Q}}(Y)$. Notice immediately that, as $M_K(X) = M_K(Y)$, we have $G_K(X) = G_K(Y)$ by Galois theory. Suppose $\iota \in G_{\mathbb{Q}}(X)$, or equivalently $X^{\iota} \cong X$. Then, by the above discussion, we also have $Y^{\iota} \cong Y$. Let $\sigma \in G_{\mathbb{Q}}(Y) \setminus G_K(Y)$; then, we also have $\sigma^{-1} \in G_{\mathbb{Q}}(Y) \setminus G_K(Y)$. By composing with complex conjugation, we get $\iota\sigma \in G_K(Y)$, which is equivalent to

$$F(\iota\sigma) \circledast F_0(\iota\sigma) = P_0.$$

In turn, this implies $F_0(\sigma)^2 = P_0$, or equivalently $\sigma \in G_K(X) \subseteq G_{\mathbb{Q}}(X)$. Therefore, $G_{\mathbb{Q}}(Y) \subseteq G_{\mathbb{Q}}(X)$, hence $M_{\mathbb{Q}}(X) \subseteq M_{\mathbb{Q}}(Y)$; as they have the same degree as extensions of $\mathbb{Q}$, it follows that $M_{\mathbb{Q}}(X) = M_{\mathbb{Q}}(Y)$. This proves that, if $\mathrm{T}(X)$ is 2-torsion in its class group, then $M_{\mathbb{Q}}(X) = M_{\mathbb{Q}}(Y)$, and thus that the field of $\mathbb{Q}$-moduli is independent of the index of primitivity in this case. □

Question 3.6.7. Is the field of $\mathbb{Q}$-moduli invariant under taking multiples of the transcendental lattice if $\mathrm{T}(X)$ is not 2-torsion in its class group?

This is currently under investigation, and we expect the answer to this question to be affirmative.

Chapter 4

Non-completeness of Picard numbers of abelian varieties

> This world has been connected. Tied to the darkness...soon to be completely eclipsed. There is so very much to learn. You understand so little...A meaningless effort. One who knows nothing can understand nothing.
>
> Ansem, *Kingdom Hearts*

4.1 Introduction

4.1.1 Computing the Picard number in general

For an algebraic variety X over the field of complex numbers the Lefschetz $(1,1)$-theorem says that the Néron-Severi group

$$\mathrm{NS}(X) = \mathrm{H}^2(X, \mathbb{Z}) \cap \mathrm{H}^{1,1}(X).$$

Consequently, the Picard number of X satisfies the inequality $1 \leq \rho(X) \leq h^{1,1}(X)$. Computing the Picard number is in general a difficult question, as already the case of projective surfaces shows. For example, the Picard number of a quintic surface S in $\mathbb{P}^3$ satisfies the inequality $\rho(S) \leq 45$. It is known that all numbers between 1 and 45 can be obtained if one allows the surface to have ADE-singularities, but it remains an open problem for smooth surfaces, where the maximum known is 41 [29], [30].

In this chapter we will concentrate on the Picard numbers of abelian varieties. To put this into perspective it is worthwhile to recall the situation for surfaces. For abelian surfaces all possible Picard numbers between 1 (or 0 if one includes the non-algebraic case) and 4 occur. Indeed, a very general abelian surface has $\rho = 1$, whereas Picard numbers from 2 to 4 can be realized by taking a product $E_1 \times E_2$ of two elliptic curves. If the two elliptic curves are not isogenous, then $\rho = 2$, if they are isogenous but they do not have complex multiplication, then $\rho = 3$, while if they also have complex multiplication $\rho = 4$. For the other surfaces with trivial canonical bundle the situation is similar: for K3 surfaces all possibilities between 1 (respectively 0) and 20 can occur as can be seen by the Torelli theorem for K3 surfaces and the Lefschetz $(1,1)$-theorem. Enriques surfaces and bi-elliptic surfaces have $p_g = 0$ and their Picard number is 10 and 2 respectively.

Turning to higher dimension, by the Beauville-Bogomolov decomposition theorem [4], every Kähler manifold with trivial first Chern class admits a finite cover which is a product of tori, Calabi-Yau varieties and irreducible holomorphic symplectic manifolds (IHSM), also know as hyperkähler manifolds. For higher dimensional Calabi-Yau varieties Y we always have $\rho(Y) = b_2(Y)$ as $h^{2,0}(Y) = h^{0,2}(Y) = 0$. For IHSM one can use Huybrechts' surjectivity of the period map [11] to conclude, as in the case of K3 surfaces, that all values $1 \leq \rho(X) \leq b_2(X) - 2$ can be obtained. This leaves us with he case of abelian variteies which is the main topic of this chapter.

4.1.2 Results and organization of the chapter

Let A be an abelian variety of dimension g. The cohomology of an abelian variety is the exterior algebra over $\mathrm{H}^1(A, \mathbb{Z}) \cong \mathbb{Z}^{2g}$. In particular, this implies that the k^{th} Betti numbers are $b_k(A) = \binom{2g}{k}$. As $\mathrm{H}^{p,0}(A) \cong \mathrm{H}^0(A, \Omega_A^p)$, we get $h^{p,0}(A) = \binom{g}{p}$, and thus $h^{1,1}(A) = g^2$. We conclude that one has the following possible Picard numbers for an abelian variety:

$$1 \leq \rho \leq g^2.$$

As we have already seen any number $1 \leq \rho(A) \leq 4$ can be achieved for abelian surfaces. The situation, however, changes significantly in higher dimension. In principle, the Picard number of an abelian variety A can be computed by decomposing it in its isogeny class into a product of powers of simple abelian varieties with no non-trivial morphisms between them, and by using a result of Murty [25] computing the Picard number of such self-products. It is then a combinatorial question as to determine the set R_g of possible Picard numbers of abelian varieties for a given genus g. Very little seems to be known about this. Our aim is to take a first step in the analysis of the set R_g. In particular, we show that there are series of gaps for the possible Picard numbers of abelian varieties, more precisely we obtain the

Main Theorem.

1. *Fix $g \geq 4$. There does not exist any abelian variety of dimension g with Picard number ρ in the following range:*

$$(g-1)^2 + 1 < \rho < g^2.$$

2. *Fix $g \geq 7$. There does not exist any abelian variety of dimension g with Picard number ρ in the following range:*
$$(g-2)^2 + 4 < \rho < (g-1)^2 + 1.$$

We would like to remark that the conditions on the dimension g given in Part 1 and 2 of the Main Theorem are necessary. In fact, as for Part 1, for $g = 2$ all Picard numbers appear, and for $g = 3$ there exists an abelian threefold of Picard number $\rho = 6$ (namely, the product of three isogenous elliptic curves without CM). Similar considerations can be made for Part 2 of the Main Theorem and $g \leq 6$.

This chapter is organized as follows. In Section 4.2 we reduce the problem to considering self-products of simple abelian varieties in Proposition 4.2.3. This then allows us to use a result of Murty [25], who computed the Picard numbers of such products in terms of the endomorphism ring. This provides us with some bounds on the Picard numbers. In Section 4.3 we give the proof of the main theorem and in Section 4.4 we briefly discuss some computer aided calculations of the set R_g for $g \leq 30$.

4.2 Preliminary work

In this section we are going to develop the tools for proving the main theorem stated in the introduction. Some of these results are certainly of interest on their own.

4.2.1 Additivity of the Picard number for certain products

As the Picard number is invariant under isogenies [6, Ch. 1, Prop. 3.2], we can pick a convenient representative in the isogeny class. A good choice for this is suggested by the following result.

Theorem 4.2.1 (Poincaré's Complete Reducibility Theorem, Thm. 5.3.7 of [7])**.** *Given an abelian variety A, there exists an isogeny*
$$A \longrightarrow A_1^{n_1} \times \cdots \times A_r^{n_r},$$
where A_i is a simple abelian variety ($i = 1, \ldots, r$), and A_i is not isogenous to A_j if $i \neq j$. Moreover, the abelian varieties A_i and the integers n_i are uniquely determined up to isogeny and permutations.

Let us now consider a product of simple abelian varieties as in Theorem 4.2.1. The fact that A_i is not isogenous to A_j for $i \neq j$ yields the following interesting splitting of the Picard group:

Proposition 4.2.2. *Let $A_1, \ldots, A_r$ be simple abelian varieties, such that A_i is not isogenous to A_j for $i \neq j$. Then, (exterior) pullback of line bundles yields an isomorphism*
$$\prod_{i=1}^{r} \mathrm{Pic}(A_i^{n_1}) \cong \mathrm{Pic}\left(\prod_{i=1}^{r} A_i^{n_i}\right),$$

Clearly, exterior pull-back of line bundles always yields an injective map, but surjectivity is a special feature. In fact, if E is an elliptic curve, the abelian surface $E \times E$ has Picard number $\rho \in \{3,4\}$, depending on the presence of CM. Therefore, the exterior pull-back map

$$\mathrm{Pic}(E) \times \mathrm{Pic}(E) \longrightarrow \mathrm{Pic}(E \times E)$$

cannot be surjective, as otherwise we would get a surjective map of the corresponding Néron-Severi groups, hence yielding a contradiction, since $\mathrm{NS}(E) \cong \mathbb{Z}$.

Proof. Exterior pullback of line bundles

$$\psi(L_1, \ldots, L_r) = L_1 \boxtimes \cdots \boxtimes L_r$$

defines the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Pic}^0(\prod_{i=1}^r A_i^{n_i}) \arrow[r] & \mathrm{Pic}(\prod_{i=1}^r A_i^{n_i}) \arrow[r] & \mathrm{NS}(\prod_{i=1}^r A_i^{n_i}) \arrow[r] & 0 \\
0 \arrow[r] \arrow[u] & \prod_{i=1}^r \mathrm{Pic}^0(A_i^{n_i}) \arrow[r] \arrow[u, "\psi^0"'] & \prod_{i=1}^r \mathrm{Pic}(A_i^{n_i}) \arrow[r] \arrow[u, "\psi"'] & \prod_{i=1}^r \mathrm{NS}(A_i^{n_i}) \arrow[r] \arrow[u, "\psi^{\mathrm{NS}}"'] & 0 \arrow[u]
\end{tikzcd}$$

We will show that ψ^0 and ψ^{NS} are isomorphisms, thus proving the proposition. Clearly ψ^0 is injective, and since ψ^0 is a homomorphism of abelian varieties of the same dimension it must be an isomorphism. To prove that ψ^{NS} is an isomorphism we recall from [7, Ch. 2] that a polarization on an abelian variety A is given by a finite isogeny $f : A \to A^\vee$ whose analytic representation is hermitian. By assumption the abelian varieties A_i and A_j are not isogeneous for $i \neq j$. Hence $\mathrm{Hom}(A_i, A_j) = \mathrm{Hom}(A_i, A_j^\vee) = 0$ and every isogeny $f : \prod_{i=1}^r A_i^{n_i} \to (\prod_{i=1}^r A_i^{n_i})^\vee$ is of the form $f = (f_1, \ldots, f_r)$ where $f_i : A_i^{n_i} \to (A_i^{n_i})^\vee$ is an isogeny. Since a direct sum of endomorphisms is hermitian if and only if all its summands are, the claim follows as any divisor is the difference of two very ample divisors (i.e. two polarizations). □

As a consequence, we get that the Picard number is additive (but not strongly additive) for product varieties coming from the Poincaré's Complete Reducibility Theorem.

Proposition 4.2.3. *Let $A_1, \ldots, A_r$ be simple abelian varieties, such that A_i is not isogenous to A_j for $i \neq j$. Then,*

$$\rho\left(\prod_{i=1}^r A_i^{n_i}\right) = \sum_{i=1}^r \rho(A_i^{n_i}).$$

4.2.2 Picard numbers of self-products

Due to additivity, we are left to see how to compute the Picard number in the case of a self-product of a simple abelian variety. If A is a simple abelian variety, we can consider $\Delta(A) := \mathrm{End}(A) \otimes \mathbb{Q}$, *i.e.* the (smallest) algebra containing $\mathrm{End}(A)$ where the multiplication maps $[n] : A \longrightarrow A$ become invertible elements ($n \in \mathbb{Z}$). We denote its centre by F, which comes with a natural involution. We will say that F is *of the first kind* if this involution acts trivially on F, and *of the second kind* otherwise. Endomorphism algebras of simple abelian varieties have been studied and classified (see [7, Proposition 5.5.7]) into four types, where the first three are of the first kind:

1. *Type I*: $\Delta(A) = F$ and $\Delta(A)$ is a totally real number field;
2. *Type II*: $\Delta(A)$ is a totally indefinite quaternion algebra over F;
3. *Type III*: $\Delta(A)$ is a totally definite quaternion algebra over F;
4. *Type IV*: F is of the second kind.

Depending on the dimension g, some of the above cases may not occur, as there are restrictions on the numerical invariants of $\Delta(A)$; for details, see [7, Prop. 5.5.7]. The following result gives a complete description of the Picard number of a self-product of a simple abelian variety.

Proposition 4.2.4 (Lemma 3.3 of [25]). *Let A be a simple abelian variety, and let E be a maximal commutative subfield of $\Delta(A)$ which is totally real for type I and a CM field in the other cases. Set $f := [F : \mathbb{Q}]$, $q := [E : F]$. Then, for $k \geq 1$, one has*

$$\rho(A^k) = \begin{cases} \frac{1}{2}fk(k+1) & \textit{Type I} \\ fk(2k+1) & \textit{Type II} \\ fk(2k-1) & \textit{Type III} \\ \frac{1}{2}q^2fk^2 & \textit{Type IV.} \end{cases}$$

Murty's result enables us to compute the following bound for the Picard number of a self-product of a simple abelian variety:

Corollary 4.2.5. *Let A be a simple abelian variety of dimension n, and let $k \geq 1$. Then $\rho(A^k) \leq \frac{1}{2}nk(2k+1)$.*

Proof. Proposition 4.2.4 applied with $k = 1$ allows us to compute the Picard number of A:

$$\rho = \rho(A) = \begin{cases} f & \textit{Type I} \\ 3f & \textit{Type II} \\ f & \textit{Type III} \\ \frac{1}{2}q^2f & \textit{Type IV.} \end{cases}$$

Now, plugging this back in Proposition 4.2.4 gives the following reformulation in terms of the Picard number of A:

$$\rho(A^k) = \begin{cases} \frac{1}{2}\rho k(k+1) & \textit{Type I} \\ \frac{1}{3}\rho k(2k+1) & \textit{Type II} \\ \rho k(2k-1) & \textit{Type III} \\ \rho k^2 & \textit{Type IV.} \end{cases}$$

The divisibility conditions for ρ given by [7, Prop. 5.5.7] imply that

$$\rho \leq \begin{cases} n & \textit{Type I} \\ \frac{3}{2}n & \textit{Type II} \\ \frac{1}{2}n & \textit{Type III} \\ n & \textit{Type IV} \end{cases}$$

and, therefore, we see that

$$\rho(A^k) \leq \begin{cases} \frac{1}{2}nk(k+1) & \textit{Type I} \\ \frac{1}{2}nk(2k+1) & \textit{Type II} \\ \frac{1}{2}nk(2k-1) & \textit{Type III} \\ nk^2 & \textit{Type IV} \end{cases}$$

from which the result follows. □

We will use this result in the proof of the Main Theorem. Notice that Corollary 4.2.5 provides us with a bound on the Picard number of A^k which is independent of the type of the endomorphism ring of A.

4.2.3 Some bounds on the Picard number

We would like to show that there are better bounds on the Picard number, if one is given a partition of the dimension. More precisely, letting A be an abelian variety, we define $r(A)$ to be the *length* of a decomposition according to Poincaré Complete Reducibility Theorem. In other words, given an abelian variety A, Theorem 4.2.1 gives an isogeny

$$A \longrightarrow A_1^{n_1} \times \cdots \times A_r^{n_r},$$

and we set $r(A) := r$. Notice that this quantity is well-defined because the factors A_i and the powers n_i are determined up to permutations and isogenies. Then, for $r \leq g$, we define $M_{r,g}$ as

$$M_{r,g} := \max\{\rho(A) \mid \dim A = g,\ r(A) = r\}.$$

In other words, $M_{r,g}$ is the largest Picard number that can be realized by a g-dimensional abelian variety that splits into a product of r non-isogenous pieces in its isogeny class.

Proposition 4.2.6. *For integers $r, g \in \mathbb{N}$ such that $r \leq g$, one has $M_{r,g} = [g-(r-1)]^2 + (r-1)$. This value is attained as the Picard number of $E^{(g-r+1)} \times E_1 \times \cdots \times E_{r-1}$, where E is a CM elliptic curve not isogenous to any of the E_i's, and E_i and E_j are not isogenous for $i \neq j$.*

Proof. If $A \sim A_1 \times \cdots \times A_r$, $\mathrm{Hom}(A_i, A_j) = 0$ for $i \neq j$, then

$$\rho(A) \leq k_1^2 + \cdots + k_r^2,$$

where $k_i := \dim A_i$ $(i = 1, \ldots, r)$. Moreover, $k_1 + \cdots + k_r = g$, and thus

$$\rho(A) \leq k_1^2 + \cdots + k_{r-1}^2 + (g - k_1 - \cdots - k_{r-1})^2.$$

Notice that $k_i \geq 1$, for $1 \leq i \leq r - 1$, and that $1 \leq k_r = g - k_1 - \cdots - k_{r-1}$. Consider the function

$$f(x_1, \ldots, x_{r-1}) = x_1^2 + \cdots + x_{r-1}^2 + (g - x_1 - \cdots - x_{r-1})^2$$

in the domain Ω, given by the conditions

$$x_1, \cdots, x_{r-1} \geq 1, \qquad x_1 + \cdots + x_{r-1} \leq g - 1.$$

The equation $z = f(x_1, \ldots, x_{r-1})$ is a paraboloid, with a unique minimum at $b = \big(g/(r-1), \ldots, g/(r-1)\big)$. Notice that b is the centroid of Ω, so that the maximum of f in Ω is at one of the vertices of Ω. Since the function f only depends on the distance from b, the maximum is in fact attained at every vertex of Ω, hence

$$M_{r,g} \leq f(1, \ldots, 1) = [g - (r-1)]^2 + (r - 1).$$

By applying Proposition 4.2.2, one can see that the abelian variety

$$E^{(g-r+1)} \times E_1 \times \cdots \times E_{r-1}$$

has Picard number $[g - (r-1)]^2 + (r-1)$, and we are done. □

4.3 Proof of Main Theorem

4.3.1 Proof of Main Theorem (1)

Let A be an abelian variety of dimension $g \geq 4$, and let $\rho := \rho(A)$. We will divide our analysis of the Picard number ρ in the following mutually exclusive cases:
(a) A has length at least two, i.e. $r(A) \geq 2$;
(b) A is a simple abelian variety;
(c) A is a self-product of a lower dimensional abelian variety.
Case (a). Suppose that, in its isogeny class, A decomposes into a product $\prod_{i=1}^r A_i^{n_i}$ with $r \geq 2$, and define

$$n := \min\{n_i \cdot \dim(A_i) | 1 \leq i \leq r\}.$$

If n is realized by considering the j^{th} factor, set

$$B_n := A_j^{n_j} \qquad \text{and} \qquad B_{g-n} := \prod_{i \neq j} A_i^{n_i}.$$

Notice that here we use the fact that $r \geq 2$, as otherwise B_{g-n} would be empty. In this setting, by Corollary 4.2.3,

$$\rho(A) = \sum_{i=1}^{r} \rho(A_i^{n_i}) = \rho(A_j^{n_j}) + \sum_{i \neq j} \rho(A_i^{n_i}) = \rho(B_n) + \rho(B_{g-n}) \leq n^2 + (g-n)^2.$$

By minimality, $n \leq g - n$, i.e. $g \geq 2n$. We claim that

$$n^2 + (g-n)^2 \leq (g-1)^2 + 1.$$

Indeed, as $1 \leq n \leq g/2$, we can look at the function $f(x) := x^2 + (g-x)^2$ in the interval $1 \leq x \leq g/2$: it is decreasing, and its maximum at $x = 1$ has value $f(1) = 1 + (g-1)^2$, thus yielding the corresponding bound on the Picard number.

Case (b). If A is simple, then Lemma 4.2.5 implies that $\rho \leq \frac{3}{2}g$. One can check that, for $g \geq 4$, it is always the case that

$$\frac{3}{2}g \leq (g-1)^2 + 1.$$

Case (c). Let B be an m-dimensional simple abelian variety, and suppose A is isogenous to B^k, for $k := g/m$. If $m = 1$ (i.e. B is an elliptic curve), then

$$\rho(B^g) = \begin{cases} \binom{g+1}{2} & B \text{ has no CM} \\ g^2 & B \text{ has CM} \end{cases}.$$

If B has CM, then A attains the top Picard number g^2; if B does not have CM, then

$$\rho(A) = \binom{g+1}{2} \leq 1 + (g-1)^2,$$

because $g \geq 4$. The case of a self-product of an elliptic curve being dealt with, we can assume $k \leq g/2$. Then,

$$\frac{1}{2}g(2k+1) \leq \frac{1}{2}g(g+1),$$

and we claim that

$$\frac{1}{2}g(g+1) \leq (g-1)^2 + 1.$$

Indeed, this holds true for $g \geq 4$, and we are done. □

4.3.2 Proof of Main Theorem (2)

To start with observe that, for $2 \leq r \leq g$, one has $M_{r,g} \leq M_{r-1,g}$. Therefore, if A is an abelian variety such that $r(A) \geq 3$, then

$$\rho(A) \leq M_{r(A),g} \leq M_{3,g} < (g-2)^2 + 4.$$

In light of this, we are left to deal with the cases $r(A) = 1, 2$.

Suppose that A is an abelian variety with $r(A) = 1$, *i.e.* $A \sim B^k$ with $\dim B = b$ and $bk = g$. If $b = 1$, then B is an elliptic curve and we have two cases according to whether B has complex multiplication. If B does have complex multiplication, then $\rho(A) = g^2$ (the top Picard number), otherwise $\rho(A) = \frac{1}{2}g(g+1) < (g-2)^2 + 4$ (as $g \geq 7$). If $b > 1$, then $k \leq g/2$ and thus, by Lemma 4.2.5,

$$\rho(B^k) \leq \frac{1}{2}g(2k+1) \leq \frac{1}{2}g(g+1) \leq (g-2)^2 + 4,$$

again because $g \geq 7$. The last standing case is when $r(A) = 2$, which we will divide into several steps.

Step 1

We deal with abelian varieties of the form $E_1^n \times E_2^{g-n}$, where E_1 and E_2 are elliptic curves, and $1 \leq n \leq g - n$. If $n = 1$, then, by Proposition 4.2.3,

$$\rho(E_1 \times E_2^{g-1}) = 1 + \rho(E_2^{g-1}),$$

which equals $M_{2,g}$ if E_2 has complex multiplication, and $1 + \frac{1}{2}g(g-1)$ otherwise. In the CM case, we obtain the second largest attainable Picard number, in the non-CM case instead one sees that it is always the case that $1 + \frac{1}{2}g(g-1) \leq (g-2)^2 + 4$. Suppose now that $n \geq 2$: we have that $\rho(E_1^n \times E_2^{g-n}) \leq n^2 + (g-n)^2$, and we want to bound the right-hand side. One has that:

$$n^2 + (g-n)^2 \leq 4 + (g-2)^2 \iff g \geq \frac{n^2 - 4}{n - 1}.$$

The function

$$f(x) := \frac{x^2 - 4}{x - 1}$$

is increasing in $[2, g-2]$, with maximum $f(g-2) = \frac{g^2 - 4g}{g-2}$. As $g \geq f(g-2)$ (here we use $g \geq 4$), this proves the right-hand side of the above equivalence, thus showing that $(g-2)^2 + 4$ bounds the Picard number in this case as well. Notice that this value is indeed attainable, and it is realized by the product $E_1^2 \times E_2^{g-2}$, with E_1 and E_2 elliptic curves with complex multiplication.

Step 2

We now consider abelian varieties of the form $E^k \times A^l$, with E an elliptic curve, $\dim A = a > 1$, $k \geq 1$, $l \geq 1$ and $g = k + al$. Notice that, by Proposition 4.2.3 and Lemma 4.2.5, one has

$$\rho(E^k \times A^l) \leq k^2 + \frac{1}{2}al(2l+1) \leq k^2 + \frac{1}{2}(g-k)(2l+1).$$

Consider the function

$$f(x,y) = x^2 + \frac{1}{2}(g-x)(2y+1),$$

in the domain $\Omega := \{(x,y) \in \mathbb{R}^2 \,|\, x \geq 1,\ y \geq 1,\ x + 2y \leq g\}$. We will prove that f is bounded from above by $(g-2)^2 + 4$ in Ω, and in turn this will show that $\rho(E^k \times A^l)$. By looking at the partials

$$\frac{\partial f}{\partial x}(x,y) = 2x - y - \frac{1}{2}, \qquad \frac{\partial f}{\partial y}(x,y) = g - x,$$

we see that f is increasing on the lines $x = \bar{x}$, for $\bar{x} \leq g$, and thus the maximum of f in Ω will lie on the line $x + 2y = g$. Therefore, we have reduced ourselves to studying the function

$$g(y) := f(g-2y, y) = (g-2y)^2 + 2y^2 + y$$

on $[1, (g-1)/2]$. It is increasing as y grows, hence its maximum is at $y_{\max} = (g-1)/2$, with value

$$g(y_{\max}) = (g-2)^2 + 3 < (g-2)^2 + 4.$$

Step 3

The last case is that of products of the form $A^k \times B^l$, with $\dim A = a > 1$, $\dim B = b > 1$, $k \geq l \geq 1$ and $g = ak + bl$. One has,

$$\begin{aligned}\rho(A^k \times B^l) &\leq \frac{1}{2}ak(2k+1) + \frac{1}{2}bl(2l+1) \\ &= \frac{1}{2}ak(2k+1) + \frac{1}{2}(g-ak)(2l+1) \\ &= ak(k-l) + gl + \frac{1}{2}.\end{aligned}$$

Let f be the function defined by

$$f(x,y,z) = xy(y-z) + gz + \frac{1}{2}g,$$

in the domain

$$\Omega := \{(x,y,z) \in \mathbb{R}^3 \,|\, x \geq 2,\ y \geq 1,\ z \geq 1,\ xy + 2z \leq g\}.$$

The partials are

$$\frac{\partial f}{\partial x}(x,y,z) = y(y-z), \quad \frac{\partial f}{\partial y}(x,y,z) = x(2y-z), \quad \frac{\partial f}{\partial z}(x,y,z) = -xy + g.$$

If we look at the lines of the form

$$L_{\bar{y},\bar{z}} :\ y - \bar{y} = z - \bar{z} = 0,$$

we see that $f|_{L_{\bar{y},\bar{z}}}(x)$ is increasing if $\bar{y} > \bar{z}$, decreasing if $\bar{y} < \bar{z}$, and constant if $\bar{y} = \bar{z}$.

Case $\bar{y} = \bar{z}$

In this case, one readily sees that $f|_{L_{\bar{y},\bar{z}}}(x) \equiv g\bar{z} + \frac{1}{2}g \leq \frac{1}{4}g^2 + \frac{1}{2}g$.

Case $\bar{y} > \bar{z}$

The maximum on the line $L_{\bar{y},\bar{z}}$ is attained for the largest values of x. As $x\bar{y} + 2\bar{z} \leq g$ and all quantities are positive, we get $x \leq \frac{g-2\bar{z}}{\bar{y}}$, and thus

$$f|_{L_{\bar{y},\bar{z}}}\Big(\frac{g-2\bar{z}}{\bar{y}}\Big) = (g-2\bar{z})(\bar{y}-\bar{z}) + g\bar{z} + \frac{1}{2}g.$$

Now, we need to maximize this quantity, *i.e.* we need to find the maximum of the function

$$h(y,z) := (g-2z)(y-z) + gz + \frac{1}{2}g,$$

in $D := \{(y,z) \,|\, 1 \leq y \leq \frac{g-2}{2},\ z \geq 1,\ y > z\}$. On the lines $z = \bar{z}$, the function h is increasing (in D), so that its maximum in D has to be looked for on the line given by $y = \frac{g-2}{2}$. Restricting h this line, we get

$$h\Big(\frac{g-2}{2}, z\Big) = 2z^2 - (g-2)z + (g^2/2 - g/2),$$

whose maximum is $\frac{1}{2}g(g-1) < (g-2)^2 + 4$.

Case $\bar{y} < \bar{z}$

The proof is analogous to the latter case. □

4.4 Some experimental data

Let us denote by R_g the set of realizable Picard numbers of g-dimensional abelian varieties. One can write down a computer program to compute all the Picard numbers of given dimension g. We briefly explain how to do this: first of all, we fix a positive integer G such that we are interested in computing R_G. In fact, the program will have to compute all R_g's, for $g \leq G$. After assigning R_1 and R_2, which we know by the discussion at the beginning of this note, for all $g \geq 3$, the program will do the following:

- compute all possible Picard numbers of simple abelian varieties of dimension g using [7, Proposition 5.5.7];
- for all k such that $0 < k < g$, use the additivity of the Picard number (Proposition 4.2.2) to compute the possible Picard numbers of products $A_k \times A_{g-k}$, where A_k (respectively, A_{g-k}) is an abelian variety of dimension k (respectively, $g-k$) and $\mathrm{End}(A_k, A_{g-k}) = 0$ (here we need the knowledge of R_h, for $h < g$);

- for all d such that $1 \leq d < g$ and $d|g$, set $k := g/d$ and use the proof of Corollary 4.2.5 to compute the possible Picard numbers of self-products A_d^k, where A_d is a simple abelian variety of dimension d.

In the following, we report the result of this computation for $g \leq 30$.

$$\begin{aligned}
R_3 &= \{1,\ldots,6,9\}\\
R_4 &= \{1,\ldots,8,10,16\}\\
R_5 &= \{1,\ldots,13,15,17,25\}\\
R_6 &= \{1,\ldots,21,26,36\}\\
R_7 &= \{1,\ldots,22,25,\ldots,29,37,49\}\\
R_8 &= \{1,\ldots,32,34,36,\ldots,40,50,64\}\\
R_9 &= \{1,\ldots,33,35,37,\ldots,42,45,50,\ldots,53,65,81\}\\
R_{10} &= \{1,\ldots,46,50,\ldots,55,58,65,\ldots,68,82,100\}\\
R_{11} &= \{1,\ldots,57,59,61,65,\ldots,70,73,82,\ldots,85,101,121\}\\
R_{12} &= \{1,\ldots,72,74,78,80,82,\ldots,87,90,101,\ldots,104,122,144\}\\
R_{13} &= \{1,\ldots,77,79,81,\ldots,89,91,97,101,\ldots,106,109,122,\ldots,125,145,169\}\\
R_{14} &= \{1,\ldots,94,96,98,100,\ldots,108,110,116,122,\ldots,127,130,145,\ldots,148,170,196\}\\
R_{15} &= \{1,\ldots,113,115,117,120,122,\ldots,129,131,137,145,\ldots,150,153,170,\ldots,173,197,\\
&\quad 225\}\\
R_{16} &= \{1,\ldots,134,136,138,145,\ldots,152,154,160,170,\ldots,175,178,197,\ldots,200,226,256\}\\
R_{17} &= \{1,\ldots,142,145,\ldots,157,159,161,169,\ldots,177,179,185,197,\ldots,202,205,226,\ldots,229,\\
&\quad 257,289\}\\
R_{18} &= \{1,\ldots,165,170,\ldots,182,184,186,194,197,\ldots,204,206,212,226,\ldots,231,234,\\
&\quad 257,\ldots,260,290,324\}\\
R_{19} &= \{1,\ldots,190,193,195,197,\ldots,209,211,213,221,226,\ldots,233,235,241,257,\ldots,262,\\
&\quad 265,290,\ldots,295,325,361\}\\
R_{20} &= \{1,\ldots,218,222,226,\ldots,238,240,242,250,257,\ldots,264,266,272,290,\ldots,295,298,\\
&\quad 325,\ldots,328,362,400\}\\
R_{21} &= \{1,\ldots,219,221,\ldots,246,251,257,\ldots,269,271,273,281,290,\ldots,297,299,305,\\
&\quad 325,\ldots,330,333,362,\ldots,365,401,441\}\\
R_{22} &= \{1,\ldots,247,250,\ldots,254,257,\ldots,277,282,290,\ldots,302,304,306,314,325,\ldots,332,\\
&\quad 334,340,362,\ldots,267,370,401,\ldots,404,442,484\}\\
R_{23} &= \{1,\ldots,278,281,\ldots,285,289,\ldots,310,315,325,\ldots,337,339,341,349,362,\ldots,369,\\
&\quad 371,377,401,\ldots,406,409,442,\ldots,445,485,529\}\\
R_{24} &= \{1,\ldots,288,290,\ldots,311,314,\ldots,318,320,325,\ldots,345,350,360,362,\ldots,376,378,\\
&\quad 386,401,\ldots,4908,410,416,442,\ldots,447,450,485,\ldots,488,530,576\}\\
R_{25} &= \{1,\ldots,321,323,325,\ldots,346,349,\ldots,353,361,\ldots,382,387,397,401,\ldots,413,415,\\
&\quad 417,425,442,\ldots,449,451,457,485,\ldots,490,493,530,531,532,533,577,625\}\\
R_{26} &= \{1,\ldots,356,358,360,\ldots,383,386,\ldots,390,398,401,\ldots,421,426,436,442,\ldots,454,\\
&\quad 456,458,466,485,486,\ldots,492,494,500,530,531,\ldots,535,538,577,\ldots,580,626,676\}\\
R_{27} &= \{1\ldots,393,395,397,\ldots,422,425,\ldots,429,437,442,\ldots,462,467,477,485,\ldots,497,\\
&\quad 499,501,509,530,\ldots,537,539,545,577,\ldots,582,585,626,\ldots,629,677,729\}\\
R_{28} &= \{1,\ldots,396,398,\ldots,432,434,436,\ldots,440,442,\ldots,470,478,485,\ldots,505,510,520,\\
&\quad 530,\ldots,542,544,546,554,577,\ldots,584,586,592,626,\ldots,631,634,677,\ldots,680,730,
\end{aligned}$$

$$\begin{aligned}
&784\} \\
R_{29} = \ &\{1\ldots, 433, 435, 437, \ldots, 473, 475, 477, \ldots, 481, 485, \ldots, 506, 509, \ldots, 513, 521, \\
&530, \ldots, 550, 555, 565, 577, \ldots, 589, 591, 593, 601, 626, \ldots, 633, 635, 641, 677, \ldots, 682, \\
&685, 730, \ldots, 733, 785, 841\} \\
R_{30} = \ &\{1\ldots, 474, 476, 478, \ldots, 483, 485, \ldots, 516, 518, 520, \ldots, 524, 530, \ldots, 551, \\
&554, \ldots, 558, 566, 577, \ldots, 597, 602, 612, 626, \ldots, 638, 640, 642, 650, 677, \ldots, 684, \\
&686, 692, 730, \ldots, 735, 738, 785, \ldots, 788, 842, 900\}
\end{aligned}$$

A few comments on these numerical data are worth making. To start with, let us notice that Part 1 of the Main Theorem is as best as it can be. More precisely, for $g = 2$ all Picard numbers occur, and for $g = 3$ we have $6 \in R_3$. Similar considerations hold for Part 2 of the Main Theorem and every $g \leq 6$.

Moreover, by looking at these data, one may guess a few more gaps in the Picard numbers of abelian varieties, for $g \gg 0$. However, the computations get out of hand very quickly, so that applying the methods that we have used for proving the Main Thereom seems inadequate. On the opposite side of the problem, one might be interested in investigating the following

Problem 4.4.1. For given g, find a positive integer $r = r(g)$ such that

$$\{1, \ldots, r\} \subset R_g.$$

At a first glance, this problem appears to be combinatorial in nature, and by combining Proposition 4.2.3 and the knownledge of R_h for $h < g$, one should be able to find such r. This problem is currently under investigation.

Bibliography

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

[2] W. Barth. Lectures on $K3$- and Enriques surfaces. In *Algebraic geometry, Sitges (Barcelona), 1983*, volume 1124 of *Lecture Notes in Math.*, pages 21–57. Springer, Berlin, 1985.

[3] W. P. Barth, K. Hulek, C. A. M. Peters, and A. Van de Ven. *Compact complex surfaces*, volume 4 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2004.

[4] A. Beauville. Variétés Kähleriennes dont la première classe de Chern est nulle. *J. Differential Geom.*, 18(4):755–782 (1984), 1983.

[5] Arnaud Beauville. Some surfaces with maximal Picard number. *J. Éc. polytech. Math.*, 1:101–116, 2014.

[6] C. Birkenhake and H. Lange. *Complex tori*, volume 177 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, 1999.

[7] C. Birkenhake and H. Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[8] 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.

[9] C. F. Gauß. Disquisitiones arithmeticae. 1801.

[10] K. Hulek and R. Laface. Non-completeness of Picard numbers for abelian varieties. In preparation.

[11] D. Huybrechts. Compact hyper-Kähler manifolds: basic results. *Invent. Math.*, 135(1):63–113, 1999.

[12] D. Huybrechts. Lectures on K3 surfaces. In press at Cambridge Studies in Advanced Mathematics, 2016.

[13] 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)*, pages 495–502. Kinokuniya Book Store, Tokyo, 1978.

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

[15] S. Koizumi. The fields of moduli for polarized abelian varieties and for curves. *Nagoya Math. J.*, 48:37–55, 1972.

[16] R. Laface. On decompositions of singular abelian surfaces. *ArXiv e-prints*, August 2015.

[17] R. Laface. The field of moduli of singular abelian and K3 surfaces. *ArXiv e-prints*, January 2016.

[18] J. L. Lagrange. *Ouvres*, volume 3 of *Gauthier-Villars*. Gauthier-Villars, Paris, 1869.

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

[20] T. Matsusaka. Polarized varieties, the fields of moduli and generalized Kummer varieties of Abelian varieties. *Proc. Japan Acad.*, 32:367–372, 1956.

[21] James S. Milne. Fields and galois theory (v4.51), 2015. Available at www.jmilne.org/math/.

[22] R. Miranda. *The basic theory of elliptic surfaces*. Dottorato di Ricerca in Matematica. [Doctorate in Mathematical Research]. ETS Editrice, Pisa, 1989.

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

[24] D. Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[25] V. K. Murty. Exceptional hodge classes on certain abelian varieties. *Mathematische Annalen*, 268(2):197–206.

[26] U. Persson. Double sextics and singular K-3 surfaces. In *Algebraic geometry, Sitges (Barcelona), 1983*, volume 1124 of *Lecture Notes in Math.*, pages 262–328. Springer, Berlin, 1985.

[27] I. I. Pjateckiĭ-Šapiro and I. R. Šafarevič. Torelli's theorem for algebraic surfaces of type K3. *Izv. Akad. Nauk SSSR Ser. Mat.*, 35:530–572, 1971.

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

[29] M. Schütt. Quintic surfaces with maximum and other Picard numbers. *J. Math. Soc. Japan*, 63(4):1187–1201, 2011.

[30] M. Schütt. Picard numbers of quintic surfaces. *Proc. Lond. Math. Soc. (3)*, 110(2):428–476, 2015.

[31] M. Schütt and T. Shioda. Elliptic surfaces. In *Algebraic geometry in East Asia—Seoul 2008*, volume 60 of *Adv. Stud. Pure Math.*, pages 51–160. Math. Soc. Japan, Tokyo, 2010.

[32] J.-P. Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[33] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[34] I. R. Shafarevich. On the arithmetic of singular $K3$-surfaces. In *Algebra and analysis (Kazan, 1994)*, pages 103–108. de Gruyter, Berlin, 1996.

[35] I. Shimada. Transcendental lattices and supersingular reduction lattices of a singular $K3$ surface. *Trans. Amer. Math. Soc.*, 361(2):909–949, 2009.

[36] G. Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

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

[38] T. Shioda and H. Inose. On singular $K3$ surfaces. In *Complex analysis and algebraic geometry*, pages 119–136. Iwanami Shoten, Tokyo, 1977.

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

[40] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[41] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[42] A. Weil. *Foundations of Algebraic Geometry*, volume 29 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, New York, 1946.

Curriculum vitae

Roberto Laface was born on June 11, 1990, in Reggio Calabria, Italy. He grew up in Reggio Calabria, where he attended the *Liceo Scientifico "Leonardo da Vinci"*. In 2005, he joined the Italian Army as a cadet of the *Scuola Militare "Teulié"* in Milan, where he served for three years. During this period, he was trained to the basics of combat, both with and without weapon. Thanks to the high-profile education provided by this institutuion, he obtained his High-school Diploma in Scientific Studies in July 2008. Since then, he is a member of *"Associazione Nazionale Ex-Allievi Teulié"*.

Immediately afterwards, despite the opportunity of continuing the military career, he enrolled at the *University of Milan* as a first-year B.Sc. student in Pure Mathematics, majoring in Algebra. Three years later, he graduated Summa cum Laude in Pure Mathematics under the supervision of Prof. Giancarlo Meloni, with a thesis on *"Some applications of Linear Logic"*, achieving the Bachelor Degree and the academic title of *"Dottore in Matematica"*.

In October 2011, he enrolled as a first-year M.Sc. student at the *University of Milan* in Pure Mathematics, majoring in Algebraic Geometry. During his first year of courses, he was a winner of a LLP ERASMUS Scholarship for the academic year 2012/2013, with destination *Universitetet i Bergen*, where he was a visiting student for a year. There, he worked under the supervision of Prof. Dr. Andreas Leopold Knutsen, and in collaboration with Prof. Antonio Lanteri (University of Milan). He graduated Summa cum Laude in Pure Mathematics in July 2013, with the thesis *"On Zariski decompositions and the orbibundle Miyaoka-Yau-Sakai inequality"*, achieving the Master Degree and the academic title of *"Dottore Magistrale in Matematica"*.

Since September 2013, he has been employed at the *Institute of Algebraic Geometry, Leibniz Universität Hannover*, as a PhD student and research assistant, under the supervision of Prof. Dr. Matthias Schütt: his research revolves around the geometry and arithmetic of K3 surfaces and related topics. Since November 2013, he is also an associate member of the *GRK 1463 "Analysis, Geometry and String Theory"*. During Spring 2016, he was a visiting scholar for two months at the *IHÉS* (Institut des Hautes Études Scientiques) as a guest of Prof. Dr. François Charles.