Distribution Agreement

Signature:

______________________________ __________

Mckenzie Rachel West Date

Brauer-Manin Computations for Surfaces

By

Mckenzie Rachel West

Doctor of Philosophy

Mathematics

David Zureick-Brown

Advisor

Ken Ono

Committee Member

Suresh Venapally

Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.

Dean of the James T. Laney School of Graduate Studies

Date

Brauer-Manin Computations for Surfaces

By

Mckenzie Rachel West

B.A., St. Olaf College, 2011

M.Sc., Emory University, 2014

Advisor: David Zureick-Brown, Ph.D.

An abstract of

A dissertation submitted to the Faculty of the

James T. Laney School of Graduate Studies of Emory University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in Mathematics

2016

Abstract

Brauer-Manin Computations for Surfaces

By Mckenzie Rachel West

The nature of rational solutions to polynomial equations is one which is fundamental to Number Theory and more generally, to Mathematics. Given the straightforward nature of this problem, one may be surprised by the difficulty when it comes to producing solutions.

The Hasse principle states that if an equation has local solutions everywhere then there is a global solution. Polynomials rarely satisfy this property. However Colliot-Thélène conjectures that another test on local solutions, the Brauer–Manin obstruction, exists for every rationally connected, smooth, projective, geometrically integral variety failing to satisfy the Hasse Principle.

We wish to explore the existence of a Brauer–Manin obstruction to the Hasse principle for certain families of surfaces. The first of which is a cubic surface written down by Birch and Swinnerton-Dyer in 1975,

$$\mathrm{Norm}_{L/K}(ax + by + \phi z + \psi w) = (cx + dy)\,\mathrm{Norm}_{K/k}(x + \theta y).$$

The left-hand side of this equality is a cubic norm and the right-hand side contains a quadratic norm. They make a correspondence between this failure and the Brauer–Manin obstruction, recently discovered by Manin, in a few specific instances. Using techniques developed in the ensuing 40 years, we show that a much wider class of norm form cubic surfaces have a Brauer–Manin obstruction to the Hasse principle, thus verifying the Colliot-Thélène conjecture for infinitely many cubic surfaces.

The second family is a general set of diagonal K3 surfaces,

$$w^2 = ax^6 + by^6 + cz^6 + dx^2y^2z^2,$$

defined as varieties in weighted projective space. This section focuses on the particular geometry of these surfaces, verifying that their Picard rank is generically 19. We conclude by computing the Galois cohomology group, $\mathrm{H}^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Pic}\,\overline{X}) \simeq (\mathbb{Z}/2\mathbb{Z})^3$. The computation of this group is fundamental to determining the existence of a Brauer–Manin obstruction.

Brauer-Manin Computations for Surfaces

By

Mckenzie Rachel West

B.A., St. Olaf College, 2011

M.Sc., Emory University, 2014

Advisor: David Zureick-Brown, Ph.D.

A dissertation submitted to the Faculty of the

James T. Laney School of Graduate Studies of Emory University

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in Mathematics

2016

Acknowledgments

First and foremost, I would like to thank my advisor, David Zureick-Brown, for his advice and support through this process. Furthermore, I would like to thank my committee members Ken Ono and Suresh as well as Parimala, an unofficial member, for their guidance.

For his help in adding to the broader context on cubic surfaces and edits to the drafts, I thank Jean-Louis Colliot-Thélène. I thank Anthony Várilly-Alvarado for proposing the Arizona Winter School project on K3 surfaces. On that note, I thank my collaborators Florian Bouyer, Edgar Costa, Dino Festi, and Christopher Nicholls for their continued work on this project.

Thanks to the Emory Algebra and Number Theory group for providing a great atmosphere in which to study. I thank the department chair, Vaidy Sunderam, and the directors of graduate studies, David Borthwick, James Lu, and Shanshuang Yang, for their guidance as well as their signatures.

I send many many thanks to Terry Ingram for all of her support and answering of frantic questions during my time at Emory. Additionally I thank Erin Nagle, the undergraduate coordinator, Edgar Leon, the IT manager, and the various staff members who have passed through the department.

Thank you to Emory University, the Emory Laney Graduate school, and the Emory Mathematics and Computer Science department for providing a quality education.

I thank the St. Olaf College Department of Mathematics, Statistics and Computer Science for setting me on the right math path. Thanks to the Delano Senior High School Mathematics Department and Math Team for showing me how cool math really is.

I thank my parents, Ric and Linda West, for their support over my many years on this earth. Thank you to Marie Jameson, who I met at my first REU, followed to Emory, and lived with in Decatur. I thank Cat Goeke, Victor and Rachel Larsen, Tim Lee, and Jim Munch for giving me refuge, supporting me, and being crazy. Thanks to my wonderful Olaf friends, UM YA YA, for their continued antics. Thanks to my awesome, crazy, cuddly dog, Pepper, and to her namesake Dr. Pepper.

Contents

Chapter 1

Introduction

A central theme in arithmetic geometry is the study of existence of rational points on an algebraic variety. In particular, we are interested in studying the conditions forcing the Hasse principle to fail, i.e., when an algebraic variety has no rational points while having points over every local field. For a general smooth projective variety, a key invariant that measures the failure of the Hasse principle is the Brauer group of the algebraic variety, denoted $\operatorname{Br} X$. In particular, given a subset $B \subset \operatorname{Br} X$ of the Brauer group, we can associate a set $X(\mathbb{A}_k)^B$ satisfying

$$X(k) \subseteq X(\mathbb{A}_k)^B \subseteq X(\mathbb{A}_k),$$

where for a given number field k, $\mathbb{A}_k$ denotes the adélec ring of k.

If $X(\mathbb{A}_k) \neq \emptyset$ and $X(\mathbb{A}_k)^{\operatorname{Br} X} = \emptyset$, we say that there is a Brauer–Manin obstruction to the Hasse principle on X. This was first noted as a generalization of quadratic reciprocity by Manin [Man71]. In general, an effective computation of the Brauer group is not practical. A more realistic approach is to gather information about the Brauer group through the Picard lattice and its Galois structure.

We will begin in Chapter 2 by introducing the definitions and methods fundamental to this research. In particular, we will define the Brauer–Manin obstruction to the Hasse principle, discuss the methods of computing the set $X(\mathbb{A}_k)^{\operatorname{Br}}$, and provide relevant results on a family of surfaces known as del Pezzo surfaces.

Chapter 3 will refine the statements of the previous chapter to ones specifically about cubic surfaces. This chapter will culminate in Theorem 3.5.3, of which the following is a direct corollary:

Theorem 1.0.1. *Take $k = \mathbb{Q}$, L/K unramified, and the ϕ_i and ψ_i to be integral units with the minimal polynomial of ψ_i/ϕ_i being separable modulo 3. Suppose p is a prime for which $p\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_2$ such that $p \| \theta\bar{\theta}$. Then the variety defined by*

$$\prod_{i=0}^{2}(x + \phi_i z + \psi_i w) = py(x + \theta y)(x + \bar{\theta} y)$$

has a Brauer-Manin obstruction to the Hasse Principle.

Lastly, Chapter 4, aims to compute the existence of a Brauer–Manin obstruction for the class of K3 surfaces,

$$X_{a,b,c,d} \colon w^2 = ax^6 + by^6 + cz^6 + dx^2y^2z^2.$$

In particular, we produce a generating set for $\operatorname{Pic} \overline{X}_{a,b,c,d}$ and moreover prove the following results:

Theorem 1.0.2. *For generic $a, b, c, d \in k^\times$, $\operatorname{Pic} \overline{X}_{a,b,c,d}$ is a lattice of rank 19 with discriminant $2^5 \cdot 3^3$.*

Moreover, generically $\mathrm{H}^1(G_k, \operatorname{Pic} \overline{X}_{1,1,1,d} \simeq (\mathbb{Z}/2\mathbb{Z})^3$. where G_k denotes the absolute Galois group of k.

Chapter 2

Background

The nature of solutions to polynomial equations is a cornerstone of mathematical study. Of particular interest are the solutions with rational coordinates. In this chapter, we will introduce the methods in which we study these points.

2.1 The Hasse principle

Suppose k is a number field and Ω_k is the set of places of k. We can extend the natural inclusion $k \hookrightarrow \mathbb{A}_k := \prod'_{v \in \Omega_k}(k_v, \mathcal{O}_v)$ to one for schemes $X(k) \to X(\mathbb{A}_k)$. In particular, if $X(\mathbb{A}_k) = \emptyset$ then $X(k) = \emptyset$. Moreover, $X(\mathbb{A}_k)$ is computable.

Proposition 2.1.1. *For X a proper k-variety, the following inclusion is an isomorphism,*

$$X(\mathbb{A}_k) \hookrightarrow \prod_{v \in \Omega_k} X(k_v).$$

Proof. See [Sko01, pp. 98–99]. □

We can see the use of this isomorphism in the following proposition that is a direct result of the Weil conjectures and Hensel's Lemma (c.f. [Har77, Appendix C]).

Proposition 2.1.2. *For X, a geometrically integral k-variety, $X(k_v)$ is non-empty for all but finitely many $v \in \Omega_v$.*

Definition 2.1.3. A class of k-varieties, $\mathcal{S}$ is said to satisfy the *Hasse principle* if for every $X \in \mathcal{S}$, $X(\mathbb{A}_k)$ non-empty implies $X(k)$ non-empty.

Thus for such varieties, determining $X(k)$ nonempty is a finite computation. Unfortunately, few varieties fail to satisfy the Hasse principle, so we must produce additional tests.

2.2 The Brauer–Manin obstruction

It is well-known that the Brauer group of a field k is isomorphic to the Galois cohomology group $\mathrm{H}^2(G_k, \overline{k}^\times)$, where $\overline{k}$ is the separable closure of k. As a generalization of $\operatorname{Br} k$, we define the Brauer group of a scheme as follows:

Definition 2.2.1. The *cohomological Brauer group* of a scheme X is

$$\operatorname{Br} X := \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m).$$

For a field L, any $x \in X(L)$ corresponds to a map $\operatorname{Spec} L \to X$ which induces a map by functoriality $\operatorname{Br} X \to \operatorname{Br} L$. Thus for each $\mathcal{A} \in \operatorname{Br} X$, we can define $\mathrm{ev}_{\mathcal{A}}(x)$ to be the image of $\mathcal{A}$ under this map.

Lemma 2.2.2. *Fix an $\mathcal{A} \in \operatorname{Br} X$, and let $(x_v) \in X(\mathbb{A}_k)$. Then for all but finitely many $v \in \Omega_k$, $\mathrm{ev}_{\mathcal{A}}(x_v)$ is trivial in $\operatorname{Br} k_v$. In particular the evaluation at all places $v \in \Omega_k$, $(\mathrm{ev}_{\mathcal{A}}(x_v))$, lies in the direct sum $\bigoplus_{v \in \Omega_k} \operatorname{Br}(k_v)$.*

Proof. Take S to be a finite set of places of k. Spread out X to to a scheme $\mathcal{X}$ on $\mathcal{O}_{k,S}$ and $\mathcal{A}$ to an algebra $\mathcal{B} \in \operatorname{Br} \mathcal{X}$. Increasing S if necessary, we can assume $x_v \in \mathcal{X}(\mathcal{O}_v)$ for all $v \notin S$. For each such x_v, $\mathrm{ev}_{\mathcal{A}}(x_v)$ comes from $\mathrm{ev}_{\mathcal{B}}(x_v)$ which lies in $\operatorname{Br} \mathcal{O}_v$. Since $\operatorname{Br} \mathcal{O}_v \cong \{0\}$, $\mathcal{A}(x_v)$ must be trivial in $\operatorname{Br} k_v$. □

Subsequently, for a fixed $\mathcal{A} \in \operatorname{Br} X$, the following diagram commutes:

$$\begin{array}{ccccccccc} & & X(k) & \hookrightarrow & X(\mathbb{A}_k) & & & & \\ & & \downarrow{\scriptstyle \mathrm{ev}_{\mathcal{A}}} & & \downarrow{\scriptstyle \mathrm{ev}_{\mathcal{A}}} & \searrow^{\phi_{\mathcal{A}}} & & & \\ 0 & \longrightarrow & \operatorname{Br} k & \longrightarrow & \bigoplus_{v\in\Omega_k} \operatorname{Br} k_v & \xrightarrow[\mathrm{inv}]{} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \end{array} \tag{2.1}$$

The bottom row of this diagram has with $\mathrm{inv} = \sum_v \mathrm{inv}_v$. Its exactness is a deep result of class field theory (c.f. [Mil13, Section VIII.4]). First noted by Manin, [Man71], as a cohomological generalization of quadratic reciprocity, the Brauer–Manin obstruction is constructed using this diagram.

Definition 2.2.3. For $\mathcal{A} \in \operatorname{Br} X$, define $X(\mathbb{A}_k)^{\mathcal{A}} := \phi_{\mathcal{A}}^{-1}(\{0\})$ a set-theoretic preimage, and

$$X(\mathbb{A}_k)^{\mathrm{Br}} := \bigcap_{\mathcal{A}\in\operatorname{Br} X} X(\mathbb{A}_k)^{\mathcal{A}}.$$

Resulting from the commutativity of (2.1), $\phi_{\mathcal{A}}(x) = 0$ for every $x \in X(k)$. Hence there is a string of inclusions

$$X(k) \subseteq X(\mathbb{A}_k)^{\mathrm{Br}} \subseteq X(\mathbb{A}_k).$$

Definition 2.2.4. We say X has a *Brauer–Manin obstruction* to the Hasse principle if $X(\mathbb{A}_k) \neq \emptyset$ while $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$.

The Brauer–Manin obstruction is thought to explain many instances in which the Hasse principle fails. It is a classical result of Hasse and Minkowski that quadrics satisfy the Hasse principle. However little is known for other classes of varieties, such as cubic and K3 surfaces. Motivated by the study of conic bundles, Colliot-Thélène and Sansuc, [CS80, Questions j_1, k_1, page 233], conjectured that smooth projective geometrically rational surfaces either satisfy the Hasse principle or have a Brauer–Manin obstruction. More recently, Colliot-Thélène has extended this conjecture to a larger family of varieties.

Conjecture 2.2.5 (Colliot-Thélène, [Col03])**.** A Brauer–Manin obstruction exists in every failure of the Hasse principle for rationally connected, smooth, projective, geometrically integral varieties.

Though it remains unproven, evidence of this generalization has been seen recently in the work of Harpaz and Wittenberg, [HW16].

2.3 Computing the Brauer group

Using the exactness of the bottom row in (2.1), $\mathrm{inv}(\mathcal{A}) = 0$ for every $\mathcal{A} \in \operatorname{Br} k$. Thus, rather than determining $\operatorname{Br} X$, we may consider elements of the quotient $\operatorname{Br} X / \operatorname{Br}_0 X$ where $\operatorname{Br}_0 X := \mathrm{im}(\operatorname{Br} k \to \operatorname{Br} X)$, which, in abuse of notation, we will often denote as $\operatorname{Br} k$. For any L Galois over k, we use the Hochschild–Serre spectral sequence,

$$\mathrm{H}^{\mathrm{p}}(G, \mathrm{H}^{\mathrm{q}}_{\text{ét}}(X_L, \mathbb{G}_m)) \Rightarrow \mathrm{H}^{\mathrm{p+q}}_{\text{ét}}(X, \mathbb{G}_m),$$

where $G = \mathrm{Gal}(L/k)$ to obtain the following exact sequence

$$\begin{aligned} 0 \to \operatorname{Pic} X \to \mathrm{H}^0(G, \operatorname{Pic} X_L) \to \mathrm{H}^2(G, L^\times) \to \ker(\operatorname{Br} X \to \operatorname{Br} X_L), \\ \to \mathrm{H}^1(G, \operatorname{Pic} X_L) \to \mathrm{H}^3(G, L^\times). \end{aligned} \tag{2.2}$$

Consider the case $L = \overline{k}$. Denote by $\operatorname{Br}_0 X$ the image of $\operatorname{Br} k$ in $\operatorname{Br} X$ and by $\operatorname{Br}_1 X$ the kernel $\ker(\operatorname{Br} X \to \operatorname{Br} \overline{X})$, often referred to as the algebraic part of the Brauer group. Since $\mathrm{H}^3(G_k, \overline{k}^\times) = 0$, c.f. [Tat10], the exact sequence 2.2 implies the following result:

Proposition 2.3.1. *If X is a smooth projective geometrically integral k-variety, then the map*

$$\frac{\operatorname{Br}_1 X}{\operatorname{Br}_0 X} \to \mathrm{H}^1(G_k, \operatorname{Pic} \overline{X}),$$

is an isomorphism.

As $\mathrm{H}^1(G_k, \operatorname{Pic} \overline{X})$ is often finite, it is convenient to consider the inclusion

$$X(\mathbb{A}_k)^{\mathrm{Br}} \subseteq \bigcap_{[\mathcal{A}] \in \mathrm{Br}_1 X / \mathrm{Br}_0 X} X(\mathbb{A}_k)^{\mathcal{A}}.$$

In the case of geometrically rational varieties, we will see later that $\mathrm{Br}_1 X = \mathrm{Br}\, X$, making the inclusion an equality.

For X a regular, integral, quasi-compact scheme, there is an injection of $\mathrm{Br}\, X$ into $\mathrm{Br}\, k(X)$, [Mil80, p. III.2.22], so elements of $\mathrm{Br}\, X$ can be realized as Azumaya algebras over the field $k(X)$.

Definition 2.3.2. Assume F_1/F_2 are fields, $\mathrm{Gal}(F_1/F_2) = \langle \sigma \rangle$ is cyclic of order n and $a \in F_2^*$, then the *cyclic algebra* $(F_1/F_2, a) \in \mathrm{Br}\, F_2$ is defined to be the quotient $F_1[T]_\sigma/(T^n - a)$. Here $F_1[T]_\sigma$ is the twisted polynomial ring, i.e. $Tb = \sigma(b)T$ for all $b \in F_1$.

In fact, cyclic $k(X)$-algebras are Azumaya algebras and thus lie in $\mathrm{Br}\, k(X)$. Moreover we can describe elements of $\mathrm{Br}\, X$ as cyclic algebras in $\mathrm{Br}\, k(X)$ using the following result (see e.g. [Cor05, Proposition 2.2.3]).

Proposition 2.3.3. *Let X be a k-variety, L/k a cyclic extension, and f an element of $k(X)$. The class of the cyclic algebra $(L/k, f) \in \mathrm{Br}\, k(X)$ is in the image of $\mathrm{Br}\, X \hookrightarrow \mathrm{Br}\, k(X)$ if and only if $(f) = \mathrm{Norm}_{L/k}(D)$ for a $D \in \mathrm{Div}(X_L)$. Moreover, if $\operatorname{Pic} X_L = (\operatorname{Pic} \overline{X})^{\mathrm{Gal}(L/k)}$ then $(L/k, f) \in \mathrm{Br}\, k$ if and only if we can take D to be principal.*

2.4 Del Pezzo surfaces

One particular family of surfaces which we will focus on are cubic surfaces. However these surfaces are just one type of the objects called del Pezzo surfaces, defined here.

Definition 2.4.1. A *del Pezzo surface* is a surface X of degree d in $\mathbb{P}^d$ with canonical sheaf $\omega_X \cong \mathcal{O}_X(-1)$.

We summarize several results about del Pezzo surfaces of [Man74] in the following theorem.

Theorem 2.4.2. *Let X be a del Pezzo surface over a number field, k, and $\overline{X} = X \times_k \overline{k}$ be the base change to the algebraic closure of k.*

1. *Del Pezzo surfaces are exactly the Fano varieties of dimension 2. A Fano variety is a smooth, projective, geometrically integral variety whose anticanonical divisor is ample.*

2. *If X has degree d, then X can be viewed as the blow up of $9-d$ generic points in $\mathbb{P}^2$, or in the case of $d = 8$, a 2-uple embedding of a quadric surface in $\mathbb{P}^3$. In the latter case $\overline{X} \simeq \mathbb{P}^1 \times \mathbb{P}^1$.*

3. *Let $x_1, \dots, x_{9-d}$ be the points as in part 2 and C be an exceptional curve on $\overline{X}$, specifically C is a curve having self intersection $(C, C) = -1$ and $C \cong \mathbb{P}^1_{\overline{k}}$. Then the image of C under the blowing-down map to $\mathbb{P}^2$ is one of the following:*

   (a) *one of the x_i,*

   (b) *a line passing through two of the x_i,*

   (c) *a conic passing through five of the x_i,*

   (d) *a cubic passing through seven of the x_i such that one of the x_i is a double point,*

   (e) *a quartic passing through eight of the x_i such that three x_i are double points,*

   (f) *a quintic passing though eight of the x_i such that six x_i are double points,*

   (g) *or a sextic passing through eight of the x_i such that seven x_i are double points and one is a triple point.*

4. *The Picard group $\operatorname{Pic}\overline{X}$ is a free abelian group of rank $10-d$ generated by ℓ, the strict transform of a line passing through none of the points $x_1, \dots, x_{9-d}$, and the exceptional curves, $e_1, \dots, e_{9-d}$, which are the strict transforms of the points $x_1, \dots, x_{9-d}$.*

Remark 2.4.3. Every del Pezzo surface is rational, that is $\overline{X}$ is birational to $\mathbb{P}^2_{\overline{k}}$ via the blowing-down map. In that case, a result of Manin [Man74, Theorem 42.8] implies that $\operatorname{Br}\overline{X} \cong \operatorname{Br}\overline{k} = \{[\overline{k}]\}$. In particular $\operatorname{Br}_1 X = \ker(\operatorname{Br} X \to \operatorname{Br}\overline{X}) = \operatorname{Br} X$.

For del Pezzo surfaces X of degree $d \geq 5$, Manin [Man74] showed that $\operatorname{Br} X/\operatorname{Br} k$ is trivial. Swinnerton-Dyer then in [Swi93] used the cohomological properties of $\mathrm{H}^1(G_k, \operatorname{Pic}\overline{X})$ to compute $\operatorname{Br} X/\operatorname{Br} k$ for $d = 3$ and 4. Completing this construction, Corn [Cor05, Theorem 1.4.1] used MAGMA to determine the possible cohomology groups for $d = 1$ and 2. Their results are summarized here.

Theorem 2.4.4. *Let X/k be a del Pezzo surface of degree d. Then $\mathrm{H}^1(G_k, \operatorname{Pic}\overline{X})$ is isomorphic to one of the following:*

$5 \leq d \leq 9$: $\{1\}$,

$d = 4$: *any of the above along with* $\mathbb{Z}/2\mathbb{Z}$ *and* $(\mathbb{Z}/2\mathbb{Z})^2$,

$d = 3$: *any of the above along with* $\mathbb{Z}/3\mathbb{Z}$ *and* $(\mathbb{Z}/3\mathbb{Z})^2$,

$d = 2$: *any of the above along with* $(\mathbb{Z}/2\mathbb{Z})^s$ $(3 \leq s \leq 6)$, $\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^t$ $(0 \leq t \leq 2)$, *and* $(\mathbb{Z}/4\mathbb{Z})^2$,

$d = 1$: *any of the above along with* $(\mathbb{Z}/2\mathbb{Z})^7$, $(\mathbb{Z}/2\mathbb{Z})^8$, $(\mathbb{Z}/3\mathbb{Z})^2$ $(3 \leq s \leq 4)$, $\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^s$ $(3 \leq s \leq 4)$, $(\mathbb{Z}/4\mathbb{Z})^2 \oplus (\mathbb{Z}/2\mathbb{Z})^t$ $(1 \leq t \leq 2)$, $\mathbb{Z}/5\mathbb{Z}$, $(\mathbb{Z}/5\mathbb{Z})^2$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, *and* $(\mathbb{Z}/6\mathbb{Z})^2$.

It is known that del Pezzo surfaces of degree $d \geq 5$ satisfy the Hasse principle. Moreover, del Pezzo surfaces over k of degree $d = 1$, 5 and 7 automatically have a k-point. These results are summarized in [Col99] and in [Sko01, Corollary 3.1.5] for the case $d = 5$. In each of the remaining cases, $d = 2$, 3 or 4, there are counterexamples to the Hasse principle, each of which is explained by a Brauer-Manin obstruction. We will explore the case of degree 3 del Pezzo surfaces in more depth in Chapter 3.

Chapter 3

Cubic Surfaces

The purpose of this chapter is to reexamine the cubic surfaces defined by Birch and Swinnteron-Dyer [BS75], updating the language and extending the results along the way. This is an important family of surfaces, as it is given by an equality of norms.

We will begin in section 3.1 by providing a history of the study of rational points on cubic surfaces and stating several relevant results on their Brauer group. Then the Birch and Swinnteron-Dyer cubics will be constructed in section 3.2.

The notation for the chapter will be fixed in section 3.3. We will explicitly describe the Brauer group for the BSD cubic surfaces in section 3.4. This computation will exploit the exceptional geometry of cubic surfaces and the previous results of Corn and Swinnerton-Dyer.

In section 3.5, there is a lemma arguing the existence of an adélic point for a family of surfaces followed by general computations of the Brauer set. Theorems 3.5.2 and 3.5.3 show that we only need to consider a specified set of primes.

Lastly, in section 3.6, we first look back at an example given in [BS75] and verify that its obstruction is given by the results of section 3.5. A second example with a Brauer–Manin obstruction given by two non-zero invariant summands is then presented.

3.1 A brief synopsis of cubic surfaces

Mordell [Mor49] conjectured that the Hasse principle holds for all projective cubic surfaces aside from cones. This conjecture was verified by Skolem [Sko55] for singular cubic surfaces and by Selmer [Sel53] for diagonal cubic surfaces

$$ax^3 + by^3 + cz^3 + dw^3 = 0,$$

for which $ab = cd$.

Later, Swinnerton-Dyer [Swi62] disproved Mordell's conjecture, providing an explicit cubic surface for which that Hasse principle failed. Cassels and Guy, [CG66], then displayed the first diagonal cubic counterexample to the Hasse Principle

$$5x^3 + 12y^3 + 9z^3 + 10w^3 = 0. \tag{3.1}$$

Around this time Manin noted the obstruction to the Hasse principle holding his name, Birch and Swinnerton-Dyer, in [BS75], considered counterexamples to the Hasse Principle for rational surfaces via very direct arguments. They comment that Manin's method should apply and provide a brief sketch to this effect. In 1987, Colliot-Thélène, Kanevsky and Sansuc [CKS87] systematically studied diagonal cubic surfaces over $\mathbb{Q}$ having integral coefficients up to 100, verifying Conjecture 2.2.5 for each one of these surfaces. They were the first to prove that the Cassels and Guy cubic (3.1) had a Brauer–Manin obstruction. Using a somewhat different method of constructing the Azumaya algebras, Corn extended the result of Colliot-Thélène, Kanevsky and Sansuc for integral coefficients up to 200 [Cor05, Theorem 3.1.1].

Now we will state some results about the geometry of cubic surfaces. With the statements about del Pezzo surfaces of degree d listed in Theorem 2, we have the following results, whose proof can be found, for example, in [Har77, p. V.4].

Corollary 3.1.1. *Cubic surfaces X in $\mathbb{P}^3_k$ are degree 3 del Pezzo surfaces,* $\operatorname{Pic}\overline{X} \cong \mathbb{Z}^7$*, generated by $\langle \ell, e_1, e_2, e_3, e_4, e_5, e_6 \rangle$. Moreover, there are exactly 27 lines on X, each having self-intersection -1, they are*

1. *the exceptional curves E_i, whose equivalence classes in* $\operatorname{Pic}\overline{X}$ *are the e_i,*

2. *the strict transform F_{ij} of the line in $\mathbb{P}^2$ containing x_i and x_j, whose equivalence classes in* $\operatorname{Pic}\overline{X}$ *are $\ell - e_i - e_j$,*

3. *and the strict transform G_j of the conic in $\mathbb{P}^2$ containing the five x_i for $i \neq j$, whose equivalence classes in* $\operatorname{Pic}\overline{X}$ *are $2\ell - \sum_{i \neq j} e_i$.*

Proposition 3.1.2. *If X is a cubic surface and $L_1, \ldots, L_6$ is any subset of six mutually skew lines chosen among the 27 lines as in corollary 3.1.1. Then there is a morphism $\pi' : X \to \mathbb{P}^2$, making X isomorphic to the blow-up of $\mathbb{P}^2$ along six points $x'_1, \ldots, x'_6$ such that $L_1, \ldots, L_6$ are the exceptional curves for π'.*

As in Theorem 2.4.4, we know that $\operatorname{Br} X / \operatorname{Br} k \xrightarrow{\sim} \mathrm{H}^1(G_k, \operatorname{Pic}\overline{X})$ is one of

$$\{0\}, \mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2, \mathbb{Z}/3\mathbb{Z} \text{ or } (\mathbb{Z}/3\mathbb{Z})^2.$$

A more explicit description of the elements of $\mathrm{H}^1(G_k, \operatorname{Pic}\overline{X})$ for X a cubic surface is given by Swinnerton-Dyer [Swi93] and describes specific subsets or partitions of $\operatorname{Pic}\overline{X}$ which correspond to the possible non-trivial elements.

Definition. A *nine* on X is a set consisting the three skew curves together with six curves intersecting exactly two of those three. A *triple-nine* is a partitioning of the 27 exceptional curves on X into three nines.

A *double-six* on X is a set of twelve exceptional curves $\{L_1, \ldots, L_6\} \cup \{M_1, \ldots, M_6\}$ on $\overline{X}$ such that

1. the L_i are pairwise skew,

2. the M_i are pairwise skew,

3. and the intersection number (L_i, M_j) is 0 if $i = j$ and 1 otherwise.

Lemma 3.1.3 (Swinnerton-Dyer [Swi93, Lemma 1], Corn [Cor05, Lemma 1.3.19]). *Non-trivial $\mathcal{A} \in \mathrm{H}^1(G_k, \operatorname{Pic} \overline{X})[2]$ correspond to G_k stable double-sixes on X with the following three properties:*

1. *neither subset of six skew exceptional curves is itself G_k stable,*
2. *no opposite pair is G_k stable,*
3. *and no set of three opposite pairs is G_k stable.*

Lemma 3.1.4 (Swinnerton-Dyer [Swi93, Lemma 6], Corn [Cor05, Lemma 1.3.22]). *Non-trivial $\mathcal{A} \in \mathrm{H}^1(G_k, \operatorname{Pic} \overline{X})[3]$ correspond to triple-nines on $\overline{X}$ such that every nine is G_k stable but no skew triple is itself G_k stable.*

Subsequently several generic results about rational points on cubic surfaces and the Hasse principle can be shown.

Lemma 3.1.5. *Let X/k be a cubic surface, and L and quadratic extension of k. If $X(L) \neq \emptyset$, then $X(k) \neq \emptyset$.*

For the proof of this lemma see e.g. [Cor05, Lemma 1.3.25].

Corollary 3.1.6. *If X is a cubic surface and $\# \mathrm{H}^1(G_k, \operatorname{Pic} \overline{X})$ is even, then X satisfies the Hasse principle.*

Proof. By Lemma 3.1.3, there is a quadratic extension L of k and a set of six skew lines which are G_L-stable. Blowing down along these six skew lines over L to obtain a del Pezzo surface of degree 9, say Y. Such surfaces are known to satisfy the Hasse principle. If $X(\mathbb{A}_k)$ is non-empty then so is $X_L(\mathbb{A}_L)$. Hence $Y(\mathbb{A}_L)$ is non-empty and $Y(L) \neq \emptyset$. By the Lang-Nishimura lemma (see [Nic55]), $X_L(L) \neq \emptyset$. The result then follows from the previous lemma. □

Remark 3.1.7. This proof is also available in [Cor05]. However it was worth repeating as this method of proof will be used later.

Using these geometric results, there is an explicit description of the $\mathcal{A} \in \operatorname{Br} X$ which give rise to Brauer–Manin obstructions to the Hasse principle for cubic surface. This result, proved by Swinnerton-Dyer [Swi99], follows a similar tone to that of Proposition 2.3.3.

Proposition 3.1.8. *If X is a del Pezzo surface of degree 3 over k, and $\mathcal{A} \in \operatorname{Br} X$ has order 3 in $\operatorname{Br} X / \operatorname{Br} k$, then there exists and extension K/k of degree 1 or 2, a cyclic cubic extension L/K, and an element $f \in k(X_K)^\times$ such that:*

1. $\operatorname{div}(f) = \operatorname{Norm}_{L/K}(D)$ *in* $\operatorname{Div} X_L$,
2. *and* $\mathcal{A} \otimes_k K = (L/K, f)$ *as elements of* $(\operatorname{Br} X_K)/\operatorname{Br} K$.

3.2 The Birch and Swinnerton-Dyer cubics

We will examine the cubic surfaces constructed by Birch and Swinnerton-Dyer:

> Let K_0/k be a non-abelian cubic extension, and L/k its algebraic closure. Suppose K/k is the unique quadratic extension which lies in L. We will assume that $(1, \phi, \psi)$ are any linearly independent generators for K_0/k, and K/k is generated by θ. Then consider the diophantine equation given by
>
> $$m \prod_{i=0}^{2} (ax + by + \phi_i z + \psi_i w) = (cx + dy)(x + \theta y)(x + \bar{\theta} y), \qquad (3.2)$$
>
> where the ϕ_i, ψ_i are the Galois conjugates of ϕ_0, ψ_0 and $\bar{\theta}$ is that of θ over k, and m, a, b, c, d are suitably chosen k-rational integers.

Birch and Swinnerton-Dyer show that as long as a, b, c, d have "certain" divisibility properties, these surfaces do not satisfy the Hasse Principle. This is done by considering a rational solution $[x, y, z, w]$ and examining the possible factorizations of the ideal $(x + \theta y)$

in O_K. They find two possible reasons the Hasse Principle may fail and give an example computation of the Brauer–Manin obstruction for each. This paper re-examines the BSD surfaces with the machinery and language of present-day Geometry and Class Field Theory.

3.3 Setup and notation

Let k be a number field with absolute Galois group G_k. Take L/k any Galois extension with $\mathrm{Gal}(L/k) \simeq S_3$. Fix K/k as the unique quadratic extension of k in L. Let O_F be the ring of integers for the field F.

Lemma 3.3.1. *Every BSD cubic* (3.2) *is isomorphic to one of the form*

$$\prod_{i=0}^{2}(x + \phi_i z + \psi_i w) = dy(x + \theta y)(x + \overline{\theta} y), \tag{3.3}$$

where $d \in O_k$, and $\{\phi_0,\ \phi_1,\ \phi_2\}$, $\{\psi_0,\ \psi_1,\ \psi_2\} \subseteq O_L$ and $\{\theta,\ \overline{\theta}\} \subseteq O_K$ are respective Galois conjugates over k with $(1, \phi_i, \psi_i)$ being a k-basis for a degree 3 extension of k.

Proof. There is an isomorphism of varieties given by

$$[x : y : z : w] \mapsto \left[ax + by : \frac{cx + dy}{(d - c\theta)(d - c\overline{\theta})} : z : w\right],$$

from the surface (3.2), to the surface

$$m(ad - bc)^2 \prod_{i=0}^{2}(x + \phi_i z + \psi_i w) = ((d - c\theta)(d - c\overline{\theta}))^2 y(x + \theta' y)(x + \overline{\theta}' y),$$

where $\theta' = (-b + a\theta)(d - c\overline{\theta})$. A subsequent isomorphism given by scaling variables results in (3.3). □

3.4 Computing the Brauer group

Since X is rational, $\ker(\operatorname{Br} X \to \operatorname{Br} \overline{X}) = \operatorname{Br} X$, [Man74, Thm. 42.8], and there is an isomorphism,

$$\operatorname{Br} X / \operatorname{Br} k \xrightarrow{\sim} \mathrm{H}^1(G_k, \operatorname{Pic} \overline{X}). \tag{3.4}$$

Moreover, $\Phi_{\mathcal{A}}$ factors through this quotient. Therefore it will be sufficient to calculate this finite group rather than determining the entire group $\operatorname{Br} X$.

Theorem 3.4.1. *Either* $\mathrm{H}^1(G_k, \operatorname{Pic} \overline{X}) \simeq \mathbb{Z}/3\mathbb{Z}$ *or* $\mathrm{H}^1(G_k, \operatorname{Pic} \overline{X})$ *is trivial.*

Proof. To prove this result, we will make use of the correspondence described in Lemma 3.1.4.

There are 9 lines, $L_{i,j}$, defined by $0 = x + \phi_i z + \psi_i w$ and

$$0 = \begin{cases} y & \text{if } j = 0, \\ x + \theta y & \text{if } j = 1, \\ x + \overline{\theta} y & \text{if } j = 2, \end{cases}$$

and 18 lines, $L_{(i,j,k),n}$ given by $z = Ax + By$ and $w = Cx + Dy$ such that A, B, C, and D satisfy the system of equations

$$\begin{cases} 1 + A\phi_i + C\psi_i \; = \; 0, \\ \theta(1 + A\phi_j + C\psi_j) = (B\phi_j + D\psi_j), \\ \overline{\theta}(1 + A\phi_k + C\psi_k) = (B\phi_k + D\psi_k), \\ (B\phi_0 + D\psi_0)(B\phi_1 + D\psi_1)(B\phi_2 + D\psi_2) = d\theta\overline{\theta}. \end{cases} \tag{3.5}$$

Let L'/k be the field of definition for the 27 lines. A triple-nine for which the individual nines are fixed by G_k is

$$\begin{pmatrix} L_{0,0} & L_{1,1} & L_{2,2} \\ L_{1,2} & L_{2,0} & L_{0,1} \\ L_{2,1} & L_{0,2} & L_{1,0} \end{pmatrix},$$
$$\begin{pmatrix} L_{(0,1,2),0} & L_{(0,1,2),1} & L_{(0,1,2),2} \\ L_{(1,2,0),0} & L_{(1,2,0),1} & L_{(1,2,0),2} \\ L_{(2,0,1),0} & L_{(2,0,1),1} & L_{(2,0,1),2} \end{pmatrix}, \quad \begin{pmatrix} L_{(0,2,1),0} & L_{(0,2,1),1} & L_{(0,2,1),2} \\ L_{(1,0,2),0} & L_{(1,0,2),1} & L_{(1,0,2),2} \\ L_{(2,1,0),0} & L_{(2,1,0),1} & L_{(2,1,0),2} \end{pmatrix}. \tag{3.6}$$

The Galois group G_k permutes the first nine, fixing no skew triple. The rows of the second two nines will be permuted via the permutation action on the roots (ϕ_0, ϕ_1, ϕ_2). The action of G_k on the columns of the second nines will determine whether or not any skew triple is fixed. If $[L' : L] = 1$ or 2, then $\mathrm{H}^1(G_k, \operatorname{Pic} \overline{X})$ is trivial as some skew triples of the later 2 nines will be fixed by G_k. Otherwise there is a non-trivial $\mathcal{A} \in \mathrm{H}^1(G_k, \operatorname{Pic} \overline{X})[3]$. The first nine in the list above must appear in every triple nine with the specified G_k action, so all possible triple nines have been found. □

Remark 3.4.2. The MAGMA code used to find the equations of (3.5) which describe the coefficients of the 18 lines can be found in Appendix B.

The map in (3.4) is generically difficult to invert. We achieve this via the following result which follows from Proposition 3.1.8 and Lemma 3.1.4.

Corollary 3.4.3. *If* $\mathrm{H}^1(G_k, \operatorname{Pic} \overline{X}) \simeq \mathbb{Z}/3\mathbb{Z}$ *then it is generated by an algebra* $\mathcal{A}$ *such that* $\mathcal{A} \otimes_k K \simeq \left(L(X)/K(X), \dfrac{x + \theta y}{y} \right)$.

Proof. Take $D = L_{0,0} + L_{1,1} + L_{1,0} - \operatorname{div}(y)$. Then

$$\begin{aligned}
\operatorname{Norm}_{L/K}(D) &= (L_{0,0} + L_{1,1} + L_{1,0})(L_{1,0} + L_{2,1} + L_{2,0}) \\
&\qquad + (L_{2,0} + L_{0,1} + L_{0,0}) - 3\operatorname{div}(y), \\
&= L_{1,1} + L_{2,1} + L_{0,1} - \operatorname{div}(y), \\
&= \operatorname{div}(x + \theta y) - \operatorname{div}(y), \\
&= \operatorname{div}\left(\frac{x + \theta y}{y}\right).
\end{aligned}$$

□

3.5 Invariant map computations

Since the $\mathcal{A} \in \operatorname{Br} X / \operatorname{Br} k$ are explicit, one may compute the map $\phi_{\mathcal{A}}$ more easily. However, before doing so, we would like to verify the existence of an adélic point.

Lemma 3.5.1. *In addition to the setup of section 3.3, assume the following are true:*

1. *L/K is unramified,*
2. *$\phi_0\phi_1\phi_2 = \psi_0\psi_1\psi_2 = \pm 1$,*
3. *the minimal polynomial for ψ_i/ϕ_i over k is separable modulo $\mathfrak{p} \mid 3\mathcal{O}_k$, and*
4. *if $\mathfrak{p} \mid d\mathcal{O}_L$ with $\mathfrak{p}\mathcal{O}_L = \mathcal{P}_1\mathcal{P}_2$ then $\mathrm{v}_1(d) \le \mathrm{v}_1(\theta)$ with $\mathrm{v}_1(\bar{\theta}) = 0$, equivalently $\mathrm{v}_2(d) \le \mathrm{v}_2(\bar{\theta})$ with $\mathrm{v}_2(\theta) = 0$, where v_i is the valuation corresponding to $\mathcal{P}_i$.*

Then $X(\mathbb{A}_k) \neq \emptyset$.

Proof. In most cases, the scheme given by $X \cap V(x)$ will be a genus 1 curve and will subsequently have a $k_{\mathfrak{p}}$ point by the Hasse bound. This will be the case whenever $\mathfrak{p} \nmid 3d\mathcal{O}_k$.

Suppose $\mathfrak{p} \mid 3\mathcal{O}_k$ and $\mathfrak{p} \nmid d\mathcal{O}_k$. Then $X \cap V(x) \to \mathbb{P}^1$ defined by $[0 : y : z : w] \mapsto [z : w]$ is one-to-one and surjective on $k_{\mathfrak{p}}$ points. Assumption 3 provides that at least one of these points is smooth.

For the primes $\mathfrak{p}$ of k dividing d, to show $X(k_\mathfrak{p}) \neq \emptyset$, it will suffice to find a $K_\mathcal{P}$ point for each prime $\mathcal{P}$ of K dividing $\mathfrak{p}$. This is a result of the fact that on cubic surfaces the existence of $k_\mathfrak{p}$-rational points is equivalent to that for quadratic extensions of $k_\mathfrak{p}$ (cf. [Cor05, Lem. 1.3.25]).

If $\mathcal{P} \mid d\mathcal{O}_K$ and $\mathcal{P}$ splits over L then $X_\mathcal{P}$ is the union of 3 lines all defined over $K_\mathcal{P}/\mathcal{P}$ and has many $K_\mathcal{P}$ points.

Lastly, suppose $\mathcal{P} \mid d\mathcal{O}_K$ and $\mathcal{P}$ remains prime in L. Then we are in the case of $\mathrm{v}_\mathcal{P}(d) \leq \mathrm{v}_\mathcal{P}(\theta)$. Then consider X' given by

$$d\prod_{i=0}^{2}(x+\phi_i z+\psi_i w) - y\left(x+\frac{\theta}{d}y\right)(dx+\overline{\theta}y),$$

which is isomorphic to X. Note that this equation has $\mathcal{O}_{\mathcal{P}_1}$ coefficients since $\mathrm{v}_1(\theta) \geq \mathrm{v}_1(d)$. Modulo $\mathcal{P}_1$, the defining equation for X' becomes

$$X_1' : \overline{\theta}_1 y^2\left(x+\left(\frac{\theta}{d}\right)_1 y\right),$$

where $\overline{\theta}_1$ and $\left(\frac{\theta}{d}\right)_1$ are the restriction of the respective constants to the quotient $\mathcal{O}_{\mathcal{P}_1}/\mathcal{P}_1$. The surface X_1' has a smooth point $[\theta_1/d : -1 : 1 : 1]$ which will lift to a $K_{\mathcal{P}_1}$ point, $[x_0 : y_0 : z_0 : w_0] \in X'(K_{\mathcal{P}_1})$. Via the isomorphism, we have $[dx_0 : y_0 : dz_0 : dw_0] \in X(K_{\mathcal{P}_1})$. □

Remark. In the case of $\mathrm{v}_1(d) > \mathrm{v}_1(\theta)$, a similar argument can be made with the additional assumption of the surjectivity of the cube map in $\mathcal{O}_{\mathcal{P}_1}/\mathcal{P}_1$.

Of course Lemma 3.5.1 is not comprehensive; there are surfaces in the class which have adélic points but do not satisfy the conditions listed above. The intention of this lemma is to provide proof that there are indeed infinitely many surfaces of this form which have an adélic point.

Remark. If $\operatorname{Br} X/\operatorname{Br} k$ is trivial, then the triple nine as in (3.6) will have enough fixed skew triples to build a set of six skew lines which is G_k-stable. We blow down X along these six skew lines to obtain a degree 9 del Pezzo surface X' defined over k. It is well-known that degree 9 del Pezzo surfaces satisfy the Hasse Principle. So by the Lang-Nishimura lemma X must also satisfy the Hasse Principle. Therefore, we will only consider surfaces X for which $\operatorname{Br} X/\operatorname{Br} k \simeq \mathbb{Z}/3\mathbb{Z}$.

There is a classical formula for inv_v provided L_v/K_v is unramified given by the local Artin map. That is, for all places v unramified in L/K,

$$\operatorname{inv}_v\left((L_v/K_v, f(P_v))_\sigma\right) = \frac{ij}{k} \mod 1,$$

where $i = \mathrm{v}_v(f(P))$, $\sigma^j = \mathrm{Frob}_{L_v/K_v}$, and $k = [L_v : K_v]$ (cf. [Ser79, p. XIV.2]).

Theorem 3.5.2. *Assume the notation of section 3.3. Suppose v is a finite place of K which is unramified in L/K such that $\mathrm{v}_v(d) = 0 \pmod 3$, and that θ or $\overline{\theta}$ has valuation 0. Then $\operatorname{inv}_v(\mathcal{A}_K(P_v)) = 0$ for all $P \in X(\mathbb{A}_K)$. Moreover, $\operatorname{inv}_\infty(\mathcal{A}_K(P_\infty)) = 0$.*

Proof. (The structure of this proof follows that of [Jah14, p. III.5.18].) In the infinite case, we must have $\operatorname{inv}_\infty(\mathcal{A}_K(P)) = 0$, as $[L : K] = 3$ and $\operatorname{inv}_\infty(\mathcal{A}_K(P_\infty)) = 0$ or $1/2$.

Suppose that v splits completely in L. Then $L_v = K_v$ and $(L_v/K_v, f(P_v))$ is trivial, so $\operatorname{inv}_v(\mathcal{A}_K(P_v)) = 0$.

If v remains prime in L then $[L_v : K_v] = 3$. Take $P_v = [x_0 : y_0 : z_0 : w_0] \in X(K_v)$. Via scaling, assume that $x_0,\ y_0,\ z_0$ and w_0 are integral and at least one has valuation 0. Since $\prod_{i=0}^{2}(x_0 + \phi_i z_0 + \psi_i w_0)$ is a norm from L to K, $y_0 = 0$ would imply $x_0 = z_0 = w_0 = 0$, which is not possible. Thus $y_0 \neq 0$. In particular, $f = \frac{x+\theta y}{y}$ is defined for all $P_v \in X(K_v)$.

For simplicity, set $\mathrm{v} = \mathrm{v}_v$ and $N = \prod_{i=0}^{2}(x + \phi_i z + \psi_i w)$. If $\mathrm{v}(N) = 0$, then $\mathrm{v}(y) = \mathrm{v}(x + \theta y) = 0$. Hence $\operatorname{inv}(\mathcal{A}_K(P_v)) = 0$. On the other hand, suppose $\mathrm{v}(N) > 0$. Since N is a norm on the residue class fields, $\mathrm{v}(x_0),\ \mathrm{v}(z_0),\ \mathrm{v}(w_0) > 0$. Hence $\mathrm{v}(y_0) = 0$. In fact, $3 \mid \mathrm{v}(N)$. Thus, $\mathrm{v}(d) + \mathrm{v}(x + \theta y) + \mathrm{v}(x + \overline{\theta} y) \equiv 0 \mod 3$. However, $\mathrm{v}(x + \theta y) = 0$ or $\mathrm{v}(x + \overline{\theta} y) = 0$, since v does not divide both θ and $\overline{\theta}$. In particular, $\mathrm{v}(x+\theta y) \equiv 0 \pmod 3$ and

$$\mathrm{inv}_v(\mathcal{A}_K(P_v)) = 0. \qquad \square$$

Remark. This result should be expected, because unramified primes of good reduction produce a trivial invariant computation.

Given the result of Theorem 3.5.2, in all cases where L/K is unramified, we simply need to consider the places of k over which d has valuation that is non-zero modulo 3. The following theorem provides a sample of the types of Brauer–Manin obstructions we may now construct for the surfaces X.

Theorem 3.5.3. *With the notation of section 3.3. Suppose L/K is unramified. Fix θ so that no primes of O_K divide both θ and $\overline{\theta}$. Let $\mathfrak{p}$ be a prime of O_k such that $\mathfrak{p}^n \mid (d)$ for some $n \not\equiv 0 \pmod 3$ which also divides $\theta\overline{\theta}$. Suppose all other primes dividing (d) split in L/K. If $X(\mathbb{A}_K) \neq \emptyset$ and $\mathfrak{p} = \mathcal{P}_1\mathcal{P}_2$ in O_K and in O_L, then $\sum_v \mathrm{inv}_v(\mathcal{A}_K(P)) \neq 0$.*

Proof. From the statement and proof of Theorem 3.5.2, we need only consider the primes $\mathcal{P}_1$ and $\mathcal{P}_2$ of O_K that lie above $\mathfrak{p}$. Via our assumption that no primes divide both θ and $\overline{\theta}$, we can assume that $\mathcal{P}_1 \mid \theta$ and $\mathcal{P}_2 \nmid \theta$. Take $\mathrm{v}_i = \mathrm{v}_{\mathcal{P}_i}$ to be the respective valuation maps. As $\mathrm{v}_i(dy(x+\theta y)(x+\overline{\theta}y)) > 0$, we must be in the case that $\mathrm{v}_i(x_0),\ \mathrm{v}_i(y_0),\ \mathrm{v}_i(z_0) > 0$ and $\mathrm{v}_i(y_0) = 0$. Then $\mathrm{v}_2(x+\theta y) = 0$, so $\mathrm{inv}_{\mathcal{P}_2}(\mathcal{A}(P)) = 0$. On the other hand $\mathrm{v}_1(x+\theta y) = \mathrm{v}_1(dy(x+\theta y)(x+\overline{\theta}y)) - \mathrm{v}_1(d) \equiv -\mathrm{v}_1(d) \mod 3$. In particular $\mathrm{inv}_{\mathcal{P}_1}(\mathcal{A}(P)) = 1/3$ or $2/3$. Thus

$$\sum \mathrm{inv}_v(\mathcal{A}(P)) = \mathrm{inv}_{\mathcal{P}_1}(\mathcal{A}(P)) \neq 0. \qquad \square$$

This theorem provides a jumping off point for similar results. One may consider the case where more places divide d, and examples of most forms can be computed immediately.

3.6 Examples

Examples that fit the situation of this Theorem 3.5.3 are easy to come by. Given any L/K unramified we can find many such θ. Then it is a quick check via Hensel's Lemma and the Weil Conjectures to show that there is an adélic point. In fact the original example of BSD fits this case.

Example. Suppose $\theta' = \frac{1}{2}(1 + \sqrt{-23})$ and ϕ_i so that $\phi_i^3 = \phi_i + 1$ and $\psi_i = \phi_i^2$. Define X_{BSD} by

$$2\prod_{i=0}^{2}(x + \phi_i z + \phi_i^2 w) = (x - y)(x + \theta' y)(x + \overline{\theta}' y).$$

Via the isomorphisms above, we have the isomorphic X given by

$$\prod_{i=0}^{2}(x + \phi_i z + \psi_i^2 w) = 32y(x + \theta y)(x + \overline{\theta} y),$$

where $\theta = -\theta' - 6$.

We find that X has adélic points but no rational points. Moreover, X has a Brauer–Manin obstruction to rational points as described in Theorem 3.5.3.

There are few published examples where the invariant map has two or more non-zero summands. Given the theorems above, examples of this can be found quickly.

Example. Suppose the ϕ_i satisfy $\phi_i^3 + \phi_i + 1 = 0$ and $\theta,\ \overline{\theta}$ are the roots of $T^2 - 4T + 35$.

Then

$$X : \prod_{i=0}^{2}(x + \phi_i z + \psi_i w) \;=\; 5^2 \cdot 7y(x + \theta y)(x + \overline{\theta} y),$$

has a Brauer–Manin obstruction to the Hasse Principle with the invariant map being

$$1/3 \;+\; 1/3 \quad \text{or} \quad 2/3 \;+\; 2/3,$$

depending on the choice of algebra $\mathcal{A}$.

Chapter 4

Diagonal K3 Surfaces

The purpose of this chapter is to provide a preliminary report on joint work with Florian Bouyer, Edgar Costa, Dino Festi and Christopher Nicholls, originating at the Arizona Winter School 2015: Arithmetic and Higher-Dimensional Varieties.

4.1 Introduction on K3 surfaces

Another interesting class of surfaces is that of K3 surfaces. Unlike del Pezzo surfaces, K3 surfaces are not rational. In particular, we no longer have the equality $\mathrm{Br}_1 X = \mathrm{Br}\, X$. Before continuing, we define these objects and give some examples.

Definition 4.1.1. An *algebraic K3 surface* is a smooth, projective 2-dimensional variety over a field k with trivial canonical sheaf and $\mathrm{H}^1(X, \mathscr{O}_X) = 0$.

We continue to fix k to be an algebraic number field, which has $\operatorname{char} k = 0$.

1. Double covers $\pi\colon X \to \mathbb{P}^2_k$ branched along a smooth sextic curve, $C \subseteq \mathbb{P}^2_k$ are degree 2 K3 surfaces.

2. Smooth quartic surfaces in $\mathbb{P}^3_k$ are K3 surfaces of degree 4.

3. Smooth complete intersections of a quadric and a cubic in $\mathbb{P}^4_k$ are K3 surfaces of degree 6.

4. Smooth complete intersections of three quadrics in $\mathbb{P}^5_k$ are degree 8 K3 surfaces.

Our work focuses on a family of diagonal degree 2 K3 surfaces. Thus we will prove that these objects as described above do satisfy $\omega_X = \mathscr{O}_X$ and $\mathrm{H}^1(X, \mathscr{O}_X)$.

Let $\pi\colon X \to \mathbb{P}^2_k$ be a double cover branched along a smooth sextic curve $C \subseteq \mathbb{P}^2_k$. Certainly X is smooth if an only if C is smooth. The Hurwitz formula, c.f. [BHPV04, p. I.17.1], implies that $\omega_X \simeq \pi^*(\omega_{\mathbb{P}^2_k} \otimes \mathscr{O}(3)) \simeq \mathscr{O}_X$. Moreover, as in [CD89, Section 0.1], since X is a double cover ramified along a sextic, we have $\pi_*\mathscr{O}_X \simeq \mathscr{O}_{\mathbb{P}^2_k} \oplus \mathscr{O}_{\mathbb{P}^2_k}(-3)$ implying $H^1(X, \mathscr{O}_X) = 0$.

Recall the isomorphism (2.3.1),

$$\frac{\mathrm{Br}_1 X}{\mathrm{Br}_0 X} \xrightarrow{\sim} \mathrm{H}^1(G_k, \operatorname{Pic} \overline{X}).$$

Our study of the Brauer–Manin obstruction will take advantage of this isomorphism, and thus require the computation of $\operatorname{Pic} \overline{X}$ and its Galois action. The geometry, or more specifically, the Hodge structure on X implies the following results about the lattice:

Proposition 4.1.2.

1. *[Huy14, Proposition 2.4] For X a K3 surface, there exist isomorphisms*

$$\operatorname{Pic} X \xrightarrow{\sim} \operatorname{NS} X \xrightarrow{\sim} \operatorname{Num} X,$$

where $\operatorname{NS} X$ *denotes the Néron–Severi group of X and* $\operatorname{Num} X$ *the numerical equivalence classes of divisors on X. Moreover, the intersection pairing $(\cdot, \cdot)$ is even, non-degenerate, and of signature* $(1, \operatorname{rk}(\operatorname{NS} X) - 1)$.

2. *[Huy14, Sections 3.2-3] For X a complex K3 surface,* $\operatorname{NS} X$ *is torsion free and* $0 \leq \operatorname{rk}(\operatorname{NS} X) \leq 20$.

Remark 4.1.3. Given this result, the lattice $(\operatorname{NS} X, (\cdot,\cdot))$ is even and non-degenerate.

Remark 4.1.4. A *complex K3 surface* is a compact complex manifold X of dimension two such that $\Omega^2_X \simeq \mathscr{O}_X$ and $\mathrm{H}^1(X, \mathscr{O}_X) = 0$. For any K3 surface over $\mathbb{C}$, the associated complex space X^{an} constructed via Serre's GAGA principle (c.f. [Ser56]) is a complex K3 surface.

Part 2 of Proposition 4.1.2 is a result of the inclusion $\operatorname{Pic} X \to \mathrm{H}^2(X, \mathbb{Z})$. For X a complex K3 surface, we have an explicit description of this cohomology group [Huy14, Proposition 3.5]:

$$\mathrm{H}^2(X, \mathbb{Z}) \simeq E_8(-1)^2 \oplus U^3,$$

where U is the hyperbolic plane and $E_8(-1)$ is a twist of the E_8 lattice.

Early computations of Brauer–Manin obstructions for K3 surfaces can be found in [Bri06], [HVV11], [Ier10], [SS05], and [Wit04]. In general, computing the Picard group of an algebraic surface is a hard problem. An effective version of the Kuga–Satake construction for degree-two K3 surfaces as in [HKT13] yields a theoretical algorithm, with a priori bounded running time, however they provide no explicit examples of these computations. In [PTL12, Section 8.6.] the authors provide an alternative algorithm. If one wishes to simply compute the rank of the Picard lattice, another approach, conditional on the Hodge conjecture for $X \times X$, is presented in [Cha11].

4.2 The particular family of surfaces

With the aim of studying the rational points on the following family of degree-two K3 surfaces

$$X_{a,b,c,d} \colon w^2 = ax^6 + by^6 + cz^6 + dx^2y^2z^2,$$

over a number field k, where $a, b, c, d \in k^\times$, we effectively compute the geometric Picard lattice for a generic element of this family and its Galois structure. Since over $\overline{k}$ the K3 surface $\overline{X}_{a,b,c,d}$ is isomorphic to $\overline{X}_{1,1,1,d'}$ for some $d' \in \overline{k}$, their geometric Picard lattices are also isomorphic. Thus, it will suffice to compute the geometric Picard lattice for a generic $X_d := X_{1,1,1,d}$ for $d \in \overline{k}$.

Theorem 4.2.1. *For a generic d, the geometric Picard lattice of* $\operatorname{Pic}\overline{X}_d$ *is a rank 19 lattice of discriminant* $2^5 \cdot 3^3$.

A possible integral basis for this lattice can be found in Appendix A. This explicit presentation of $\operatorname{Pic}\overline{X}_d$ leads us to the following theorem whose proof is a simple computation in MAGMA, see Appendix B.2.

Theorem 4.2.2. *Let $d \in \overline{k}$ be generic and X_d the corresponding K3 surface. Write $K = k(d)$. Then we have*

$$\begin{aligned} \mathrm{H}^0\left(G_K, \operatorname{Pic}\overline{X}_d\right) &\simeq \mathbb{Z}; \\ \mathrm{H}^1\left(G_K, \operatorname{Pic}\overline{X}_d\right) &\simeq (\mathbb{Z}/2\mathbb{Z})^3. \end{aligned}$$

Theorem 4.2.3. *The surface X_d is isogenous over $\mathbb{Q}(d)$ to the Kummer surface associated to the abelian surface $E \times E$, where E is a elliptic curve with j-invariant $-(4d)^3$.*

Corollary 4.2.4. *The geometric Picard number of X_d is 19 unless $-(4d)^3$ is the j-invariant of an elliptic curve with complex multiplication.*

Remark 4.2.5. Theorem 4.2.3 and Corollary 4.2.4 are direct results of Elkies' explicit formula for an isogeny between the surface $Y^2 = X^3 + dt^2X^2 + t^5(t+1)^2$ and the Kummer surface associated to $E \times E$. Elkies' construction is analogous to the Shioda–Inose construction, defined by Morrison [Mor84], but works over $k(d)$.

We prove Theorem 4.2.1 in two parts. First, we establish the rank of $\operatorname{Pic}\overline{X}_d$, which is done using bounding arguments. To find the lower bound, we construct a sublattice, Λ, in Section 4.3. This is done by constructing a set of divisors on $\overline{X}_d$ and acting on these divisors by a subset of $\mathrm{O}\left(\operatorname{Pic}\overline{X}_\eta\right)$. This subset, or more specifically the Galois group

$\mathrm{Gal}(L/K)$ where L is the field of definition for our divisors is computed in Section 4.4. In Section 4.5 we prove that the lattice Λ has rank 19. In the case of an upper bound for the rank of $\mathrm{Pic}\,\overline{X}_d$, we combine the Tate conjecture and the Artin–Tate conjecture which is done in Section 4.5.

Second, we verify that the sublattice Λ is in fact the entire $\mathrm{Pic}\,\overline{X}_d$. Given the previous results, we know that Λ is a finite index sublattice of $\mathrm{Pic}\,\overline{X}_d$. Given this fact we show, in Section 4.6, that the finite quotient $\mathrm{Pic}\,\overline{X}_d/\Lambda$ is trivial.

4.3 Geometry

The K3 surface

$$X_d\colon w^2 = x^6 + y^6 + z^6 + dx^2y^2z^2, \tag{4.1}$$

over $K\colon = k(d)$, is a double cover of $\mathbb{P}^2_K$, branched along the sextic curve

$$C_d\colon x^6 + y^6 + z^6 + dx^2y^2z^2 = 0,$$

via projection map $\pi\colon X \to \mathbb{P}^2$ defined by $\pi([w\colon x\colon y\colon z]) = [x\colon y\colon z]$.

We will pull back divisors on $\mathbb{P}^2_K$ via this map, thus producing divisors on X. Given an irreducible divisor D on $\mathbb{P}^2_K$, we can compute the pullback as follows. Firstly, write

$$\pi^{-1}(D) = \bigcup_{i=1}^{n} D_i \cup \bigcup_{j=1}^{m} E_j,$$

as a union of prime divisors on X, where the $\pi(D_i)$ are dense in D and the $\pi(E_j)$ are not. Then

$$\pi^*(D) = \sum_{i=1}^{n} e_i D_i,$$

where the e_i are the ramification indices at D_i, having the property that,

$$\sum_{i=1}^{n} e_i \deg\left(\pi|_{D_i}\right) = \deg(\pi).$$

As $\deg(\pi) = 2$, the only possible pullbacks are:

1. $\pi^*(D) = D_1 + D_2$, with $\deg\left(\pi|_{D_i}\right) = 1$;

2. $\pi^*(D) = 2D_1$, with $\deg\left(\pi|_{D_1}\right) = 1$;

3. or $\pi^*(D) = D_1$, with $\deg\left(\pi|_{D_1}\right) = 2$.

In the first case, we say that $\pi^*(D)$ is split.

Let H be a hyperplane divisor in $\mathbb{P}^2$. If D is a degree ℓ curve in $\mathbb{P}^2$, then $D \sim \ell H$, hence

$$\pi^*(D) \sim \pi^*(dH) = \ell\pi^*(H).$$

Thus, in the third case above,

$$\pi^*(D) = D_1 \sim \ell\pi^*(H),$$

so the bullback lies in the sublattice of $\operatorname{Pic} \overline{X}_d$ generated by $\pi^*(H)$. In the second case, we have

$$\pi^*(D) = 2D_1 \sim d\pi^*(H),$$

indicating that the pullback is a multiple of $\pi^*(H)$ when ℓ is even.

Motivated by these results, we search for divisors D on $\mathbb{P}^2_K$ such that the pullback, $\pi^*(D)$, splits as the sum of two divisors on X_d. This condition is satisfied by curves D on $\mathbb{P}^2_K$ that are everywhere tangent to the branch locus C_d in $\mathbb{P}^2_K$. We verify this statement here, though it is also available in [EJ08a].

Let D be a curve in $\mathbb{P}^2_K$ given by $h(x, y, z) = 0$ and $f_d(x, y, z) = x^6 + y^6 + z^6 + dx^2y^2z^2$ be the polynomial defining C_d over K. If D meets C_d with even multiplicity at each point of intersection, then the divisor $C_d|_D \in \mathscr{O}_D(6)$ is divisible by 2, thus we can write $C_d|_D = 2D'$ for some $D' \in \mathscr{O}_D(3)$. In particular, f is the square of some section $g_3 \in \mathscr{O}_D(3)$. Lifting g_3 to a section $\tilde{g}_3$ of $\mathscr{O}(3)$, we have an inclusion of affine varieties

$$V(p) \subset V\left(f - \tilde{g}_3^2\right).$$

Further,

$$\pi^{-1}(D) \subset V(h) \cup C_d,$$

making

$$\pi^{-1}(D) \subset V\left(w^2 - \tilde{g}_3^2\right).$$

Therefore, the pullback is $\pi^*(D) = D_1 + D_2$, where

$$D_i = V\left(w + (-1)^i \tilde{g}_3\right).$$

Using this result, we produce a family of divisors, Ω_d, which were found by pulling back conics everywhere tangent to C_d. Specifically, $\Omega_d = \{A_{i,j}\}_{i,j\in\{0,1,2\}} \cup \{B_1, B_2, B_3\}$ where

$$A_{i,j}: \begin{cases} 0 = x^2 + \zeta_3^i y^2 + \zeta_3^j z^2, \\ w = \beta_{i+j} xyz, \end{cases}$$

$$B_1: \begin{cases} 0 = 2xy - c_0 z^2, \\ w = x^3 - y^3; \end{cases}$$

$$B_2: \begin{cases} 0 = \frac{\sqrt{3}}{9}\left(\beta_0\beta_1 + \beta_1\beta_2 + \beta_2\beta_0 + d\right) x^2 - \frac{\sqrt{3}}{3}(y^2 + z^2) - yz, \\ w = \frac{\sqrt{3}}{27}\left((\beta_0 + \beta_1 + \beta_2)^3 - \left(\beta_0^3 + \beta_1^3 + \beta_2^3\right)\right) x^3 - (\beta_0 + \beta_1 + \beta_2)\, xyz; \end{cases}$$

$$B_3: \begin{cases} 0 = c_0 x^2 + \frac{(3c_0 - d)(3c_0 + 2d)\zeta_4}{2\beta_0\beta_1\beta_2} xy + 2y^2 - z^2 = 0, \\ w = \frac{2c_0 + c_2}{c_0 c_2}\left(c_0 x^3 + 3\frac{(3c_0 + 2d)\zeta_4}{\beta_0\beta_1\beta_2} c_0 x^2 y + 4xy^2 + 3\frac{(3c_0 + 2d)\zeta_4}{\beta_0\beta_1\beta_2} y^3\right); \end{cases}$$

where ζ_3 and ζ_4 are choices of primitive 3rd and 4th roots of unity, respectively, the β_i satisfy $\beta_i^2 = d + 3\zeta_3^i$ and the c_i are the three roots of $x^3 + dx^2 + 4$. These divisors intersect C tangentially at six points.

Remark 4.3.1. In the case of lines tritangent to C_d, a Gröbner bases shows that such lines only exist for some special values of d. In fact, a tritangent exists if and only if

$$d(5 + d)(33 + 2d)(25 - 5d + d^2)(1089 - 66d + 4d^2) = 0.$$

Remark 4.3.2. There are many other natural ways to write down divisors on X_d. For example, X_d is a double cover of the degree-one del Pezzo surface $Y_d : w = x^3 + y^3 + z^3 + dxyz$. It is well-known that $\operatorname{Pic} \overline{Y}_d$ is a rank 9 lattice, generated by the 240 exceptional curves on $\overline{Y}_d$.

The set Ω generates a proper sublattice of $\operatorname{Pic} \overline{X}_d$. Since $\operatorname{Pic} \overline{X}_d$ is stable under the action of $\mathrm{O}\left(\operatorname{Pic} \overline{X}_d\right)$, we can act by $\mathrm{O}\left(\operatorname{Pic} \overline{X}_d\right)$ on the sublattice generated by Ω. We have chosen Ω in such a way that we need not consider the full isometry group of $\operatorname{Pic} \overline{X}_d$. In particular, we restrict our attention to natural action of the automorphism group $\operatorname{Aut} X_d$ and the Galois group $\operatorname{Gal}(L/K)$ on $\operatorname{Pic} \overline{X}_d$. We compute $\operatorname{Gal}(L/K)$ in Section 4.4. For now consider the explicit subgroup of $\operatorname{Aut} X_d$, constructed as follows:

Let $\sigma \in S_3$ be a permutation of the set $\{x, y, z\}$ and consider the automorphism that σ induces on $\mathbb{P}(1, 1, 1, 3)$:

$$\begin{aligned} \varphi_\sigma \colon \mathbb{P}(1,1,1,3) &\to \mathbb{P}(1,1,1,3) \\ [x\colon y\colon z\colon w] &\mapsto [\sigma(x)\colon \sigma(y)\colon \sigma(z)\colon w]. \end{aligned}$$

Moreover, for $i, j, k \in \mathbb{Z}/6\mathbb{Z}$ we have the following automorphism of $\mathbb{P}(1, 1, 1, 3)$:

$$\begin{aligned} \psi_{i,j,k} \colon \mathbb{P}(1,1,1,3) &\to \mathbb{P}(1,1,1,3) \\ [x\colon y\colon z\colon w] &\mapsto \left[\zeta_6^i x\colon \zeta_6^j y\colon \zeta_6^k z\colon w\right]. \end{aligned}$$

Let G denote the subgroup of $\operatorname{Aut} X_d$ generated by $\{\varphi_\sigma\}_\sigma \cup \{\psi_{i,j,k}\}_I$ where $I = \{i, j, k \mid 2k + 2i + 2j \equiv 0 \bmod 6\}$.

Lemma 4.3.3. *The group G is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z} \times S_3$ and embeds into* $\operatorname{Aut} X_d$.

Proof. The second statement follows from two observations. First, φ_σ and $\psi_{i,j,k}$ map X_d to itself, as each of these automorphisms fix the defining equation of X_d. Second, the fixed point of any given non-trivial map $g \in G$, are contained in a hyperplane. In particular, such g cannot act trivially on X_d.

Let G_ψ be the subgroup of G corresponding to the $\{\psi_{i,j,k}\}_I$, and $G_\sigma \cong S_3$ be the subgroup generated by ϕ_σ. For the second claim, it suffices to show $G_\psi \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z}$, as $G_\psi \cap G_\sigma = \{\mathrm{id}\}$, and the $\psi_{i,j,k}$ commutes with the φ_σ. We give an explicit isomorphism:

$$\begin{aligned} \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\to G_\psi \\ (i, j, k) &\mapsto \psi_{i,3j,3k-i-3j}, \end{aligned}$$

Injectivity is immediate and surjectivity follows from the fact that $\psi_{i,j,k} = \psi_{i+\ell,j+\ell,k+\ell}$ as automorphisms of $\mathbb{P}(1,1,1,3)$, for all $3\ell = 0 \bmod 6$. □

With this construction, define

$$H\colon = \langle G \cup \mathrm{Gal}(L/K)\rangle \subset \mathrm{O}\left(\mathrm{Pic}\,\overline{X}_d\right) \tag{4.2}$$

and

$$\Lambda\colon = H \cdot \Omega \subset \mathrm{Pic}\,\overline{X}_\eta. \tag{4.3}$$

In other words, H is a subgroup of the group of isometries of $\mathrm{Pic}\,\overline{X}_d$ and Λ is the sublattice of $\mathrm{Pic}\,\overline{X}_d$ generated by the orbits of the divisors in Ω under the group H.

Remark 4.3.4. Note that in general for a K3 surface Y, the action of $\mathrm{Aut}\,Y$ on $\mathrm{Pic}\,\overline{Y}$ is not faithful. However, if $\mathrm{rk}\,\overline{Y} = 19$ and the discriminant of $\mathrm{Pic}\,\overline{Y}$ is not a power of 2, then the action of $\mathrm{Aut}\,X_d$ on $\mathrm{Pic}\,\overline{X}_d$ is faithful, by the global Torelli theorem.

4.4 The Galois group in the generic case

Let $K = k(d)$, then X_d is defined over K. Let L be the minimal field extension of K over which the divisors $A_{i,j}$, B_1, B_2 and B_3 are defined. In this section we will verify that for a generic d,

$$\mathrm{Gal}(L/K) \cong C_2 \times D_4 \times S_3. \tag{4.4}$$

Consider the following polynomials

$$f_1 = x^2 - (d+3)\,, \tag{4.5}$$

$$f_2 = x^4 - (2d-3)\,x^2 + \left(d^2 - 3d + 9\right), \tag{4.6}$$

$$f_3 = x^3 + dx^2 + 4, \tag{4.7}$$

$$f_4 = x^2 + 1. \tag{4.8}$$

Lemma 4.4.1. *The combined splitting field of $f_1,\ f_2,\ f_3$ and f_4 coincides with L.*

Proof. Let L' denote the combined splitting field of $f_1,\ f_2,\ f_3$ and f_4. As noted in Section 4.3, we have

$$f_1 = (x-\beta_0)(x+\beta_0);$$
$$f_2 = (x-\beta_1)(x+\beta_1)(x-\beta_2)(x+\beta_2);$$
$$f_3 = (x-c_0)(x-c_1)(x-c_2);$$
$$f_4 = (x-\zeta_4)(x+\zeta_4);$$

where ζ_3 and ζ_4 are choices of primitive 3rd and 4th roots of unity respectively, β_i satisfy $\beta_i^2 = d + 3\zeta_3^i$ and c_i are the three roots of $x^3 + dx^2 + 4$. Hence, $f_1,\ f_2,\ f_3$ and f_4 split in L and $L' \subseteq L$.

On the other hand, to show $L \subseteq L'$ it suffices to show that $\sqrt{3} \in L'$. As $\beta_1^2 = d + 3\zeta_3$, we have $\zeta_3 \in L'$ and $\sqrt{-3} \in L'$. Note that $\sqrt{-3} = (-1)\zeta_4\sqrt{3}$ and since $\zeta_4 \in L'$, $\sqrt{3} \in L'$ as well. □

In order to verify that (4.4) is an isomorphism we will begin by recalling the following well-known results about splitting fields and the corresponding Galois groups of specific polynomials.

Theorem 4.4.2 ([KW89, Theorem 3])**.** *Assume F is a field of characteristic not 2. Let $\tilde{F}$ be the splitting field of $x^4 + ax^2 + b$, an irreducible polynomial over F. Then,*

$$\operatorname{Gal}\left(\tilde{F}/F\right) \cong \begin{cases} C_2^2 & \text{if and only if } b \text{ is a square in } F, \\ C_4 & \text{if and only if } b(a^2-4b) \text{ is a square in } F, \\ D_4 & \text{if and only if } b \text{ and } b(a^2-4b) \text{ are not squares in } F. \end{cases}$$

Corollary 4.4.3. *Let F, $x^4 + bx^2 + d$, and $\tilde{F}$ be as above. Further, assume that we are in the last case, i.e., $[\tilde{F} : F] = 8$ and $\operatorname{Gal}\left(\tilde{F}/F\right) \cong D_4$. Denote the four roots of f by $\pm\alpha_1$ and*

$\pm\alpha_2$. *Then F has exactly three quadratics extensions which intermediate fields of* $\tilde{F}/F$*:*

$$F\left(\alpha_1^2\right), F\left(\alpha_1\alpha_2\right), \text{ and } F\left(\alpha_1\alpha_2\left(\alpha_1^2-\alpha_2^2\right)\right).$$

Proof. By assumption

$$\operatorname{Gal}\left(\tilde{F}/F\right) \cong D_4 = \left\langle r, s | r^2 = s^4 = 1, rs = s^3 r\right\rangle.$$

This has three subgroups of index 2, namely $\left\langle sr, s^2\right\rangle$, $\left\langle r, s^2\right\rangle$ and $\langle s\rangle$. Each of which correspond to the fields listed above. □

We now recall a well known theorem of Galois theory that classifies the splitting field of an irreducible cubic polynomial, see for example [Ste04, Section 22.2].

Theorem 4.4.4. *Let* $\tilde{F}$ *be the splitting field of* $f(x) = x^3 + ax^2 + bx + c$*, an irreducible polynomial over* F*. Then either*

1. $\Delta(f)$ *is a square in* F *and* $\operatorname{Gal}\left(\tilde{F}/F\right) \cong C_3$*,*
2. *or* $\Delta(f)$ *is not a square and* $\operatorname{Gal}\left(\tilde{F}/F\right) \cong S_3$*.*

In the latter case, $\tilde{F} \cong F\left(\alpha, \sqrt{\Delta(f)}\right)$ *where* α *is a root of* f*.*

Proposition 4.4.5. *Let* f_1, f_2 *be as in equations* (4.5) *and* (4.6)*, defined over* $K = \mathbb{Q}(d)$*. Let* $L_{1,2}$ *be their splitting field. Then, for a generic d,*

$$[L_{1,2} : K] = 2^4 \text{ and } \operatorname{Gal}\left(L_{1,2}/K\right) \cong D_4 \times C_2.$$

Proof. First consider $f_1(x) = x^2 - (d+3) = (x-\beta_0)(x+\beta_0)$ over K. For a general d, we have $d+3$ is not a square in K, so its splitting field is $K(\beta_0)$, and $[K(\beta_0) : K] = 2$.

Next we have

$$\begin{aligned} f_2(x) &= x^4 - (2d-3)x^2 + \left(d^2 - 3d + 9\right) \\ &= (x-\beta_1)(x+\beta_1)(x-\beta_2)(x+\beta_2) \end{aligned}$$

over $K(\beta_0)$. If $d^2 - 3d + 9$ is a square in $K(\beta_0)$, then for some $a, b \in K$, we have

$$\begin{aligned} d^2 - 3d + 9 &= (a + b\beta_0)^2, \\ &= a^2 + b^2(d+3) + ab\beta_0. \end{aligned}$$

This implies $ab = 0$. As we are considering a general d, we have d^2-3d+9 is not a square in K so $b \neq 0$. Further the quotient $\left(d^2 - 3d + 9\right)/(d+3)$ is generically not a square. Hence, $d^2 - 3d + 9$ is generically not a square in $K(\beta_0)$.

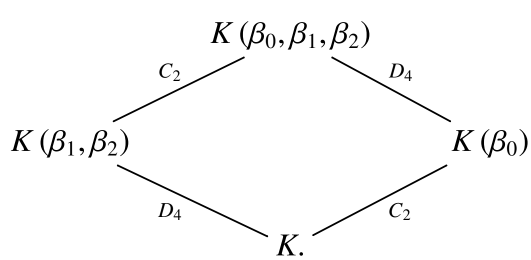
Now notice that

$$\left(d^2 - 3d + 9\right)\left((2d-3)^2 - 4\left(d^2 - 3d + 9\right)\right) = -27\left(d^2 - 3d + 9\right),$$

which is also not a square in $K(\beta_0)$. Hence, by Theorem 4.4.2, we have that the splitting field of f_2 over $K(\beta_0)$ is $K(\beta_0, \beta_1, \beta_2)$,

$$[K(\beta_0, \beta_1, \beta_2) : K(\beta_0)] = 2^3, \text{ and } \operatorname{Gal}(K(\beta_0, \beta_1, \beta_2)/K(\beta_0)) \cong D_4.$$

Subsequently, we have $\operatorname{Gal}(K(\beta_1, \beta_2) : K) \cong D_4$ and there is a diagram of fields as follows:



Therefore, $\mathrm{Gal}\left(K\left(\beta_0,\beta_1,\beta_2\right):K\right) \cong D_4 \times C_2$. □

Proposition 4.4.6. *Let f_3 be as in equation (4.7) defined over $L_{1,2} = K(\beta_0,\beta_1,\beta_2)$. Let $L_{1,2,3}$ be its splitting field over $L_{1,2}$, then*

$$[L_{1,2,3} : L_{1,2}] = 2 \cdot 3 \textit{ and } \mathrm{Gal}\left(L_{1,2,3}/L_{1,2}\right) \cong S_3.$$

Proof. We have that

$$\begin{aligned} f_3(x) &= x^3 + dx^2 + 4 \\ &= (x - c_1)(x - c_2)(x - c_3), \text{ and} \\ \Delta(f_3) &= -2^4(d+3)\left(d^2 - 3d + 9\right) = -2^4\beta_0^2\beta_1^2\beta_2^2. \end{aligned}$$

Thus, $\Delta(f_3)$ is a square in $L_{1,2}$ if and only if -1 is a square in $L_{1,2}$ or equivalently $\zeta_4 \in L_{1,2}$. Since $[K(\zeta_4) : K] = 2$, if $\zeta_4 \in L_{1,2}$, then there is an index 2 subgroup of $\mathrm{Gal}(L_{1,2}, K) \cong D_4 \times C_2$ fixing $K(\zeta_4)$. There are 7 index 2 subgroups of $D_4 \times C_2$. Corollary 4.4.3 provides us with their corresponding fixed fields, which are:

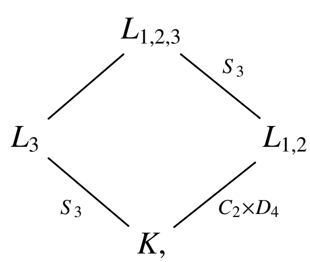
- $K\left(\beta_1^2\right)$ of discriminant (up to squares) -3,
- $K(\beta_1\beta_2)$ of discriminant $(d^2 - 3d + 9)$,
- $K\left(\beta_1\beta_2\left(\beta_1^2 - \beta_2^2\right)\right)$ of discriminant $-3\left(d^2 - 3d + 9\right)$,
- $K(\beta_0)$ of discriminant $d + 3$,
- $K\left(\beta_0\beta_1^2\right)$ of discriminant $-3(d + 3)$,
- $K(\beta_0\beta_1\beta_2)$ of discriminant $(d + 3)\left(d^2 - 3d + 9\right)$,
- and $K\left(\beta_0\beta_1\beta_2\left(\beta_1^2 - \beta_2^2\right)\right)$ of discriminant $-3(d + 3)\left(d^2 - 3d + 9\right)$.

In the case of a general d, up to squares, none of these discriminants are -1. In particular none of these fields are isomorphic to $K(\zeta_4)$. Hence -1 is not a square in $L_{1,2}$, so by Theorem 4.4.4, we have $\mathrm{Gal}(L_{1,2,3}/L_{1,2}) \cong S_3$. □

Theorem 4.4.7. *Let* f_1, f_2, f_3 *and* f_4 *be as in equations* (4.5) *through* (4.8) *over* $K := \mathbb{Q}(d)$. *Let* L_i *be the splitting field of* f_i *over* K, *and* L *the compositum of these four fields. Then,* $[L : K] = 2^5 \cdot 3$ *and*

$$\mathrm{Gal}\,(L/K) \cong \mathrm{Gal}\,(L_1/K) \times \mathrm{Gal}\,(L_2/K) \times \mathrm{Gal}\,(L_3/K) \cong C_2 \times D_4 \times S_3.$$

Proof. As f_3 has a non-square discriminant in $K\,(\beta_0, \beta_1, \beta_2) \cong L_{1,2}$, it has a non-square discriminant in $K \subset L_{1,2}$. Hence we have the following diagram



giving us that

$$\mathrm{Gal}(L_{1,2,3}/K) \cong \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K) \times \mathrm{Gal}(L_3/K) \cong C_2 \times D_4 \times S_3.$$

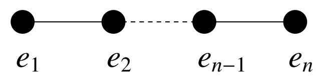
It is clear when considering the proof of Proposition 4.4.6 that $f_4 = x^2 + 1$ splits completely over over $L_{1,2,3}$ and hence $L \cong L_{1,2,3}$. □

4.5 Computations and numerical data

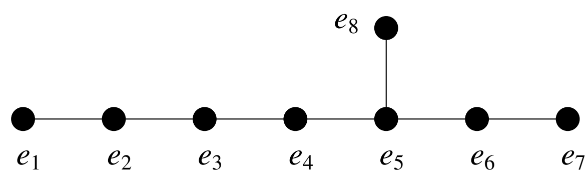
In this section we cover some of the key computations that we use in Section 4.6. We begin by recalling the following notation of Section 4.3. There is an explicit set of divisors Ω, with field of definition denoted by L/K. We also have a group $H \subset O\left(\operatorname{Pic} \overline{X}_d\right)$ that acts on $\operatorname{Pic} \overline{X}_d$, and Λ denotes the lattice generated by the H-orbits of Ω.

The proof of the following proposition will make use of the lattices A_n and E_8, whose Dynkin diagrams are shown here.

$A_n:$



$E_8:$



Define the twists $A_n(-1)$ and $E_8(-1)$ to be the lattices with basis $\{e_i\}$ corresponding to the diagrams above along with the bilinear form

$$\left\langle e_i, e_j \right\rangle := \begin{cases} -2 & i = j, \\ 1 & e_i \bullet\!\!-\!\!\!-\!\!\bullet\, e_j, \\ 0 & \text{otherwise.} \end{cases}$$

The *hyperbolic plane lattice*, U, is the unique (up to isomorphism) rank 2 even indefinite unimodular lattice. Changing base if necessary, we may assume that U has Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

Proposition 4.5.1. *For generic d, the lattice Λ is a sublattice of* $\operatorname{Pic} \overline{X}_d$*, of discriminant* $2^5 \cdot 3^3$*, signature* $(1, 18)$ *and discriminant group isomorphic* $\mathbb{Z}/6\mathbb{Z} \times (\mathbb{Z}/12\mathbb{Z})^2$*. Further,* Λ *is isometric to the lattice*

$$E_8(-1) \oplus U \oplus A_5(-1) \oplus A_2(-1) \oplus \begin{pmatrix} -8 & -4 \\ -4 & -8 \end{pmatrix}. \tag{4.9}$$

Proof. Using our explicit description of Λ it is easy to compute all the invariants mentioned above. In fact, this computation can made even simpler by deducing it over $\mathbb{F}_{79}$, a finite field whose order gives good reduction.

For the the isometry between Λ and the lattice as in (4.9), it is sufficient, by [Nik80, Corollary 1.13.3], to check that both lattices are even and indefinite, and have the same rank, discriminant, signature, number of generators for the discriminant group, and discriminant form. Each of these properties is confirmed using the sofware MAGMA [BCP97]. □

Since Λ is a rank 19 sublattice of $\operatorname{Pic} \overline{X}_d$, we immediately obtain the following result.

Corollary 4.5.2. *The geometric Picard number of X_d is at least* 19.

The remainder of this section will be focused on determining an upper bound for the geometric Picard number of X_d for a generic d. As in [Huy14], any one-dimensional family of K3 surfaces having a single member, X with geometric Picard number 19 is parametrized by a modular curve $\mathcal{X}$. Furthermore, the points of $\mathcal{X}$ with complex multiplication correspond to exactly those surfaces having geometric Picard number 20. All other K3 surfaces in the family have geometric Picard number 19.

In particular, to determine a generic upper bound, it suffices to show that there is a d such that X_d has geometric Picard number 19. To complete this task, we consider the specialization to finite fields.

Let X be a smooth projective surface over $\mathbb{F}_q$, and write

$$P_2(X,t) := \det\left(1 - t\,\mathrm{Frob}|H^2_{\acute{e}t}(\overline{X}, \mathbb{Q}_\ell)\right) \in \mathbb{Z}[t],$$

where Frob is the Frobenius automorphism. The Weil conjectures imply that $P_2(X,t)$ has reciprocal roots of absolute value q. On the other hand, the Tate Conjecture allows that the geometric Picard number of X equals the multiplicity of q as a reciprocal root of $P_2(X,t)$. The Artin–Tate conjecture relates $\mathrm{NS}\,X$, the Néron–Severi group of X, with $P_2(X,t)$:

The Tate conjecture implies the Artin–Tate conjecture when the characteristic is odd (see [Mil75a, Theorem 6.1] and [Mil75b]).

Suppose now that X is a K3 surface. In this case the Tate conjecture has been shown to hold in odd characteristic (see [Cha13; Mad15; Mau14]). Furthermore $\#\operatorname{Br} X$ is a perfect square (see, e.g. [LLR05]). As in Proposition 4.1.2 $\operatorname{Pic} X \simeq \operatorname{NS} X$, hence $\operatorname{Pic}^0 X = 0$. Lastly, via Riemann-Roch, the Euler characteristic of X is $\chi(X, \mathcal{O}_X) = 2$. Putting this together, if X is a K3 surface, then

$$\operatorname{disc} \operatorname{Pic} X_{\mathbb{F}_q} = \lim_{s \to 1} \frac{(-1)^{\rho(X)-1} P_2(X, q^{-s})}{q(1 - q^{1-s})^{\rho(X)}} \bmod \mathbb{Q}^{\times 2}. \tag{4.10}$$

Usually, one computes P_2 by counting points in sufficiently many extensions of the base field. For K3 surfaces, this requires computations in fields of size at least p^{10}. Such computations have been performed in [Lui07; EJ08a; EJ08b; EJ11a; EJ11b] for primes less than 10. This direct approach however is not computationally feasible for larger primes. For a quartic K3 surface one can compute P_2 by explicitly approximating the Frobenius action on a p-adic cohomology, namely Monsky–Washnitzer cohomology, see [AKR10; CT14]. Our approach is the one described in [EJ16], a method inspired by [Har15]. We are very thankful to Elsenhans, who computed for us P_2 for X_d over $\mathbb{F}_p$, with $4 < p < 100$. In practice, given Proposition 4.5.1, it would suffice to count points over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$. However, this project began by acquiring this upper bound, which was then followed by attempts at determining divisors in $\overline{X}_d$.

Given these results, we now show that there is a desired specialization. For example, we consider the surface X_1.

$$P_2(X_1 \bmod 5, t) = (1-5t)^8(1+5t)^8\left(1+5^2t^2\right)^2\left(1-6t+5^2t^2\right)$$
$$P_2(X_1 \bmod 11, t) = (1-11t)^{11}(11t+1)^5\left(1+11^2t^2\right)^2\left(1-6t+11^2t^2\right).$$

Therefore,

$$\operatorname{rk}\operatorname{Pic}(X_1 \bmod 5)_{\overline{\mathbb{F}}_5} = 20 \text{ and } \operatorname{disc}\operatorname{Pic}(X_1 \bmod 5)_{\overline{\mathbb{F}}_5} = 1 \bmod \mathbb{Q}^{\times 2};$$
$$\operatorname{rk}\operatorname{Pic}(X_1 \bmod 11)_{\overline{\mathbb{F}}_{11}} = 20 \text{ and } \operatorname{disc}\operatorname{Pic}(X_1 \bmod 11)_{\overline{\mathbb{F}}_{11}} = 7 \bmod \mathbb{Q}^{\times 2}.$$

From these computations, we conclude that, $\operatorname{rk}\operatorname{Pic} X_1 \leq 19$.

Remark 4.5.3. One may note that in the second set of equations here, we have that the rank of the Picard group over $\overline{\mathbb{F}}_p$ is 20. In fact, over finite fields, the Picard rank is always even. It is the addition of the discriminant computation that implies that the rank of $\operatorname{Pic}\overline{X}_d$ is 19.

We now conclude with the desired result.

Proposition 4.5.4. *For generic d the Picard number of X_d is 19. Further, the lattice Λ is a finite index sublattice of* $\operatorname{Pic} X_d$.

4.6 The Picard group lattice

In this section we complete the proof of Theorem 4.2.1. That is, we wish to show not only is Λ a finite index sublattice of $\operatorname{Pic}\overline{X}_d$, but it is in fact equal to the entire lattice, i.e. $\Lambda = \operatorname{Pic}\overline{X}_d$.

From Propositions 4.5.1 and 4.5.4 we know that Λ are both rank 19 lattices. It follows that $\operatorname{Pic}(\overline{X}_d)/\Lambda$ is a finite abelian group of order $[\operatorname{Pic}(\overline{X}_d) \colon \Lambda]$.

For any inclusion of lattices $L' \subseteq L$, the corresponding discriminants are related by the equation $\operatorname{disc}(L') = [L \colon L']^2 \cdot \operatorname{disc}(L)$. Since $\operatorname{disc}(\Lambda) = 2^5 \cdot 3^3$, we know that $[\operatorname{Pic}(X) \colon \Lambda]^2 \mid 2^5 \cdot 3^3$. In particular, $[\operatorname{Pic}(X) \colon \Lambda] \mid 2^2 \cdot 3$.

Therefore, we can verify that $\operatorname{Pic}(X)/\Lambda$ is trivial by showing that there are no possible elements of order dividing 2 or 3 in $\operatorname{Pic}(X)/\Lambda$.

To begin, consider the bijection,

$$\{D \in \operatorname{Pic}(\overline{X}_d) \colon \; pD \in \Lambda\} \leftrightarrow \Lambda \cap p \operatorname{Pic}(\overline{X}_d),$$

$$D \mapsto pD$$

Note that the left hand side consists of elements of $\operatorname{Pic}(\overline{X}_d)$ whose order in $\operatorname{Pic}(\overline{X}_d)/\Lambda$ divides p. Denote the image in $\Lambda/p\Lambda$ of $\Lambda \cap p \operatorname{Pic}(\overline{X}_d)$ by Λ_p.

Lemma 4.6.1. *This image, Λ_p, is the kernel of the natural map*

$$\Lambda/p\Lambda \to \operatorname{Pic} \overline{X}_d / p \operatorname{Pic} \overline{X}_d,$$

$$D + p\Lambda \mapsto D + p \operatorname{Pic} \overline{X}_d.$$

Moreover, Λ_p is a H-invariant subspace of $\Lambda/p\Lambda$, where H is as in (4.2).

Proof. By definition, elements of Λ_p are those $D + p\Lambda \in \Lambda/p\Lambda$ such that $D \in p \operatorname{Pic} \overline{X}_d$. Hence Λ_p is the kernel of the map described. Moreover, kernels of homomorphisms of vector spaces must are automatically invariant under vector space automorphisms. □

Thus we can rewrite the problem $\operatorname{Pic} \overline{X}_d/\Lambda = 0$ as $\Lambda_p = 0$ for all primes p. Since $\operatorname{Pic} \overline{X}_d/\Lambda$ has order dividing 12, $\Lambda_p = 0$ for all primes $p \neq 2$ or 3.

To show that Λ_2 and Λ_3 are zero, we construct a computable subspace of $\Lambda/p\Lambda$ which contains Λ_p. Consider the natural map

$$\Lambda/p\Lambda \to \operatorname{Hom}(\Lambda, \mathbb{Z}/p\mathbb{Z}),$$

$$D + p\Lambda \mapsto (D' \mapsto (D, D') \pmod{p}),$$

where $(\cdot, \cdot)$ is the intersection pairing. Define M_p to be the kernel of this map.

Lemma 4.6.2. *The kernel, M_p, is a H-invariant subspace of $\Lambda/p\Lambda$ containing Λ_p.*

The proof of this result is straightforward and similar to that of Lemma 4.6.1 and is thus omitted.

Remark 4.6.3. In general, the intersection pairing (D, D') for $D, D' \in \Lambda/p\Lambda$ is defined modulo p, since if $C = D + p\lambda$ and $C' = D' + p\mu$, then $(C, C') = (D, D') + p(D, \mu) + p(\lambda, D') + p^2(\lambda, \mu) \equiv (D, D') \pmod{p}$.

However, for $D,\ D' \in M_p$, $(D, D') \equiv 0 \pmod{p}$ and $(D', D') \equiv 0 \pmod{2}$, so self-intersection is defined modulo $2p^2$ on M_p.

By the bijection in (4.6), elements of Λ_p are in one-to-one correspondence with elements of $\mathrm{Pic}(\overline{X}_d)/\Lambda$ of order dividing p. Since $[\mathrm{Pic}(\overline{X}_d) \colon \Lambda]$ divides 12, Λ_2 has dimension at most 2 and Λ_3 has dimension at most 1 as subspaces of $\Lambda/p\Lambda$.

Remark 4.6.4. Note that we call a divisor E on X *effective* if E is linearly equivalent to an effective divisor. For a divisor E, this is equivalent to the existence of a global section of $\mathscr{O}_X(E)$. This is a result of the fact each such global section is a function $f \in \Gamma(X, \mathscr{O}_X)$ such that $\mathrm{div}(f) + E \geq 0$, giving the equivalence of E to an effective divisor.

Lemma 4.6.5. *If D is a divisor on a K3 surface X such that $D^2 = -2$, then one of D or $-D$ is effective.*

Proof. We use Riemann–Roch, which states

$$\chi(X, \mathscr{O}_X(D)) = \frac{1}{2} D \cdot (D - K_X) + \chi(X, \mathscr{O}_X),$$

where $\chi(X, \mathscr{O}_X)$ denotes the Euler characteristic. Recall that X a K3 surface, we have $\chi(X, \mathscr{O}_X) = 2$, and the canonical bundle K_X is trivial. Thus $\frac{1}{2} D \cdot (D - K_X) = \frac{1}{2} D^2 = -1$. Expanding the left hand side, we see that

$$h^0(X, \mathscr{O}_X(D)) - h^1(X, \mathscr{O}_X(D)) + h^2(X, \mathscr{O}_X(D)) = 1.$$

By Serre duality, $h^2(X, \mathscr{O}_X(D)) = h^0(X, K_X \otimes \mathscr{O}_X(D)^\vee) = h^0(X, \mathscr{O}_X(-D))$, and so we arrive at the formula,

$$h^0(X, \mathscr{O}_X(D)) + h^0(X, \mathscr{O}_X(-D)) = 1 + h^1(X, \mathscr{O}_X(D)) \geq 1.$$

Thus one of $h^0(X, \mathscr{O}_X(D))$ and $h^0(X, \mathscr{O}_X(-D))$ is positive, which is equivalent to D or $-D$ being effective. □

Proof ($\operatorname{Pic} \overline{X}_d = \Lambda$*).* The general strategy is to compute M_p for $p = 2, 3$ and consider the possible H-invariant subspaces of M_p. If a divisor is contained in Λ_p, then its entire H-orbit is as well. Thus for each $v \in M_p$ we compute the H-invariant subspace it generates. The MAGMA code verifying these computations is available in Appendix B.2.1, or more specifically in `verifyfulllattice.m`.

We first consider the case $p = 3$. As before, the dimension of Λ_3 as a subspace of $\Lambda/3\Lambda$ is at most 1. The kernel, M_3 has dimension 3, and there are 2 possible nonzero vectors in $\Lambda/3\Lambda$ which generate H-invariant subspaces of dimension 1. For each of these we want to show they are not 3-divisible in $\operatorname{Pic} \overline{X}_d$. The self intersections are -84 and -66, respectively. If $C \in \Lambda$ with $C = 3C'$ in $\operatorname{Pic} \overline{X}_d$, then $C^2 = 9C'^2$, and since 9 does not divide their self intersections, these are not 3-divisible in $\operatorname{Pic}(X_D)$. Hence $\Lambda_3 = 0$.

Next consider the case $p = 2$. In the same way, we arrive at 4 possible nonzero vectors generating H-invariant subspaces of $\Lambda/2\Lambda$ having dimension at most 2. One of these can be eliminated since the self intersection is not divisible by 4. Each of the remaining 3 subspaces generates the same 2-dimensional H-invariant subspace, so it suffices to eliminate any one of them as being 2-divisible in $\operatorname{Pic} \overline{X}_d$.

Let $\mathcal{L}$ denote the element of $\Lambda/2\Lambda$ with $\mathcal{L}^2 = -8$, and let C be a lift of $\mathcal{L}$ to Λ with $C^2 = -8$. Suppose that $C = 2C'$ with $C' \in \operatorname{Pic} \overline{X}_d$. Then $C'^2 = -2$, so one of C' or $-C'$ is effective by Lemma 4.6.5. By replacing C with $-C$ if necessary, we may assume that C' is effective. Thus, for an ample divisor E, we have $(C', E) > 0$. In particular, let H denote the hyperplane class in $\operatorname{Pic} \overline{X}_d$, which is ample, then $(C', H) > 0$ and $(C, H) = 2(C', H) > 0$.

However, by a computation we find two curves D_1, D_2 such that $D_1 - D_2$ is numerically equivalent to C. Moreover, $D_1^2 = D_2^2 = -2$ and $(D_1, D_2) = 2$. Thus

$$(H, C) = (H, D_1) - (H, D_2) = 2 - 2 = 0,$$

which contradicts the fact that $(C, H) > 0$. Hence C is not 2-divisible in $\mathrm{Pic}(X)$, so $\Lambda_2 = 0$. Therefore Λ is in fact the full lattice, $\mathrm{Pic}\,\overline{X}_d$. □

Appendix A

A Generating Set

The following list of 19 divisors form a generating set for the lattice Pic $\overline{X}_d$, as in Chapter 4.

$$A_{1,1,+}: \begin{cases} x^2 + \zeta_3 y^2 + \zeta_3 z^2 &= 0 \\ w + \beta_2 xyz &= 0 \end{cases} \qquad A_{0,0,+}: \begin{cases} x^2 + y^2 + z^2 &= 0 \\ w + \beta_0 xyz &= 0 \end{cases}$$

$$A_{2,1,-}: \begin{cases} x^2 + \zeta_3^2 y^2 + \zeta_3 z^2 &= 0 \\ w - \beta_0 xyz &= 0 \end{cases} \qquad A_{1,2,-}: \begin{cases} x^2 + \zeta_3 y^2 + \zeta_3^2 z^2 &= 0 \\ w - \beta_0 xyz &= 0 \end{cases}$$

$$A_{2,2,-}: \begin{cases} x^2 + \zeta_3^2 y^2 + \zeta_3^2 z^2 &= 0 \\ w - \beta_1 xyz &= 0 \end{cases} \qquad A_{1,0,+}: \begin{cases} x^2 + \zeta_3 y^2 + z^2 &= 0 \\ w + \beta_1 xyz &= 0 \end{cases}$$

$$A_{2,0,-}: \begin{cases} x^2 + \zeta_3^2 y^2 + z^2 &= 0 \\ w - \beta_2 xyz &= 0 \end{cases} \qquad B_8: \begin{cases} 2xy + c_1 z^2 &= 0 \\ x^3 + y^3 - w &= 0 \end{cases}$$

$$B_9: \begin{cases} 2yz - c_0 x^2 &= 0 \\ y^3 - z^3 + w &= 0 \end{cases} \qquad B_{10}: \begin{cases} 2yz + c_0 x^2 &= 0 \\ y^3 + z^3 - w &= 0 \end{cases}$$

$$B_{11}: \begin{cases} 2x^2 - 2\frac{(3c_0+2d)(3c_0-d)}{(c_0-c_1)(c_1-c_2)(c_2-c_0)}xy + c_0y^2 - z^2 & = 0 \\ (2c_0 + c_1)\left(c_0y^3 - \frac{(9c_0+6d)\zeta_4}{\beta_0\beta_1\beta_2}c_0y^2x + 4yx^2 - \frac{(9c_0+6d)\zeta_4}{\beta_0\beta_1\beta_2}x^3\right) - c_0c_1w & = 0 \end{cases}$$

$$B_{12}: \begin{cases} c_0z^2 - 2\frac{(3c_0+2d)(3c_0-d)}{(c_0-c_1)(c_1-c_2)(c_2-c_0)}zy + 2y^2 - x^2 & = 0 \\ (2c_0 + c_1)\left(c_0z^3 - \frac{(9c_0+6d)\zeta_4}{\beta_0\beta_1\beta_2}c_0z^2y + 4zy^2 - \frac{(9c_0+6d)\zeta_4}{\beta_0\beta_1\beta_2}y^3\right) - c_0c_1w & = 0 \end{cases}$$

$$B_{13}: \begin{cases} c_2x^2 - 2\frac{(3c_2+2d)(3c_2-d)}{(c_0-c_1)(c_1-c_2)(c_2-c_0)}xz + 2z^2 - y^2 & = 0 \\ (2c_2 + c_0)\left(c_2x^3 - \frac{(9c_0+6d)\zeta_4}{\beta_0\beta_1\beta_2}c_2x^2z + 4xz^2 - \frac{(9c_0+6d)\zeta_4}{\beta_0\beta_1\beta_2}z^3\right) - c_0c_2w & = 0 \end{cases}$$

$$B_{14}: \begin{cases} \frac{\sqrt{3}}{9}(\beta_0\beta_1 + \beta_1\beta_2 + \beta_2\beta_0 + d)\zeta_3^2x^2 - \frac{\sqrt{3}}{3}(y^2 + \zeta_3z^2) + \zeta_3^2yz & = 0 \\ \frac{\sqrt{3}}{27}\left((\beta_0 + \beta_1 + \beta_2)^3 - (\beta_0^3 + \beta_1^3 + \beta_2^3)\right)x^3 + (\beta_0 + \beta_1 + \beta_2)xyz - w & = 0 \end{cases}$$

$$B_{15}: \begin{cases} \frac{\sqrt{3}}{9}(-\beta_0\beta_1 - \beta_1\beta_2 + \beta_2\beta_0 + d)y^2 - \frac{\sqrt{3}}{3}(\zeta 3^2x^2 + \zeta_3z^2) - xz & = 0 \\ \frac{\sqrt{3}}{27}\left((\beta_0 - \beta_1 + \beta_2)^3 - (\beta_0^3 - \beta_1^3 + \beta_2^3)\right)y^3 - (\beta_0 - \beta_1 + \beta_2)xyz + w & = 0 \end{cases}$$

$$B_{16}: \begin{cases} \frac{\sqrt{3}}{9}(-\beta_0\beta_1 + \beta_1\beta_2 - \beta_2\beta_0 + d)y^2 - \frac{\sqrt{3}}{3}(x^2 + z^2) + xz & = 0 \\ -\frac{\sqrt{3}}{27}\left((-\beta_0 + \beta_1 + \beta_2)^3 - (-\beta_0^3 + \beta_1^3 + \beta_2^3)\right)y^3 + (\beta_0 - \beta_1 - \beta_2)xyz - w & = 0 \end{cases}$$

$$B_{17}: \begin{cases} \frac{\sqrt{3}}{9}(-\beta_0\beta_1 + \beta_1\beta_2 - \beta_2\beta_0 + d)\zeta_3y^2 - \frac{\sqrt{3}}{3}(\zeta_3^2x^2 + z^2) - \zeta_3xz & = 0 \\ \frac{\sqrt{3}}{27}\left((-\beta_0 + \beta_1 + \beta_2)^3 - (-\beta_0^3 + \beta_1^3 + \beta_2^3)\right)y^3 + (\beta_0 - \beta_1 - \beta_2)xyz - w & = 0 \end{cases}$$

$$B_{18}: \begin{cases} \frac{\sqrt{3}}{9}(-\beta_0\beta_1 + \beta_1\beta_2 - \beta_2\beta_0 + d)\zeta_3^2x^2 - \frac{\sqrt{3}}{3}(\zeta_3y^2 + z^2) + \zeta_3^2yz & = 0 \\ \frac{\sqrt{3}}{27}\left((-\beta_0 + \beta_1 + \beta_2)^3 - (-\beta_0^3 + \beta_1^3 + \beta_2^3)\right)x^3 - (\beta_0 - \beta_1 - \beta_2)xyz - w & = 0 \end{cases}$$

$$B_{19}: \begin{cases} \frac{\sqrt{3}}{9}(\beta_0\beta_1 + \beta_1\beta_2 + \beta_2\beta_0 + d)\zeta_3y^2 - \frac{\sqrt{3}}{3}(x^2 + \zeta_3^2z^2) - \zeta_3xz & = 0 \\ \frac{\sqrt{3}}{27}\left((\beta_0 + \beta_1 + \beta_2)^3 - (\beta_0^3 + \beta_1^3 + \beta_2^3)\right)x^3 - (\beta_0 + \beta_1 + \beta_2)xyz - w & = 0 \end{cases}$$

Appendix B

MAGMA Code

B.1 Birch and Swinnerton-Dyer cubic surfaces

The following MAGMA code is used to find the 18 lines on the simplified Birch and Swinnerton-Dyer cubic surfaces, (3.3), of the form $z = Ax + By$ and $w = Cx + Dy$ as described in (3.5).

B.1.1 MAGMA code

```
//Label the constants as coefficients
L<phi0,phi1,phi2,psi0,psi1,psi2,theta,thetabar,d> :=\
  PolynomialRing(Rationals(),9);
//We search for lines of the form z=Ax+By, w=Cx+Dy
R<A,B,C,D> := PolynomialRing(L,4);
AmbSpace<x,y,z,w> := PolynomialRing(R,4);
//The surface X is given by cubic here
cubic := d*y*(x+theta*y)*(x+thetabar*y)\
  -(x+phi0*z+psi0*w)*(x+phi1*z+psi1*w)*(x+phi2*z+psi2*w);
//Parametrize the lines over P1 as [s:t] -> [s,t,A*s+B*t,C*s+D*t]
```

```
ParamSpace<s,t> := PolynomialRing(R,2);
withLines := Evaluate(cubic,[s,t,A*s+B*t,C*s+D*t]);

//Then the first three equations for the lines are given by direct
//  factorizaiton of the resulting equation evaluated at [1,0],
//  [theta,-1], and  [thetabar,-1]. The final equation which is
//  cubic, can be determined by subtracting  d*theta*thetabar
//  from the point given by [s,t]=[0,1].
Factorization(Evaluate(withLines,[1,0]));
Factorization(Evaluate(withLines,[theta,-1]));
Factorization(Evaluate(withLines,[thetabar,-1]));
Factorization(Evaluate(withLines,[0,1])-d*theta*thetabar);
```

B.1.2 Output

```
[
  <phi2*A + psi2*C + 1, 1>,
  <phi1*A + psi1*C + 1, 1>,
  <phi0*A + psi0*C + 1, 1>
]
[
  <phi2*theta*A - phi2*B + psi2*theta*C - psi2*D + theta, 1>,
  <phi1*theta*A - phi1*B + psi1*theta*C - psi1*D + theta, 1>,
  <phi0*theta*A - phi0*B + psi0*theta*C - psi0*D + theta, 1>
]
[
  <phi2*thetabar*A-phi2*B+psi2*thetabar*C-psi2*D+thetabar, 1>,
  <phi1*thetabar*A-phi1*B+psi1*thetabar*C-psi1*D+thetabar, 1>,
```

```
  <phi0*thetabar*A-phi0*B+psi0*thetabar*C-psi0*D+thetabar, 1>
]
[
  <phi2*B + psi2*D, 1>,
  <phi1*B + psi1*D, 1>,
  <phi0*B + psi0*D, 1>
]
```

B.2 K3 surface computations

The following MAGMA code is used to verify the results discussed in Chapter 4.

B.2.1 MAGMA code

main.m

```
 load "basicdefinitions.m";

// These divisors will be used to generate the entire Picard group,
// by considering their orbits under a subgroup G of the
// automorphism group, as well as under the Galois group of K2.
// They are, in order, Aij, B1, B2, B3.
InitialDivisors := [
[x^2 + y^2 + z^2,w-b0*x*y*z],
[x^2 + y^2 + zeta3*z^2, w-b1*x*y*z],
[x^2 + zeta3*y^2 + zeta3^2*z^2, w-b0*x*y*z],
[x^2-d/3*y^2+z^2,3*r3*w+b0*b1*b2*y^3],
[2*x*y-c0*z^2,x^3-y^3-w],
[r3/9*(b0*b1+b1*b2+b2*b0+d)*x^2-r3/3*(y^2+z^2)-y*z,
       r3/27*((b0+b1+b2)^3-(b0^3+b1^3+b2^3))*x^3\
```

```
        -(b0+b1+b2)*x*y*z-w], [c0*x^2\
        +2*((3*c0+2*d)*(3*c0-d))/((c0-c1)*(c1-c2)*(c2-c0))*x*y\
        +2*y^2-z^2, (2*c0+c2)*(c0*x^3\
        +(9*c0+6*d)*4*c0/((c0-c1)*(c1-c2)*(c2-c0))*x^2*y+\
        4*x*y^2+(9*c0+6*d)*4/((c0-c1)*(c1-c2)*(c2-c0))*y^3)-c0*c2*w]
];

// This file contains functions to compute orbits under groups.
load "computeggalorbits.m";
print "Computing G orbits of initial divisors";
GOrbitDivs := computeOrbitsOfDivisors(G, InitialDivisors);
print "There are", #GOrbitDivs, "G orbits of the initial divisors";


print "Computing GGalTOrbitDivs";
GGalTOrbitDivs := computeOrbitsOfDivisors(GalT, GOrbitDivs);
#GGalTOrbitDivs;
load "computegrammatrices.m";
ListDivsp := computeSchemesModP(GGalTOrbitDivs);
print "Computing Gram matrix for the", #ListDivsp, "divisors";
A0:=GramMatrixD(ListDivsp,dp,F);
Gram0 := computeGramOfBasis(A0);
print "The Gram matrix has determinant",\
Factorisation(Determinant(Gram0));
load "comparelatticestructure.m";
print "We compare the lattice we have with the lattice we expect";
compareLattices(Gram0);
```

```
load "computegaloismatrices.m";

MgenGGal := computeGaloisRepresentations(SetDivsGGal,\
 genG cat genGalT);
M19genGGal := reduceto19(MgenGGal, A0);


// Now we check that the lattice L we have is equal
// to the Picard lattice.

load "verifyfulllattice.m";

// Finally, compute the galois action.

load "computegaloisactionH1.m";
```

basicdefinitions.m

```
// In this file we compute the Picard lattice
// of the surface X_d : w^2=x^6+y^6+z^6+dx^2y^2z^2
// defined over Q(d).


// We define the field of definition of Pic(X_d), denoted by K2,
// together with the weighted projective space and
// the surface itself


preK<zeta12>:=CyclotomicField(12);
zeta3:=zeta12^4;
zeta4:=zeta12^3;
zeta6:=zeta12^2;
K<d>:=FunctionField(preK);
R:=PolynomialRing(K,3);
K1<b0,b1,b2>:=quo<R|Ideal([R.1^2 - d-3, R.2^2 - d\
```

```
 - 3*zeta3, R.3^2-(d+3*zeta3^2)])>;
S:=PolynomialRing(K1);
K2<c0>:=quo<S|S.1^3+d*S.1^2+4>;
delta:=4*zeta4*b0*b1*b2;
eps:=delta/(c0*(3*c0+2*d));
c1:=(-d-c0+eps)/2;
c2:=-d-c0-c1;
assert c2 eq (-d-c0-eps)/2;
r3 := -zeta4*(2*zeta3+1);
assert r3^2 eq 3;

PT<x,y,z,w>:=ProjectiveSpace(K2,[1,1,1,3]);
T:=CoordinateRing(PT);

fS:=x^6+y^6+z^6+d*x^2*y^2*z^2-w^2;
S:=Scheme(PT,fS);

// In order to compute the Gram matrix, we will need
// to perform some computations over a finite field FF_p^n
// that is of good reduction for X_d.
// We take p = 79.
// The residue field of K2 above p is FF_79^2.
// We also define the constants we need to define the vectors
// and the weighted projective space.

p:=79;
F<alpha>:=GF(p^2);
```

```
// Considering the case d=7 mod 79
dp:=F!7;

Pol<t>:=PolynomialRing(F);

zeta12p:=Roots(t^12-1)[12][1];
zeta6p:=zeta12p^2;
zeta4p:=zeta12p^3;
zeta3p:=zeta12p^4;
hE:=t^3+dp*t^2+4;
cp:=Roots(hE);
c0p:=cp[1][1];
c1p:=cp[2][1];
c2p:=cp[3][1];
_,b0p:=IsSquare(3+dp);
_,b1p:=IsSquare(3*zeta3p+dp);
_,b2p:=IsSquare(3*zeta3p^2+dp);

PP<X,Y,Z,W>:=ProjectiveSpace(F,[1,1,1,3]);
PPW:=CoordinateRing(PP);

// We define the reduction maps mod p,
// namely the reduction map of fields and polynomial rings.
// We define the reduction of X mod p.

prePsi:=hom<preK->F | zeta12p>;
Psi:=hom<K->F| prePsi, dp>;
```

```
Psi1:=hom<K1->F | Psi, [b0p,b1p,b2p]>;
Psi2:=hom<K2->F | Psi1, c0p>;
PsiP:=hom<T->PPW | Psi2, [X,Y,Z,W]>;

assert Psi2(c1) eq c1p;
assert Psi2(c2) eq c2p;

fSp:=PsiP(fS);
Sp:=Scheme(PP,fSp);

// Now that we defined the environments we will need later
// we can define the divisors over K2 that
// we need to generate the Picard lattice.

s3m1:=1/((2*zeta3+1)*zeta4);



// we check that these divisors are subschemes of the surfaces S
// and we also check that the reductions of these polynomials mod p
// define subschemes of Sp
checkDivisorsAreSubschemes := function(divisors)
    SetDivs1sc:=[Scheme(PT,eqn) : eqn in divisors];

    for i in [1..#SetDivs1sc] do
        i;
        C:=SetDivs1sc[i];
        assert IsCurve(C);
```

```
        assert IsSubscheme(C,S);
        I:=C meet S;
        assert Dimension(I) eq 1;
    end for;

    SetDivs1p:=[[PsiP(eqn[1]),PsiP(eqn[2])]:eqn in divisors];
    SetDivs1psc:=[Scheme(PP,eqn) : eqn in SetDivs1p ];

    for i in [1..#SetDivs1psc] do
        i;
        C:=SetDivs1psc[i];
        assert IsCurve(C);
        assert IsSubscheme(C,Sp);
        I:=C meet Sp;
        assert Dimension(I) eq 1;
    end for;
    return true;
end function;

// In order to generate the Picard lattice
// we need to take the orbits of these divisors
// under the action of the automorphism subgroup

// We define the subgroup of the automorphism group we know

computeAutomorphismGroup := function()
    Var:={x,y,z};
```

```
    Perm:=Permutations(Var);



    idT:=hom<T->T | x,y,z,w>;
    t1:=hom<T->T | y,x,z,w>;
    t2:=hom<T->T | y,z,x,w>;
    p105:=hom<T->T | zeta6*x,y,zeta6^(-1)*z,w >;
    p015:=hom<T->T | x,zeta6*y,zeta6^(-1)*z,w >;
    p003:=hom<T->T | x,y,-z,w >;
    genG:=[t1,t2,p105,p015,p003];

    S3:=[hom<T -> T | perm[1],perm[2],perm[3],w> : perm in Perm];
    C2a:=[idT,p003];
    C6a:=[hom<T->T | zeta6^i*x, y, zeta6^(-i)*z,w >: i in [0..5]];
    C2b:=[p015,idT];
    GG:=car<S3,C6a,C2b,C2a>;
    G:=[s[1]*s[2]*s[3]*s[4] : s in GG];
    return G, genG;
end function;

G, genG := computeAutomorphismGroup();

// We check the number of elements in G
checkAutomorphismGroup := function(G)
    assert #{[s(x)/LeadingCoefficient(s([x,y,z,w])[1]),\
    s(y)/LeadingCoefficient(s([x,y,z,w])[1]),\
    s(z)/LeadingCoefficient(s([x,y,z,w])[1]),\
```

```
    s(w)/LeadingCoefficient(s([x,y,z,w])[1])^3] : s in G} eq #G;
    return true;
end function;

// We check that G keeps S fixed
checkGFixesS := function()
    for s in G do
        assert s(fS) eq fS;
    end for;
    return true;
end function;

// We compute now a list of divisors that is invariant
// under the action of <G,Gal>.
// We will use this list to compute a representation of the action
// of <G,Gal>.

// First we define the Galois group
// and the maps induced on the polynomial ring
// Notice that we know that [K2:Q(d)]=96

computeGaloisGroup := function()
    Gal:=[];
    EPhi12:=[1,5,7,11];
    Ipm:=[1,-1];
    GalK1K:=CartesianPower(Ipm,3);
    cc:=[K2!c0,K2!c1,K2!c2];
```

```
    GalLE:=CartesianPower(Ipm,2); // Chris: unused

    for i in EPhi12 do
        presigma := hom<preK->K2| zeta12^i>;
        sigma := hom<K->K2 | presigma, d>;
        for s in GalK1K do
            if sigma(zeta3) eq K2!zeta3 then
            sigma1:=hom<K1->K2 | sigma, [s[1]*b0,s[2]*b1,s[3]*b2]>;
        else
            sigma1:=hom<K1->K2 | sigma, [s[1]*b0,s[2]*b2,s[3]*b1]>;
        end if;
        for j in [1..#cc] do
            c:=cc[j];
            sigma2:=hom<K2->K2 | sigma1, c>;
            Append(~Gal,sigma2);
        end for;
        end for;
    end for;
    return Gal;
end function;
Gal := computeGaloisGroup();

ImgenGal:={[zeta12,-b0,-b1,b2,c0],[zeta12^5,b0,b2,b1,c0],\
[zeta12,-b0,b1,b2,c1],[zeta12,-b0,b1,b2,c2],[-zeta12,-b0,b1,b2,c0]};

gen:=[zeta12,b0,b1,b2,c0];
genGal:=[];
```

```
for s in Gal do
    imgen:=[s(gg) : gg in gen];
    if imgen in ImgenGal then
    Append(~genGal,s);
    end if;
end for;

GalT:=[hom<T->T | s,[x,y,z,w]> : s in Gal];
genGalT:=[hom<T->T | s,[x,y,z,w]> : s in genGal];
```

computeggalorbits.m

```
computeOrbitsOfDivisors := function(group, divisors)
    Orbit:={};
    for eqn in divisors do
        for t in group do
        eqn11:=t(eqn[1]);
        eqn12:=t(eqn[2]);
        if Psi2(LeadingCoefficient(eqn11)) ne F!0 and
Psi2(LeadingCoefficient(eqn12)) ne F!0 then
            Include(~Orbit, [eqn11/LeadingCoefficient(eqn11),
eqn12/LeadingCoefficient(eqn12)]);
        else
            Include(~Orbit, [eqn11, eqn12]);
        end if;
        end for;
    end for;
```

```
    // Return the orbits as a list
    return [orbit : orbit in Orbit];
end function;

// we check that all these divisors are subschemes of S
checkGOrbitDivisorsAreSubschemes := function(divisors)
    // First check over PT
    schemes := [Scheme(PT,eqn) : eqn in divisors];
    for i in [1..#schemes] do
        C:=schemes[i];
        assert IsCurve(C);
        assert IsSubscheme(C,S);
        I:=C meet S;
        assert Dimension(I) eq 1;
    end for;

    // Now check mod p
    divisorsModp :=[[PsiP(eqn[1]),PsiP(eqn[2])] : eqn in divisors];
    schemesModp :=[Scheme(PP,eqn) : eqn in divisorsModp];

    for i in [1..#schemesModp] do
        C:=schemesModp[i];
        assert IsCurve(C);
        assert IsSubscheme(C,Sp);
        I:=C meet Sp;
        assert Dimension(I) eq 1;
    end for;
```

```
    return true;
end function;

//// We now compute the reductions of these divisors modulo p
//DivsGp:=[[PsiP(eqn[1]),PsiP(eqn[2])]:eqn in GOrbitDivs];
//
//checkNumberOfDivisorsOverReduction := function()
//    DivsGpp:={[eqn[1]/LeadingCoefficient(eqn[1]),eqn[2]\
/LeadingCoefficient(eqn[2])] : eqn in DivsGp};
//    assert #DivsGp eq #DivsGpp;
//    return true;
//end function;

// We skim the list GGalTOrbitDivs deleting the repetitions,
// getting two different lists of equations of divisors:
// SetDivsGGal and SetDivsp.
// The elements of the list at the same position are the same
// up to a scalar
// SetDivsp will be used to reduce the equation mod p
// SetDivsGGal will be used to compute the matrices
// corresponding to the action of <G,Gal> on Pic(S)

// This function takes in a list of divisors defined over K2
// and removes the
// repetitions. It returns the equations of the divisors both
//over K2 and modulo
// p, as well as the corresponding schemes.
```

```
removeRepeatedDivisors := function(divisors)
    SetDivsNP:=[eqn : eqn in divisors | \
    {LeadingCoefficient(eqn[1]), LeadingCoefficient(eqn[2])} \
    eq {1}];
    SetDivsP:=[eqn : eqn in divisors | \
    {LeadingCoefficient(eqn[1]), LeadingCoefficient(eqn[2])}\
    ne {1}];

    #SetDivsP;
    #SetDivsNP;
    assert #SetDivsP+#SetDivsNP eq #divisors;

    SetDivsP1:=[[eqn[1]/LeadingCoefficient(eqn[1]),eqn[2]/\
    LeadingCoefficient(eqn[2])]: eqn in SetDivsP];
    SetDivsP2:=Set(SetDivsP1);
    IndProb:=[Index(SetDivsP1,eqn) : eqn in SetDivsP2 ];
    SetDivsP3:=[SetDivsP[i] : i in IndProb];
    SetDivsP4:=[[eqn[1]/LeadingCoefficient(eqn[1]),eqn[2]/\
    LeadingCoefficient(eqn[2])]: eqn in SetDivsP3];

    SetDivsGGal:= SetDivsNP cat SetDivsP4;
    SetDivsp:=SetDivsNP cat SetDivsP3;
    assert #SetDivsp eq #SetDivsGGal;
    #SetDivsp;

    Divsp:=[[PsiP(eqn[1]),PsiP(eqn[2])]:eqn in SetDivsp];
    ListDivsp:=[Scheme(PP,eqn) : eqn in Divsp];
```

```
    return SetDivsGGal, SetDivsp, ListDivsp;
end function;
```

computegrammatrices.m

```
// We compute the lattice these divisors generate.
// GramMatrixD computes the intersection pairing between
// pairs of divisors in the list.
function GramMatrixD(List,D,F)
    m:=#List;
    M:=ScalarMatrix(Integers(),m,-2);

    for i in [1..m] do
        for j in [1..i] do
        Int:=List[i] meet List[j];
            if Dimension(Int) eq 1 then
            M[i,j]:=2*ArithmeticGenus(Int)-2;
        else
            M[i,j]:=Degree(Int);
        end if;
        M[j,i]:=M[i,j];
        end for;
    end for;
    return M;
end function;

function computeGramOfBasis(gram)
    L0:=Lattice(gram);
    B0:=Basis(L0);
```

```
    Sol0:=Solution(gram,[Vector(b) : b in B0]);
    M0:=Matrix(Sol0);
    return M0*gram*Transpose(M0);
end function;

// This function takes in a list of divisors defined over K2 and
// removes the repetitions. It returns the equations of the divisors
// both over K2 and modulo p, as well as the corresponding schemes.
computeSchemesModP := function(divisors)
    SetDivsNP:=[eqn : eqn in divisors |\
    {LeadingCoefficient(eqn[1]),LeadingCoefficient(eqn[2])} eq {1}];
    SetDivsP:=[eqn : eqn in divisors |\
    {LeadingCoefficient(eqn[1]),LeadingCoefficient(eqn[2])} ne {1}];

    assert #SetDivsP+#SetDivsNP eq #divisors;

    SetDivsP1:=[[eqn[1]/LeadingCoefficient(eqn[1]),eqn[2]/\
    LeadingCoefficient(eqn[2])]: eqn in SetDivsP];
    SetDivsP2:=Set(SetDivsP1);
    IndProb:=[Index(SetDivsP1,eqn) : eqn in SetDivsP2 ];
    SetDivsP3:=[SetDivsP[i] : i in IndProb];

    SetDivsp:=SetDivsNP cat SetDivsP3;

    Divsp:=[[PsiP(eqn[1]),PsiP(eqn[2])]:eqn in SetDivsp];
    ListDivsp:=[Scheme(PP,eqn) : eqn in Divsp];
    return ListDivsp;
```

```
end function;
```

comparelatticestructure.m

```
// We check that the lattice obtained
// is isometric to
// E_8(-1) + U + A_5(-1) + A_2(-1) + [[-8 -4] [-4 -8]]
// by checking they have the same rank, ,discriminant, signature,
// discriminant group and discriminant form.


/*   auxiliary function   */
function Rep2(x)
return x-2*Round(x/2);
end function;
/*   end auxiliary function    */


compareLattices := function(gram)
    L:=LatticeWithGram(gram: CheckPositive:= false);
    AL,DL,phi:=DualQuotient(L);


    mE8:=-Matrix(GramMatrix(Lattice("E",8)));
    mE8:=ChangeRing(mE8,Integers());
    U:=Matrix([[0,1],[1,0]]);
    mA5:=-Matrix(GramMatrix(Lattice("A",5)));
    mA2:=-Matrix([[2,-1],[-1,2]]);
    m4F:=Matrix([[-8, -4], [-4, -8]]);


    Dec1:=<  <mE8,1>, <U,1>, <mA2,1>, <mA5,1> , <m4F,1>>;
    L1:=Dec1[1,1];
```

```
for i in [1..#Dec1] do
    if i eq 1 and Dec1[i,2] ne 1 then
    for j in [2..Dec1[1,2]] do
        L1:=DiagonalJoin(L1,Dec1[i,1]);
        end for;
    end if;
    if i gt 1 then
    for j in [1..Dec1[i,2]] do
        L1:=DiagonalJoin(L1,Dec1[i,1]);
    end for;
    end if;
end for;

L1:=LatticeWithGram(L1: CheckPositive:= false);
AL1,DL1,phi1:=DualQuotient(L1);

q:={* Rep2(Norm((phi^-1)(g))) : g in AL *};
q1:={* Rep2(Norm((phi1^-1)(g1))) : g1 in AL1 *};

assert pSignature(L1,-1) eq pSignature(L,-1);
assert Rank(L1) eq Rank(L);
assert Factorisation(Determinant(L1)) eq\
 Factorisation(Determinant(L));
assert #Generators(AL1) eq #Generators(AL);
assert q eq q1;
assert IsIsomorphic(AL,AL1);
return true;
```

```
end function;
```

computegaloismatrices.m

```
// A priori, we have listed 432 divisors. We want to compute
// the 432x432 matrices that correspond to the elements of G and
// Galois.
// Notice that they will all be 432x432 permutation marices.
// Since these divisors generate a rank 19 lattice we can
// write these matrices as 19x19 matrices.

// We now find find 19x19 matrices for the action of elements of
// G and GalT on the basis B0.

print "Computing the matrices corresponding to the\
generators of the Galois group";

// We skim the list GGalTOrbitDivs deleting the repetitions,
// getting two different lists of equations of divisors:
// SetDivsGGal and SetDivsp.
// The elements of the list at the same position are the
// same up to a scalar.
// SetDivsp will be used to reduce the equation mod p
// SetDivsGGal will be used to compute the matrices
// corresponding to the action of <G,Gal> on Pic(S)

// This function takes in a list of divisors defined over
// K2 and removes the repetitions. It returns the
// equations of the divisors both over K2 and modulo
```

```
// p, as well as the corresponding schemes.
removeRepeatedDivisors := function(divisors)
    SetDivsNP:=[eqn : eqn in divisors |\
     {LeadingCoefficient(eqn[1]),LeadingCoefficient(eqn[2])} \
     eq {1}];
    SetDivsP:=[eqn : eqn in divisors |\
     {LeadingCoefficient(eqn[1]),LeadingCoefficient(eqn[2])} \
     ne {1}];

    #SetDivsP;
    #SetDivsNP;
    assert #SetDivsP+#SetDivsNP eq #divisors;

    SetDivsP1:=[[eqn[1]/LeadingCoefficient(eqn[1]),eqn[2]/\
     LeadingCoefficient(eqn[2])]: eqn in SetDivsP];
    SetDivsP2:=Set(SetDivsP1);
    IndProb:=[Index(SetDivsP1,eqn) : eqn in SetDivsP2 ];
    SetDivsP3:=[SetDivsP[i] : i in IndProb];
    SetDivsP4:=[[eqn[1]/LeadingCoefficient(eqn[1]),eqn[2]/\
     LeadingCoefficient(eqn[2])]: eqn in SetDivsP3];

    SetDivsGGal:= SetDivsNP cat SetDivsP4;

    SetDivsp:=SetDivsNP cat SetDivsP3;
    assert #SetDivsp eq #SetDivsGGal;
    #SetDivsp;
```

```
    Divsp:=[[PsiP(eqn[1]),PsiP(eqn[2])]:eqn in SetDivsp];
    ListDivsp:=[Scheme(PP,eqn) : eqn in Divsp];
    return SetDivsGGal, SetDivsp, ListDivsp;
end function;
SetDivsGGal, SetDivsp, ListDivsp :=\
removeRepeatedDivisors(GGalTOrbitDivs);

// This function computes the Galois representations
// of the given group elementsby computing their action on
// the given divisors.
computeGaloisRepresentations := function(divisors, groupGenerators)
    nD:=#divisors;
    groupGraphs:=[];

    for s in groupGenerators do
        Graph:=[];
        for i in [1..nD] do
            eqn:=divisors[i];
            eqn1:=[s(eqn[1]),s(eqn[2])];
            j:=Index(divisors,[eqn1[1]/LeadingCoefficient(eqn1[1]),
    eqn1[2]/LeadingCoefficient(eqn1[2])]);
            Append(~Graph,j);
        end for;
        Append(~groupGraphs,Graph);
    end for;

    // Here we compute 432x432 matrices corresponding
```

```
    // to the generators of the Galois group.
    MgroupGenerators:=[];
    for Gr in groupGraphs do
        Ms:=[[0: i in [1..nD]] : j in [1..nD]];
        for i in [1..nD] do
            Ms[i][Gr[i]]:=1;
        end for;
        Append(~MgroupGenerators,Matrix(Ms));
    end for;
    return MgroupGenerators;
end function;

    // We want to write our 432x432 matrices as 19x19 matrices
    // acting on our basis B0. The matrix M0 gives us a map

    // The matrix M0 defines a map from ZZ^19 to ZZ^720
    // We need a section of this map, N0
    // With this we compute the 19x19 matrices

reduceto19 := function(MgroupGens, gram)
    B0 := Basis(Lattice(gram));
    BB0:=Matrix(B0);
    Id19:=ScalarMatrix(19,1);
    N0:=Matrix(Solution(BB0,[gram[i] : i in [1..Nrows(gram)]]));
    M0 := Matrix(Solution(gram,[Vector(B0[i]) : i in [1..#B0]]));

    assert M0*N0 eq Id19;
```

```
    assert N0*Gram0*Transpose(N0) eq gram;


    M19groupGenerators := [M0*M*N0 : M in MgroupGens];
    return M19groupGenerators;
end function;
```

verifyfulllattice.m

```
// Load in the data we calculated in 'computegrammatrices.m'
// This consists of A0, B0, Gram0. We also load in the matrices in
// computegaloismatrices.m, since we need M19genGGal.


// This function computes the self intersection of the element
// v of a lattice L, where L has intersection form given by M.
function QuadInt(v,w,M)
    v1:=ChangeRing(Matrix(v),Integers());
    w1:=ChangeRing(Matrix(w),Integers());
    return (v1*M*Transpose(w1))[1,1];
end function;


// Notes: There are two bases to work with. To compute
// the intersection of divisors in the basis consisting of the
// list of 432 divisors, simply take two
// 1x720 vectors D, E and compute D * A0 * Transpose(E).
// Working in the basis described by M0, one can do the
// same but with 1x19
// vectors and then compute D * Gram0 * Transpose(E).
// The 19 basis elements are the rows of M0.
// Thus given a 1x19 vector, C, one
```

```
// can get an equivalent 1x720 vector by computing C * M0.
B0 := Basis(Lattice(A0));
M0 := Matrix(Solution(A0, Matrix(B0)));

// We wish to show that L0 (equivalently, LG) is the
// full Picard lattice. We will do this by showing that the
// map i_p : L0/pL0 --> Pic(X)/pPic(X) is
// injective for each prime p dividing [Pic(X) : L0].
// We know that [Pic(X) : L0]
// divides 12, so we only have to consider p = 2, 3.

// Define i_p : Lambda / p Lambda --> Pic(X) / p Pic(X),
// and let Lambda_p denote
// the kernel of i_p. Then we wish to show that Lambda_2
// and Lambda_3 are both zero. We can embed Lambda_p
// inside a group that we can calculate. Let kp
// denote the kernel of the natural map Lambda /
// p Lambda -> Hom(Lambda, Z/pZ),
// sending x to [y -> (x, y) mod p]. We can compute kp
// and the crucial fact is that Lambda_p <= kp.
// Moreover, Lambda_p is in bijection with elements of
// order dividing p in Pic(X) / Lambda, which we know to
// have size dividing 12.  Hence Lambda_2 is of dimension
// at most 2 and Lambda_3 is of dimension at most
// 1. We want to show they are both dimension 0.
// Another fact we will use is
// that Lambda_p is left fixed (as a subspace) by the
```

```
// action of <G, Gal>. So the
// idea is to compute kp and then compute the possible
// subspaces of kp after we have taken <G, Gal>-orbits.

// For p = 3, we compute the space k3, which contains
// Lambda_3, and aim to show
// that Lambda_3 is the zero space. A nonzero element
// of Lambda_3 is precisely a
// nonzero element x of Lambda / 3 Lambda such that x
// is in 3 Pic(X). We find the elements of k3 which generate
// a <G, Gal>-invariant subspace of k3 of
// dimension 1, and then show that each of these is not
// 3-divisible in Pic(X) by considering the self
// intersection number.

F3:=GF(3);
V3:=VectorSpace(F3,19);
Gram3:=ChangeRing(Gram0,F3);
k3:=sub<V3 | Kernel(Gram3)>;
print "k3 is the vector space", k3;

// These are generators for <G, Gal> in characteristic 3.
GenGG3:=[ChangeRing(M,F3) : M in M19genGGal];
GG3:=MatrixGroup<19,F3|GenGG3>;

print "The subspace Lambda_3 is at most one-dimensional,\
and is invariant under <G,Gal>, so we compute the\
```

```
possible <G,Gal>-invariant subspaces inside k3, which
are:";
k3Subspaces:=[v : v in k3 | Dimension(sub<V3 | Orbit(GG3,v)>) le 1];
print k3Subspaces;

print "A vector will only give an element of Lambda_3 if it is\
3-divisible in Pic(X). In particular, we require that C in\
Lambda can be written C = 3C' for some C' in Pic(X).\
But then (C,C) = 9(C',C'), so that 9 divides (C,C). This
holds for";
possibleLambda3 := [v : v in k3Subspaces |\
QuadInt(v,v,Gram0) mod 9 eq 0];
print possibleLambda3;

assert possibleLambda3 eq [V3![0 : i in [1..19]]];

// We conclude that only the zero vector is a possible
// element of Lambda_3, so Lambda_3 = 0.



// For p = 2, we get 4 possible nonzero divisors, with the
// <G, Gal>-orbit of each spanning at most a 2-dimensional
// subspace of k2. We have to decide
// whether each of these v is 2-divisible in Pic(X),
// since this is equivalent to
// v lying in Lambda_2. One v has self-intersection not
// divisible by 4, so cannot be 2-divisible.
```

```
// The <G, Gal>-orbits of any of the remaining 3 are
// equal, containing all three vectors.
// Hence we have to decide whether any one
// of them is 2-divisible in Pic(X).

F2:=GF(2);
V2:=VectorSpace(F2,19);
Gram2:=ChangeRing(Gram0,F2);
k2:=sub<V2 | Kernel(Gram2)>;
print "The vector space k2 is", k2;

// These are generators for <G, Gal> in characteristic 2.
GenGG2:=[ChangeRing(M,F2) : M in M19genGGal];
GG2:=MatrixGroup<19,F2|GenGG2>;

k2Subspaces := [v : v in k2 |\
Dimension(sub<V2 | Orbit(GG2, v)>) le 2];
print "The possible elements of Lambda_2 are";
print k2Subspaces;

print "We eliminate the ones with self intersection\
not divisible by 4, since\
they can't be 2-divisible in Pic(X). This leaves";
possibleLambda2 := [v : v in k2Subspaces |\
QuadInt(v,v,Gram0) mod 4 eq 0];
print possibleLambda2;
```

```
print "We note that any of the nonzero vectors\
generates the whole subspace
possibleLambda2, under the <G, Gal> action.";
[Orbit(GG2, v) : v in possibleLambda2];

print "So it remains to eliminate a single one\
of these nonzero vectors as being
2-divisible.";

// The following vector has self intersection -8.
w := possibleLambda2[2];

// Lift w to a divisor in our lattice.
C := ChangeRing(Matrix(w), Integers());
print "Can check that C (the lift of w) has C^2 = -8";
C * Gram0 * Transpose(C);

print "We want to find divisors having intersection\
with the basis equal to that
of C, which is";
desiredintersection := C * Gram0;
desiredintersection;

print "We want to find D1, D2 in <G, Gal>D such that\
D1 - D2 = C in Pic(X). We\
can check equivalence by seeing how C*Gram0\
compares with (D1-D2)*Gram0";
```

```
// This function finds D1, D2 in <G, Gal>D
// (where D is our original list of curves) such that
// D1 - D2 is linearly equivalent to C.
findLinearlyEquivalent := function()
    numCurves := Nrows(A0);
    Id := ScalarMatrix(numCurves, 1);
    for i in [1..numCurves] do
        for j in [1..numCurves] do
            D := Matrix(Id[i]) - Matrix(Id[j]);
            if D * A0 * Transpose(M0) eq desiredintersection then
                return Matrix(Id[i]), Matrix(Id[j]);
            end if;
        end for;
    end for;
    return false;
end function;
D1, D2 := findLinearlyEquivalent();
print "D1, D2 are", D1, D2;
indexD1 := [i : i in [1..Ncols(D1)] | D1[1,i] ne 0][1];
indexD2 := [i : i in [1..Ncols(D2)] | D2[1,i] ne 0][1];
print "They are numbers", indexD1, "and",\
indexD2, "in our list of divisors.";

print "We see that D1, D2 have self-intersection -2,\
and (D1, D2) = 2";
D1 * A0 * Transpose(D1);
```

```
D2 * A0 * Transpose(D2);
D1 * A0 * Transpose(D2);

print "Thus we have found explicitly the D1, D2\
such that C ~ D1 - D2 and D1^2 = D2^2 = -2,\
(D1,D2) = 2. This provides the contradiction as in the proof.";

print "The equations of the divisors are:";
schemeD1 := ListDivsp[indexD1];
schemeD2 := ListDivsp[indexD2];
print schemeD1, schemeD2;

print "We can check that they intersect as\
D1^2 = -2, D2^2 = -2, and (D1, D2) = 2";
print "D1^2 = ", 2*ArithmeticGenus(schemeD1) - 2;
print "D2^2 = ", 2*ArithmeticGenus(schemeD2) - 2;
print "(D1, D2) = ", Degree(schemeD1 meet schemeD2);
```

computegaloisactionH1.m

```
// Now we just want to use the matrices for the Galois generators.
print "Computing Galois representations for the\
generators of the Galois group";
MgenGal := computeGaloisRepresentations(SetDivsGGal, genGalT);
M19genGal := reduceto19(MgenGal, A0);

Gal19:=MatrixGroup<19,Integers()|M19genGal>;

// Using the matrix representation of the action of GG on L0
```

```
// we can compute the H^1(Gal,Pic), and H^1(H,Pic) for
// any H<Gal subgroup, not necessarily normal, subgroup of G.

gmpic:=GModule(Gal19);
cmpic:=CohomologyModule(Gal19,gmpic);
cgpic:=CohomologyGroup(cmpic,1);
print "We compute H^1(Gal, Pic) to be", cgpic;

print "Now we consider subgroups H < Gal.";
subs:=[H`subgroup : H in Subgroups(Gal19) | #H`subgroup ne 1];
nzsubs:=[];
indxs:={};

for H in subs do
  gmpicH:=GModule(H);
  cmpicH:=CohomologyModule(H,gmpicH);
  cgpicH:=CohomologyGroup(cmpicH,1);
  //cgpicH;
  //Order(H);
  //Degree(cgpicH);
  if Degree(cgpicH) ne 0 then
    Append(~nzsubs,H);
    Include(~indxs,Degree(cgpicH));
  end if;
end for;

// We try to see whether an automorphism of X_D coming from a Galois
```

```
// automorphism can be viewed as a proper geometric automorphism.
//  To have this, one should act as +1 or -1 on
// the discriminant group

L:=LatticeWithGram(Gram0: CheckPositive:= false);
AL,DL,phi:=DualQuotient(L);
BD:=Basis(DL);
/*
for b in BD do
    phi(b);
end for;
*/

BAL:=[BD[19]-BD[4]+9*BD[1],BD[1],BD[3]];
for b in BAL do
    phi(b);
end for;

for gg in Gal19 do
    gg1:=ChangeRing(gg,Rationals());
    if [phi(Vector(bb)*gg1) : bb in BAL] in \
     {[AL.1,AL.2,AL.3], [-AL.1,-AL.2,-AL.3]} then
  gg;
    end if;
end for;

// None of the Galois automorphisms is a geometric automorphism.
```

B.2.2 Output

```
Loading "main.m"

Loading "basicdefinitions.m"

Loading "computeggalorbits.m"

Computing G orbits of initial divisors

There are 150 G orbits of the initial divisors

Computing GGalTOrbitDivs

432

Loading "computegrammatrices.m"

Computing Gram matrix for the 432 divisors

The Gram matrix has determinant [ <2, 5>, <3, 3> ]

Loading "comparelatticestructure.m"

We compare the lattice we have with the lattice we expect

true

Loading "computegaloismatrices.m"

Computing the matrices corresponding to the generators of the Galois
group

0

432

432

Loading "verifyfulllattice.m"

k3 is the vector space

Vector space of degree 19, dimension 3 over GF(3)

Generators:

(1 0 0 0 0 0 0 2 0 1 0 0 2 2 2 1 2 1 0)

(0 0 1 1 0 2 2 2 2 1 0 2 2 2 0 0 2 1 0)

(0 0 0 0 1 2 1 1 1 1 0 2 0 2 1 2 2 0 0)
```

```
Echelonized basis:
(1 0 0 0 0 0 0 2 0 1 0 0 2 2 2 1 2 1 0)
(0 0 1 1 0 2 2 2 2 1 0 2 2 2 0 0 2 1 0)
(0 0 0 0 1 2 1 1 1 1 0 2 0 2 1 2 2 0 0)
The subspace Lambda_3 is at most one-dimensional,
and is invariant under <G,Gal>, so we compute the possible
<G,Gal>-invariant subspaces inside k3, which are:
[
    (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0),
    (1 0 1 1 1 1 0 2 0 0 0 1 1 0 0 0 0 2 0),
    (2 0 2 2 2 2 0 1 0 0 0 2 2 0 0 0 0 1 0)
]
A vector will only give an element of Lambda_3
if it is 3-divisible in
Pic(X). In particular, we require that C in Lambda can be written
C = 3C' for some C' in Pic(X). But then (C,C) = 9(C',C'), so that
9 divides (C,C). This holds for
[
    (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
]
The vector space k2 is
Vector space of degree 19, dimension 3 over GF(2)
Generators:
(0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0)
(0 0 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0)
(0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)
Echelonized basis:
```

```
(0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0)
(0 0 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0)
(0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)
The possible elements of Lambda_2 are
[
    (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0),
    (0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0),
    (0 1 1 1 0 0 1 0 1 1 1 0 0 0 0 0 0 0 0),
    (0 0 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0),
    (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1)
]
We eliminate the ones with self intersection not divisible
by 4, since they can't be 2-divisible in Pic(X). This leaves
[
    (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0),
    (0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0),
    (0 1 1 1 0 0 1 0 1 1 1 0 0 0 0 0 0 0 0),
    (0 0 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0)
]
We note that any of the nonzero vectors generates the whole subspace
possibleLambda2, under the <G, Gal> action.
[
    {
        (0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)
    },
    {
        (0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0),
```

```
        (0 0 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0),
        (0 1 1 1 0 0 1 0 1 1 1 0 0 0 0 0 0 0 0)
    },
    {
        (0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0),
        (0 0 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0),
        (0 1 1 1 0 0 1 0 1 1 1 0 0 0 0 0 0 0 0)
    },
    {
        (0 1 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 0 0),
        (0 0 1 0 0 0 1 0 0 1 0 0 0 0 0 0 0 0 0),
        (0 1 1 1 0 0 1 0 1 1 1 0 0 0 0 0 0 0 0)
    }
]
```

So it remains to eliminate a single one of these nonzero vectors as being 2-divisible.

Can check that C (the lift of w) has C^2 = -8

```
[-8]
```

We want to find divisors having intersection with the basis equal to that of C, which is

```
[ 2  2 -2 -4  0  0 -2  0 -2  4 -4  0  0  0  2 -2 -2  2  0]
```

We want to find D1, D2 in <G, Gal>D such that D1 - D2 = C in Pic(X). We can check equivalence by seeing how C*Gram0 compares with (D1-D2)*Gram0. D1, D2 are

```
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

```
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0]

[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 0 0]
We see that D1, D2 have self-intersection -2, and (D1, D2) = 2
```

```
[-2]
[-2]
[2]
Thus we have found explicitly the D1, D2 such that C ~ D1 - D2
and D1^2 = D2^2 = -2, (D1,D2) = 2. This provides the contradiction
as in the proof.
Loading "computegaloisactionH1.m"
Computing Galois representations for the generators of the
Galois group
We compute H^1(Gal, Pic) to be
Full Quotient RSpace of degree 3 over Integer Ring
Column moduli:
[ 2, 2, 2 ]
Now we consider subgroups H < Gal.
3*AL.1 + 11*AL.3
8*AL.2 + 4*AL.3
4*AL.1 + 2*AL.2 + 2*AL.3
```

Bibliography

[AKR10] T. Abbott, K. Kedlaya, and D. Roe. "Bounding Picard numbers of surfaces using p-adic cohomology". In: *Arithmetics, geometry, and coding theory (AGCT 2005)*. Vol. 21. Sémin. Congr. Paris: Soc. Math. France, 2010, pp. 125–159.

[BHPV04] W. Barth, K. Hulek, C. Peters, and A. Van de Ven. *Compact Complex Surfaces*. second. Vol. 4. A Series of Modern Surveys in Mathematics. Springer, 2004.

[BS75] B.J. Birch and P. Swinnerton-Dyer. "The Hasse problem for rational surfaces". In: *J. reine angew. Math* 274.275 (1975), pp. 164–174.

[BCP97] W. Bosma, J. Cannon, and C. Playoust. "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265.

[Bri06] M. Bright. "Brauer groups of diagonal quartic surfaces". In: *J. Sympolic Comput.* 41.5 (2006), pp. 544–558.

[CG66] J.W.S. Cassels and M.J.T. Guy. "On the Hasse principle for cubic surfaces". In: *Mathematika* 13.02 (1966), pp. 111–120.

[Cha11] F. Charles. "On the Picard number of K3 surfaces over number fields". In: *Algebra Number Theory* 8.1 (2011), pp. 1–17.

[Cha13] F. Charles. "The Tate conjecture for $K3$ surfaces over finite fields". In: *Invent. Math.* 194.1 (2013), pp. 119–145.

[Col03] J.-L. Colliot-Thélène. “Points rationnels sur les fibrations”. In: *Higher Dimensional Varieties and Rational Points (Budapest 2001)*. Ed. by K. J. Böröczky, J. Kollár, and T. Szamuely. Vol. 12. Bolyai Society Mathematical Series. Springer-Verlag, 2003, pp. 171–221.

[Col99] J.-L. Colliot-Thélène. “Points rationnels sur les variétés non de type général, Chapitre II”. Cours IHP, lecture notes, `http://www.math.u-psud.fr/~colliot/Cours99_ChapII.pdf`. 1999.

[CKS87] J.-L. Colliot-Thélène, D. Kanevsky, and J.-J. Sansuc. *Arithmétique des surfaces cubiques diagonales*. Vol. 1290. Lecture Notes in Math. Springer, 1987, pp. 1–108.

[CS80] J.-L. Colliot-Thélène and J.-J. Sansuc. “La descente sur les variétés rationnelles”. French. In: *Journées de Géométrie Algébrique d’Angers, Juillet 1979/Algebraic Geometry, Angers, 1979 ed.* (1980), pp. 223–237.

[Cor05] P. Corn. “Del Pezzo surfaces and the Brauer-Manin obstruction”. PhD thesis. Harvard University, 2005.

[CD89] F. Cossec and I. Dolgachev. *Enriques Surfaces I*. Vol. 76. Progress in Mathematics. Birkhäuser Boston, 1989.

[CT14] E. Costa and Y. Tschinkel. “Variation of Néron-Severi ranks of reductions of K3 surfaces”. In: *Exp. Math.* 23.4 (2014), pp. 475–481.

[EJ08a] A.-S. Elsenhans and J. Jahnel. “$K3$ surfaces of Picard rank one and degree two”. In: *Algorithmic number theory*. Vol. 5011. Lecture Notes in Comput. Sci. Berlin: Springer, 2008, pp. 212–225.

[EJ08b] A.-S. Elsenhans and J. Jahnel. “$K3$ surfaces of Picard rank one which are double covers of the projective plane”. In: *Higher-dimensional geometry over finite fields*. Vol. 16. NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. Amsterdam: IOS, 2008, pp. 63–77.

[EJ11a] A.-S. Elsenhans and J. Jahnel. “On the computation of the Picard group for $K3$ surfaces”. In: *Math. Proc. Cambridge Philos. Soc.* 151.2 (2011), pp. 263–270.

[EJ16] A.-S. Elsenhans and J. Jahnel. *Point counting on $K3$ surfaces and an application concerning real and complex multiplication*. arXiv:1602.04327. 2016.

[EJ11b] A.-S. Elsenhans and J. Jahnel. “The Picard group of a $K3$ surface and its reduction modulo p”. In: *Algebra Number Theory* 5.8 (2011), pp. 1027–1040.

[HW16] Y. Harpaz and O. Wittenberg. “On the fibration method for zero-cycles and rational points”. In: *Annals of Mathematics* 183.1 (2016), pp. 229–295.

[Har77] R. Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[Har15] D. Harvey. “Computing zeta functions of arithmetic schemes”. In: *Proc. Lond. Math. Soc. (3)* 111.6 (2015), pp. 1379–1401. ISSN: 0024-6115. DOI: 10.1112/plms/pdv056. URL: http://dx.doi.org/10.1112/plms/pdv056.

[HKT13] B. Hassett, A. Kresch, and Y. Tschinkel. “Effective computation of Picard groups and Brauer–Manin obstructions of degree two K3 surfaces over number fields”. In: *Rendiconti del Circolo Matematico di Palermo* 62.1 (2013), pp. 137–151.

[HVV11] B. Hassett, A. Várilly-Alvarado, and P. Varilly. “Transcendental obstructions to weak approximations on general K3 surfaces”. In: *Adv. Math.* 228.3 (2011), pp. 1377–1404.

[Huy14] D. Huybrechts. *Lecture on K3 surfaces*. Accessed: 03-24-2016. 2014. URL: http://www.math.uni-bonn.de/people/huybrech/K3Global.pdf.

[Ier10] E. Ieronymou. “Diagonal quartic surfaces and transcendental elements of the Brauer group”. In: *J. Inst. Math. Jussieu* 9.04 (2010), pp. 769–798.

[Jah14] J. Jahnel. *Brauer groups, Tamagawa measures, and rational points on algebraic varieties*. Vol. 198. American Mathematical Soc., 2014.

[KW89] L.-C. Kappe and B. Warren. “An elementary test for the Galois group of a quartic polynomial”. In: *Amer. Math. Monthly* 96.2 (1989), pp. 133–137. ISSN: 0002-9890. DOI: 10.2307/2323198. URL: http://0-dx.doi.org.pugwash.lib.warwick.ac.uk/10.2307/2323198.

[LLR05] Q. Liu, D. Lorenzini, and M. Raynaud. “On the Brauer group of a surface”. In: *Invent. Math.* 159.3 (2005), pp. 673–676. ISSN: 0020-9910. DOI: 10.1007/s00222-004-0403-2. URL: http://dx.doi.org/10.1007/s00222-004-0403-2.

[Lui07] R. van Luijk. “K3 surfaces with Picard number one and infinitely many rational points”. In: *Algebra Number Theory* 1.1 (2007), pp. 1–15.

[Mad15] K. Madapusi Pera. “The Tate conjecture for K3 surfaces in odd characteristic”. In: *Invent. Math.* 201.2 (2015), pp. 625–668.

[Man74] Y. Manin. *Cubic forms: algebra, geometry, arithmetic*. Vol. 4. North-Holland Publishing Co., Amsterdam, 1974.

[Man71] Y. Manin. “Le groupe de Brauer-Grothendieck en géométrie diophantienne”. In: *Actes du Congres International des Mathématiciens (Nice, 1970)*. Vol. 1. World Scientific. 1971, pp. 401–411.

[Mau14] D. Maulik. “Supersingular K3 surfaces for large primes”. In: *Duke Math. J.* (2014), pp. 2357–2425.

[Mil13] J.S. Milne. *Class Field Theory (v4.02)*. Available at www.jmilne.org/math/. 2013.

[Mil80] J.S. Milne. *Etale Cohomology (PMS-33)*. Princeton Mathematical Series 33. Princeton university press, 1980.

[Mil75a] J.S. Milne. “On a conjecture of Artin and Tate”. In: *Ann. of Math. (2)* 102.3 (1975), pp. 517–533. ISSN: 0003-486X.

[Mil75b] J.S. Milne. *On a conjecture of Artin and Tate - addendum*. `http://www.jmilne.org/math/articles/add/1975a.pdf`. 1975.

[Mor49] L.J. Mordell. “Rational points on cubic surfaces”. In: *Pub. Math. Debrecen* 1 (1949), pp. 1–6.

[Mor84] D.R. Morrison. “On K3 surfaces with large Picard number”. In: *Invent. Math.* 35 (1984), pp. 105–121.

[Nic55] H. Nichimura. “Some remarks on rational points”. In: *Mem. Coll. Sci. Univ. Kyoto. Ser. A. Math.* 29 (1955), pp. 189–192.

[Nik80] V. V. Nikulin. “Integer symmetric bilinear forms and some of their geometric applications”. In: *Math USSR-Izv* 14.1 (1980), pp. 103–167.

[PTL12] B. Poonen, D. Testa, and R. van Luijk. “Computing Néron–Severi groups and cycle class groups”. In: *Compos. Math.* 151.04 (2012), pp. 713–734.

[Sel53] E.S. Selmer. “Sufficeient congruence conditions for the existence of rational points on certain cubic surfaces”. In: *Math. Scand.* 1 (1953), pp. 113–119.

[Ser56] J.-P. Serre. “Géom’etrie algébrique et géométrie analytique”. In: *Ann. Inst. Fourier, Grenable* 6 (1955–1956), pp. 1–42.

[Ser79] J.-P. Serre. *Local fields*. Vol. 67. Springer-Verlag, 1979.

[Sko55] T. Skolem. “Einige Bemerkungen über die Auffindung von tationalen Punken auf gewissen algebraischen Gebilden”. In: *Math. Zeitschrift* 63 (1955), pp. 295–312.

[Sko01] A. Skorobogatov. *Torsors and rational points*. Vol. 144. Cambridge University Press, 2001.

[SS05] A. Skorobogatov and P. Swinnerton-Dyer. “2-descent on elliptic curves and rational points on certain Kummer surfaces”. In: *Adv. Math.* 198.2 (2005), pp. 448–483.

[Ste04] I. Stewart. *Galois theory*. CRC Press, 2004.

[Swi99] H.P.F. Swinnerton-Dyer. “Brauer–Manin obstructions on some del Pezzo surfaces”. In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 125-02. Cambridge Univ Press. 1999, pp. 193–198.

[Swi93] H.P.F. Swinnerton-Dyer. “The Brauer group of cubic surfaces”. In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 113-03. Cambridge Univ Press. 1993, pp. 449–460.

[Swi62] H.P.F. Swinnerton-Dyer. “Two special cubic surfaces”. In: *Mathematika* 9 (1962), pp. 54–56.

[Tat10] J. Tate. “Global Class FIeld Theory”. In: *Algebraic Number Theory*. Ed. by J.W.S. Cassels and A. Fröhlich. London Mathematical Society, 2010, pp. 162–203.

[Wit04] O. Wittenberg. “Transcendental Brauer–Manin obstruction on a pencil of elliptic curves”. In: *Arithmetic of higher-dimensional algebraic varieties*. Vol. 226. Progr. Math. Birkhäuser Boston, 2004, pp. 259–267.