Rational points on K3 surfaces

by

Ronald Martinus van Luijk

Grad. (University of Utrecht, Netherlands) 2000

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY of CALIFORNIA, BERKELEY

Committee in charge:

Professor Hendrik Lenstra, Chair
Professor Bjorn Poonen
Professor David A. Forsyth

Spring 2005

The dissertation of Ronald Martinus van Luijk is approved:

Chair Date

Date

Date

University of California, Berkeley

Spring 2005

Rational points on K3 surfaces

Copyright 2005
by
Ronald Martinus van Luijk

Abstract

Rational points on K3 surfaces

by

Ronald Martinus van Luijk
Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Hendrik Lenstra, Chair

In this thesis I consider several problems of a Diophantine nature that relate to algebraic surfaces.

Frits Beukers has asked whether there is an integral matrix

$$\begin{pmatrix} 0 & a & b \\ a & 0 & c \\ b & c & 0 \end{pmatrix}$$

with all its eigenvalues integral and not in $\{0, \pm a, \pm b, \pm c\}$. Using the theory of elliptic surfaces, I show that up to scaling infinitely many such matrices exist.

A Heron triangle is a triangle with integral sides and integral area. There are pairs of nonsimilar Heron triangles with the same area and the same perimeter. The problem of finding three such triangles, brought to my attention by Richard Guy, can again be solved with the use of elliptic surfaces. I show that for each positive integer N there is in fact an infinite parametrized family of N such triangles.

In both cases, the solution involves showing that the set of rational points on a certain K3 surface is Zariski dense. I also compute the geometric Picard number of these surfaces. This important geometric invariant equals the rank of the Néron-Severi group of the surface over an algebraic closure of its base field. This group, consisting of divisor classes modulo algebraic equivalence, has rank at most 22 for K3 surfaces.

In general, little is known about the arithmetic of K3 surfaces, especially for those with geometric Picard number 1. I prove that in the moduli space of polarized K3 surfaces of degree 4, the set of surfaces defined over $\mathbb{Q}$ with geometric Picard number 1 and infinitely many rational points is dense in both the Zariski topology and the real analytic topology. This answers a question posed by Sir Peter Swinnerton-Dyer and Bjorn Poonen. Its effective proof, citing explicit examples, also disposes of an old challenge attributed to David Mumford.

For the convenience of the reader, I provide proofs of several theorems involving constructions of elliptic surfaces and the behavior of the Néron-Severi group under reduction. Some of these results are well known to experts, but a substantial search in the literature failed to reveal complete proofs. I also give a scheme-theoretic summary of the theory of elliptic surfaces, including a new proof of the classification of singular fibers.

Professor Hendrik Lenstra
Dissertation Committee Chair

To my family

Contents

Acknowledgements

This thesis brings an end to a wonderful time spent in Berkeley, California. I am grateful to everybody that contributed to this part of my life, the thesis itself, or even both.

It is an honor to thank my adviser Hendrik Lenstra for his excellent guidance on so many levels. His passion and his ability to instantly approach a mathematical problem from the right point of view are truly inspiring. A special thanks also goes to Bjorn Poonen. His work and ideas and the discussions I have had with him are a great source of inspiration as well. Without Hendrik and Bjorn this thesis would not have been the same.

I would like to thank Frits Beukers and Richard Guy for the problems that led to Chapters 3 and 4 of this thesis. The problem discussed in Chapter 5 came to my attention at the American Institute of Mathematics at a memorable conference organized by Bjorn Poonen and Yuri Tschinkel. I am indebted to the Institut Henri Poincaré in Paris for the marvelous working conditions that led to the solution of this problem. I thank Arthur Ogus, Robin Hartshorne, Jasper Scholten, Bert van Geemen, Tom Graber, Bas Edixhoven, Jan Stienstra, Noriko Yui, Jaap Top, Peter Stevenhagen, Jean-Louis Colliot-Thélène, and David Harari for the useful discussions we have had.

I thank my family for their endless support in all ways thinkable. It is impossible to imagine what my life would have looked like without my parents, and I feel blessed to have brothers as cool and caring as Jeroen and Peter.

I thank my house mates Max Cowan, Nana Koami, Walter Kim, Hans Roskam, Bob Risebrough, and Barbara and Howard Mackey for the perfect atmosphere at home. In and around Evans, my second home in Berkeley, I enjoyed the company of many people. I especially want to thank my good friends Grace Lyo, Dave Spivak, Aaron Greicius, Jeremy Marzuola, Ioan Berbec, Jared Weinstein, Alex Barnard, Frank Calegari, Alf Onshuus, John Voight, and Samit Dasgupta for being there.

I am delighted that my brain was not influenced by only mathematics during my stay in Berkeley. I thank Jessica Shugart and the entire Berkeley hang gliding club for altering my mind in their own special way.

Ronald van Luijk
Berkeley, 2005

Chapter 1

Introduction

For millennia, mathematicians have been fascinated by what we now call Diophantine equations. These are systems of polynomial equations with integral coefficients for which we seek integral or rational solutions. A typical example of a result is the existence of infinitely many Pythagorean triples of coprime integers (a, b, c), which satisfy $a^2 + b^2 = c^2$. The solutions to this equation correspond to rational points on an algebraic curve. Some Diophantine problems however, ask for the existence of rational points on varieties of higher dimension. The geometry of these varieties governs their arithmetic, but how exactly is not clear at all. This is one of the main problems of higher-dimensional arithmetic geometry. Many fundamental questions about the distribution of rational points on algebraic surfaces are still wide open. With the arithmetic of curves being understood as well as it is, the third millennium is ripe for these higher-dimensional questions.

This thesis focuses on the case of so called K3 surfaces, which are the 2-dimensional analogues of elliptic curves in the sense that their canonical sheaf is trivial. Smooth quartic surfaces in $\mathbb{P}^3$ are examples of K3 surfaces. Little is known about the arithmetic of these surfaces. It is for instance not known whether there exists a K3 surface over the rational numbers (or any number field) on which the set of rational points is neither empty nor dense.

As rational points on surfaces tend to accumulate on low genus curves, the study of divisors on surfaces is an important tool. The group of divisor classes modulo algebraic equivalence on a surface X is called the Néron-Severi group of X. For a K3 surface the Néron-Severi group is a finitely generated free abelian group. Together with the intersection pairing it carries a lot of combinatorial information. Its rank is called the Picard number of X, denoted $\rho(X)$. Bogomolov and Tschinkel proved in [BT] that if X is a K3 surface over a number field K with $\rho(X_{\overline{K}}) \geq 2$, then in most cases the rational points are potentially dense. This means that there is a finite extension L of K such that the set $X(L)$ of L-rational points on X is Zariski dense in X. Nothing is known about potential density of rational points on K3 surfaces X with $\rho(X_{\overline{K}}) = 1$. In fact, until recently it was an old challenge, attributed to Mumford, to find even just one explicit example of a K3 surface X over a number field K with $\rho(X_{\overline{K}}) = 1$. This challenge will be disposed of in Chapter 5, where we will see explicit examples of such surfaces with $K = \mathbb{Q}$ that also contain infinitely many rational points. Moreover, we will prove that the set of such surfaces is dense in the moduli space of polarized K3 surfaces of degree 4, in both the Zariski topology and the real analytic topology.

For the convenience of the reader, Chapter 2 describes all the prerequisites with a proof or a reference. Most importantly this chapter contains a treatment of Shioda's theory of elliptic surfaces in a scheme-theoretic language, a new proof of the classification of singular fibers, some constructions of elliptic fibrations, and the behavior of the Néron-Severi group under good reduction. For these last results no complete proof appears to be available in the literature.

Chapters 3 and 4 both solve an explicit 2-dimensional Diophantine problem. The solutions make use of elliptic K3 surfaces. In each case we find the full Néron-Severi group of the surface involved and use this for a deeper study of the geometry of the surface.

Chapter 2

Lattices and surfaces

2.1 Lattices

In this section we will define lattices and finite quadratic forms and we will state some results with proof or reference for later use.

For any abelian groups A and G, a symmetric bilinear map $A \times A \to G$ is called *nondegenerate* if the induced homomorphism $A \to \mathrm{Hom}(A, G)$ is injective. We will not require a lattice to be definite, only nondegenerate.

Definition 2.1.1 *A* lattice *is a free $\mathbb{Z}$-module L of finite rank, endowed with a symmetric, bilinear, nondegenerate map $\langle \_\,, \_ \rangle \colon L \times L \to \mathbb{Q}$, called the* pairing *of the lattice. An* integral lattice *is a lattice whose pairing is $\mathbb{Z}$-valued. A lattice L is called* even *if $\langle x, x \rangle \in 2\mathbb{Z}$ for every $x \in L$. A* sublattice *of L is a submodule L' of L, such that the induced bilinear map on L' is nondegenerate. A sublattice L' of L is called* primitive *if L/L' is torsion-free. The positive or negative definiteness or signature of a lattice is defined to be that of the vector space $L_{\mathbb{Q}}$ together with the induced pairing.*

Remark 2.1.2 From the identity $2\langle x, y \rangle = \langle x + y, x + y \rangle - \langle x, x \rangle - \langle y, y \rangle$ it follows that every even lattice is integral.

Remark 2.1.3 If L is a lattice, then its pairing induces an inner product on the vector space $L_{\mathbb{Q}}$, i.e., a nondegenerate symmetric bilinear map $L_{\mathbb{Q}} \times L_{\mathbb{Q}} \to \mathbb{Q}$.

Definition 2.1.4 *If L is a subgroup of a lattice Λ, then the orthogonal complement $L^{\perp}$ of L in Λ is*

$$L^{\perp} = \{x \in \Lambda \mid \langle x, y \rangle = 0 \text{ for all } y \in L\}.$$

Lemma 2.1.5 *If L is a sublattice of a lattice Λ, then its orthogonal complement $L^{\perp}$ is a primitive sublattice of rank equal to $\mathrm{rk}\,\Lambda - \mathrm{rk}\,L$. We have $(L^{\perp})^{\perp} = L_{\mathbb{Q}} \cap \Lambda$.*

Proof. To prove that $L^\perp$ is a sublattice (i.e., the induced pairing on $L^\perp$ is nondegenerate) of the right rank, we may tensor with $\mathbb{Q}$ and prove a similar statement for the corresponding inner product spaces. This is an easy exercise, see for instance [La], Prop. XV.1.2. The most important hypothesis is that the induced inner product on $L_\mathbb{Q}$ is nondegenerate. The fact that $L^\perp$ is primitive follows immediately from the definition of $L^\perp$ and the fact that the pairing is bilinear. From the relation between the ranks we find that $(L^\perp)^\perp$ is a sublattice of Λ, containing the primitive sublattice $L' = L_\mathbb{Q} \cap \Lambda$, with the same rank as L'. This implies $(L^\perp)^\perp = L'$. $\square$

Definition 2.1.6 *For a lattice L with pairing $\langle \_\,,\_\rangle$, we denote by $L(n)$ the lattice with the same underlying module as L and the pairing $n \cdot \langle \_\,,\_\rangle$.*

Definition 2.1.7 *Let M be a module over a commutative ring R with a map $\langle \_\,,\_\rangle \colon M \times M \to R$. Then the* Gram matrix *with respect to a sequence $x = (x_1, \ldots, x_r)$ of elements in M is $I_x = (\langle x_i, x_j\rangle)_{i,j}$.*

Definition 2.1.8 *The* discriminant *of a lattice L is defined by* $\operatorname{disc} L = \det I_x$*, where I_x is the Gram matrix with respect to any $\mathbb{Z}$-basis x of L. A lattice L is called* unimodular *if it is integral and* $\operatorname{disc} L = \pm 1$.

Lemma 2.1.9 *Let L' be a sublattice of finite index in a lattice L. Then we have* $\operatorname{disc} L' = [L : L']^2 \operatorname{disc} L$.

Proof. This is a well known fact, see also [Shi3], section 6. $\square$

Definition 2.1.10 *Let V be a finite dimensional inner product space over a field k. Then the* discriminant $\operatorname{disc} V$ *of V is defined to be the image in $k^*/(k^*)^2$ of the determinant of the Gram matrix associated to any basis of V.*

Remark 2.1.11 The discriminant of an inner product space V of dimension n is well defined because the determinants of the Gram matrices associated to two different bases differ by a square factor. For $k = \mathbb{Q}$ this discriminant is equal to the image in $\mathbb{Q}^*/\mathbb{Q}^{*2}$ of the discriminant of any lattice in V of dimension n. This fact will be used in chapter 5.

Definition 2.1.12 *Let L be a lattice. We define the* dual lattice L^* *by*

$$\{x \in L_\mathbb{Q} \mid \langle x, y\rangle \in \mathbb{Z} \text{ for all } y \in L\}.$$

Lemma 2.1.13 *Let L be an integral lattice. Then* $|\operatorname{disc} L| = [L^* : L]$.

Proof. There is an isomorphism $L^* \cong \operatorname{Hom}(L, \mathbb{Z})$. If x is a basis for L, then the dual basis x' of $\operatorname{Hom}(L_\mathbb{Q}, \mathbb{Q})$ generates $\operatorname{Hom}(L, \mathbb{Z})$ as a $\mathbb{Z}$-module. Hence, for the Gram matrices I_x and $I_{x'}$ we find $I_{x'} = I_x^{-1}$. Thus, $\operatorname{disc} L^* = 1/(\operatorname{disc} L)$. By Lemma 2.1.9 we have $\operatorname{disc} L = [L^* : L]^2 \operatorname{disc} L^*$, from which the equality follows. $\square$

Lemma 2.1.14 *Let Λ be an integral lattice with sublattice L and set $L' = L_{\mathbb{Q}} \cap \Lambda$ inside $\Lambda_{\mathbb{Q}}$. Then the orthogonal projection $\pi\colon \Lambda \to L_{\mathbb{Q}}$ is contained in L'^*. If L is unimodular then the image is exactly L and Λ is the orthogonal direct sum of L and $L^\perp$.*

Proof. Take $x \in \Lambda$, then for every $z \in L'$ we have $\langle \pi(x), z\rangle = \langle x, z\rangle \in \mathbb{Z}$, so we find $\pi(x) \in L'^*$. If L is unimodular, then we have $L^* = L'^* = L' = L$, so we get $\pi(\Lambda) \subset L$. As we obviously have $L \subset \pi(\Lambda)$, we conclude $\pi(\Lambda) = L$. The kernel of π being $L^\perp$, we get a short exact sequence $0 \to L^\perp \to \Lambda \to L \to 0$. The final statement follows from the fact that the inclusion $L \subset \Lambda$ is a section whose image is orthogonal to $L^\perp$. □

Lemma 2.1.15 *Let Λ be a lattice with sublattice L. Then we have*

$$\operatorname{disc}(L^\perp \oplus L) = (\operatorname{disc} L^\perp)(\operatorname{disc} L) \qquad \textit{and}$$
$$\operatorname{disc} L^\perp = \operatorname{disc}\Lambda \cdot [\Lambda : L^\perp \oplus L]^2 / \operatorname{disc} L.$$

Proof. By taking bases for L and $L^\perp$ and using the union as a basis for $L^\perp \oplus L$, we easily verify the first equation. By Lemma 2.1.5 the lattice $L^\perp \oplus L$ has finite index in Λ. By Lemma 2.1.9 we find $\operatorname{disc}(L^\perp \oplus L) = [\Lambda : L^\perp \oplus L]^2 \operatorname{disc}\Lambda$. Combining this with the first equation, we find the second equation. □

We will now define discriminant forms as defined by Nikulin [Ni], § 1.3.

Definition 2.1.16 *Let A be a finite abelian group. A* finite symmetric bilinear form *on A is a symmetric bilinear map $b\colon A \times A \to \mathbb{Q}/\mathbb{Z}$.*

A finite quadratic form *on A is a map $q\colon A \to \mathbb{Q}/2\mathbb{Z}$, such that for all $n \in \mathbb{Z}$ and $a \in A$ we have $q(na) = n^2 q(a)$ and such that the unique map $b\colon A \times A \to \mathbb{Q}/\mathbb{Z}$ determined by $q(a + a') - q(a) - q(a') \equiv 2b(a, a') \bmod 2\mathbb{Z}$ for all $a, a' \in A$ is a finite symmetric bilinear form on A. The form b is called* the bilinear form of *q.*

Lemma 2.1.17 *Let L be an even lattice and set $A_L = L^*/L$. Then we have $\#A_L = |\operatorname{disc} L|$ and the map*

$$q_L\colon A_L \to \mathbb{Q}/2\mathbb{Z}\colon x \mapsto \langle x, x\rangle + 2\mathbb{Z}$$

is a finite quadratic form on A_L.

Proof. The first statement is a reformulation of Lemma 2.1.13. The map q_L is well defined, as for $x \in L^*$ and $\lambda \in L$, we have $\langle x+\lambda, x+\lambda\rangle - \langle x, x\rangle = 2\langle x, \lambda\rangle + \langle \lambda, \lambda\rangle \in 2\mathbb{Z}$. The unique map $b\colon A_L \times A_L \to \mathbb{Q}/\mathbb{Z}$ as in Definition 2.1.16 is given by $(a, a') \mapsto \langle a, a'\rangle + \mathbb{Z}$, which is clearly a finite symmetric bilinear form. Thus, q_L is a finite quadratic form. □

Definition 2.1.18 *If L is an even lattice, then the map q_L as in Lemma* 2.1.17 *is called the* discriminant-quadratic form *associated to L.*

Lemma 2.1.19 *Let L be a primitive sublattice of an even unimodular lattice Λ. Let $L^\perp$ denote the orthogonal complement of L in Λ. Then $q_L \cong -q_{L^\perp}$, i.e., there is an isomorphism $A_L \to A_{L^\perp}$ making the following diagram commutative.*

$$\begin{tikzcd} A_L \arrow[r, "\cong"] \arrow[d, "q_L"'] & A_{L^\perp} \arrow[d, "q_{L^\perp}"] \\ \mathbb{Q}/2\mathbb{Z} \arrow[r, "{[-1]}"] & \mathbb{Q}/2\mathbb{Z} \end{tikzcd}$$

Proof. See [Ni], Prop. 1.6.1. □

Lemma 2.1.20 *Let Λ be a integral lattice with sublattice T and set $T' = T_{\mathbb{Q}} \cap \Lambda$ and $L = T^\perp$ and $A = \Lambda/T$. Let $m > 0$ be an integer satisfying $mT'^* \subset T'$. Then the orthogonal projection $\Lambda \to T_{\mathbb{Q}}$ induces a homomorphism $A \to T'^*/T$ whose kernel M has finite index in A. The orthogonal projection $\Lambda \to L_{\mathbb{Q}}$ induces a homomorphism $\gamma\colon A \to \frac{1}{m}L \cap L^*$ with kernel $A_{\mathrm{tors}} \cong T'/T$. The homomorphism γ maps M isomorphically to L.*

Proof. Let π_L and π_T denote the orthogonal projections $\Lambda \to L_{\mathbb{Q}}$ and $\Lambda \to T_{\mathbb{Q}}$ respectively. It follows from Lemma 2.1.14 that the images of π_L and π_T are contained in L^* and T'^* respectively. To show that the image of π_L is also contained in $\frac{1}{m}L$, take $x \in \Lambda$ and set $y = \pi_T(x) \in T'^*$ and $z = \pi_L(x) \in L^*$. Then $x = y + z$, and as we have $my \in mT'^* \subset T' \subset \Lambda$, we get $mz = mx - my \in \Lambda$, so $mz \in \Lambda \cap L^* = L$. The kernel of π_L is $L^\perp = T'$, see Lemma 2.1.5. This implies that π_L induces a homomorphism $\gamma\colon A = \Lambda/T \to \frac{1}{m}L \cap L^*$ with kernel T'/T, which is exactly A_{tors}.

The map π_T induces a homomorphism $\Lambda \to T'^*/T$ with kernel $L + T$. Thus this homomorphism induces a map $\delta\colon A \to T'^*/T$ with kernel $M = (L+T)/T$. Because the cokernel of δ is finite, M has finite index in A. As we have $L \cap T = (0)$, the quotient map $\Lambda \to A$ restricts to an injection $\iota\colon L \hookrightarrow A$ whose image is M. Since the composition $\gamma \circ \iota = \pi_L|_L$ is the identity on L, we find that γ sends M isomorphically to L. □

Let Λ be an integral lattice with sublattice T and set $T' = T_{\mathbb{Q}} \cap \Lambda$. Applying Lemma 2.1.20 to the sublattice T' of Λ, we find that Λ/T' injects into $\frac{1}{m}L$ with $L = T^\perp$, so Λ/T' also has the structure of a lattice. Its discriminant is related to those of Λ and T by the following lemma.

Lemma 2.1.21 *Let T be a sublattice of a lattice Λ and set $T' = T_{\mathbb{Q}} \cap \Lambda$. Then Λ/T' is a lattice and we have*

$$\operatorname{disc} \Lambda = \frac{(\operatorname{disc} T)(\operatorname{disc} \Lambda/T')}{|(\Lambda/T)_{\mathrm{tors}}|^2}.$$

Proof. By Lemma 2.1.9 the right-hand side does not change if we replace T by T'. In that case Λ/T' is a lattice by Lemma 2.1.20. It has no torsion, so the equality follows from the short exact sequence $0 \to T' \to \Lambda \to \Lambda/T' \to 0$ of lattices. □

The following lemma will be used later to understand the intersection pairing on the free abelian group generated by the irreducible components of a fiber of an elliptic fibration.

Lemma 2.1.22 *Let S be a nonempty finite set, let G be the free abelian group on the elements of S, and let $F = \sum_{\Theta \in S} n_\Theta \Theta$ be an element of G. Let $G \times G \to \mathbb{Z}$ be a symmetric bilinear map, denoted by $(g,h) \mapsto g \cdot h$. Consider the following statements.*

- (i) *For all $\Theta, \Phi \in S$ with $\Theta \neq \Phi$ we have $\Theta \cdot \Phi \geq 0$ (effectivity hypothesis).*
- (ii) *We have $n_\Theta > 0$ for all $\Theta \in S$ and $F \cdot y = 0$ for all $y \in G$ (fiber hypothesis).*
- (ii)′ *We have $F \neq 0$ and $n_\Theta \geq 0$ for all $\Theta \in S$ and $F \cdot y = 0$ for all $y \in G$ (alternative fiber hypothesis).*
- (iii) *For all $\Theta, \Phi \in S$ with $\Theta \neq \Phi$ there is a sequence of elements $\Theta = \Psi_0, \Psi_1, \ldots, \Psi_t = \Phi$ such that $\Psi_{l-1} \cdot \Psi_l > 0$ for $1 \leq l \leq t$ (connectedness hypothesis).*
- (iv) *The greatest common divisor of the n_Θ in* (ii) *is* 1 *(simplicity hypothesis).*
- (a) *We have $y^2 \leq 0$ for all $y \in G$.*
- (b) *We have $y^2 = 0$ if and only if $ay = bF$ for some $a, b \in \mathbb{Z}$ with $a \neq 0$.*
- (c) *The group $G/\langle F \rangle$ inherits the structure of a negative definite lattice.*

Then (i), (ii)′, *and* (iii) *together imply* (ii), *while* (i) *and* (ii) *together imply* (a), *the statements* (i)–(iii) *together imply* (b), *and the statements* (i)–(iv) *together imply* (c).

Proof. For the first implication, suppose that there exists $\Theta \in S$ with $n_\Theta = 0$. Then from $F \cdot \Theta = 0$ and (i) and the fact $n_\Phi \geq 0$ for all $\Phi \in S$ we find $n_\Phi = 0$ for all $\Phi \in S$ with $\Phi \cdot \Theta > 0$. Using the same argument, by induction we find $n_\Phi = 0$ for all $\Phi \in S$ for which there exists a sequence $\Theta = \Psi_0, \Psi_1, \ldots, \Psi_t = \Phi$ as in (iii). By (iii) such a sequence exists for all $\Phi \in S$, so we find $n_\Phi = 0$ for all Φ, which contradicts (ii)′.

For the remaining implications we will follow the proof of Bombieri and Mumford, see [BM], p. 28. For a similar proof, see [Si2], Prop. III.8.2. Assume (i) and (ii), write $y = \sum a_\Theta \Theta$ with $\Theta \in S$ and $a_\Theta \in \mathbb{Z}$ and set $x_\Theta = a_\Theta / n_\Theta$. As we have $n_\Theta > 0$ and $\Theta \cdot \Phi \geq 0$ for $\Theta, \Phi \in S$ with $\Theta \neq \Phi$, the inequality $x_\Theta x_\Phi \leq \frac{1}{2}(x_\Theta^2 + x_\Phi^2)$ implies

$$\begin{aligned}
y^2 &= \sum_{\Theta, \Phi \in S} x_\Theta x_\Phi n_\Theta n_\Phi \Theta \cdot \Phi \\
&\leq \sum_\Theta x_\Theta^2 n_\Theta^2 \Theta \cdot \Theta + \sum_{\Theta \neq \Phi} \frac{1}{2} x_\Theta^2 n_\Theta n_\Phi \Theta \cdot \Phi + \sum_{\Theta \neq \Phi} \frac{1}{2} x_\Phi^2 n_\Theta n_\Phi \Theta \cdot \Phi \\
&= \sum_\Theta x_\Theta^2 n_\Theta^2 \Theta \cdot \Theta + \sum_{\Theta \neq \Phi} x_\Theta^2 n_\Theta n_\Phi \Theta \cdot \Phi = \sum_\Theta x_\Theta^2 n_\Theta \Theta \cdot F = 0.
\end{aligned}$$

Now assume also (iii). For (b), if we have equality $y^2 = 0$, then for all Θ, Φ with $\Theta \cdot \Phi \neq 0$ we have $x_\Theta = x_\Phi$. Hence for a sequence as in (iii) we find $x_\Theta = x_{\Psi_0} = \ldots = x_{\Psi_t} = x_\Phi$. Thus, we have $ay = bF$ for any $a, b \in \mathbb{Z}$ with $\frac{b}{a} = x_\Theta$ for any Θ. Finally, if we assume (iv), then $G/\langle F\rangle$ is torsion free, and thus free. As $F \cdot y = 0$ for all $y \in G$, the map $G \times G \to \mathbb{Z}$ induces a symmetric bilinear map $G/\langle F\rangle \times G/\langle F\rangle \to \mathbb{Z}$. It is nondegenerate by (b) and negative definite by (a). $\square$

Remark 2.1.23 Table 2.1 gives some examples of groups G with a map $G \times G \to \mathbb{Z}$ denoted by $(g, h) \mapsto g \cdot h$ that satisfy all assumptions and statements (i)–(iv) of Lemma 2.1.22. The first column contains the names (also called the type) of the examples for future reference. The second column states the rank of G. The third column shows a graph describing the map $G \times G \to \mathbb{Z}$. The graph contains $r = \operatorname{rk} G$ vertices. The group G is the free abelian group on these vertices. For any two vertices $\Theta \neq \Phi$ the number $\Theta \cdot \Phi$ equals the number of edges between Θ and Φ. The integers at the vertices are the coefficients n_Θ for the element $F = \sum n_\Theta \Theta$ as in Lemma 2.1.22. The self-intersection numbers Θ^2 can be computed from $F \cdot \Theta = 0$. The map $G \times G \to \mathbb{Z}$ is then uniquely determined by bilinear extension. The lattice $G/\langle F\rangle$ is isomorphic to the opposite of a standard root lattice, stated in the fourth column (see Definition 2.1.6). For a description of the notation A_n, D_n, and E_n, see [CS], § 4.6–8, or [Bo], § VI.4. For more on the occurrence of root lattices, see Remark 2.1.25. The fifth column contains the number $n^{(1)}$ of vertices Θ with $n_\Theta = 1$. This number is equal to the absolute value of the discriminant of the lattice $G/\langle F\rangle$, see [CS], Table 4.1.

The following proposition says that the examples of table 2.1 yield in fact all possible examples satisfying certain extra hypotheses. The proof is a combinatorial exercise. This Proposition is used to classify the singular fibers of elliptic surfaces. Several proofs are available, see for instance [Ko1], Thm. 6.2, or [Si2], Thm. IV.9.4, or [Ne], or [Ta3]. Some of these proofs use additional geometric hypotheses. All proofs distinguish a fair number of cases. We have included a proof different from all the above that is clean and efficient, distinguishing only a small number of cases.

Proposition 2.1.24 *Let G be the free abelian group on a nonempty finite set S with an element $F = \sum n_\Theta \Theta$ and a map $G \times G \to \mathbb{Z}$ satisfying all assumptions and statements* (i)–(iv) *of Lemma* 2.1.22*. Assume moreover that for all $\Theta \in S$ we have $\Theta^2 \geq -2$ and Θ^2 is even. Then the triple consisting of the group G, the element F, and the pairing $G \times G \to \mathbb{Z}$ is isomorphic to one of the examples given in Table* 2.1*. If we have $\#S > 1$, then $\Theta^2 = -2$ for all $\Theta \in S$.*

Proof. Let Δ be the graph on S with $\Theta \cdot \Phi$ edges between Θ and Φ if $\Theta \neq \Phi$. By a path in Δ we mean a sequence $\Psi_1, \ldots, \Psi_r$ such that $\Psi_j \cdot \Psi_{j+1} \neq 0$ for $j = 1, \ldots, r-1$ and such that $\Psi_i \neq \Psi_j$ for $i \neq j$. We will first deal with a few exceptional cases. If we have $\#S = 1$, say $S = \{\Theta\}$, then the fiber hypothesis and the simplicity hypothesis together give $F = \Theta$, so G is of type I_1. For $\#S > 1$, suppose that there are $\Theta \neq \Phi$ such that $\Theta \cdot \Phi \geq 2$. Then since we have $\Theta^2 \geq -2$, the equation $0 = F \cdot \Theta = \sum n_\Psi \Psi \cdot \Theta$ gives

$$2n_\Theta \geq -n_\Theta \Theta^2 = \sum_{\Psi \neq \Theta} n_\Psi \Psi \cdot \Theta \geq n_\Phi \Phi \cdot \Theta \geq 2n_\Phi.$$

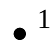
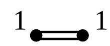
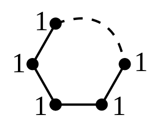
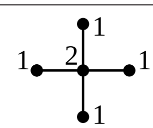
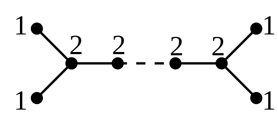
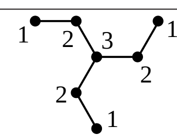
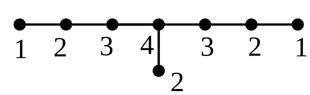
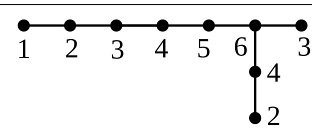
Type	$r = \operatorname{rk} G$	Configuration	$G/\langle F\rangle$	$n^{(1)}$
I_1	1		0	1
I_2	2		$A_1(-1)$	2
I_n $(n \geq 3)$	n		$A_{n-1}(-1)$	n
I_0^*	5		$D_4(-1)$	4
I_n^* $(n \geq 1)$	$n+5$		$D_{n+4}(-1)$	4
IV^*	7		$E_6(-1)$	3
III^*	8		$E_7(-1)$	2
II^*	9		$E_8(-1)$	1

Table 2.1: groups satisfying the hypotheses of Lemma 2.1.22

By symmetry we find $n_\Theta = n_\Phi$ and from equality we find $\Theta^2 = \Phi^2 = -2$ and $\Theta \cdot \Phi = 2$, and $\Psi \cdot \Theta = \Psi \cdot \Phi = 0$ for all $\Psi \neq \Theta, \Phi$. From the connectedness hypothesis we find $\#S = 2$, so G is of type I_2.

From now on, we will assume $\#S \geq 2$ and for all $\Theta, \Phi \in S$ with $\Theta \neq \Phi$ we have $\Theta \cdot \Phi \in \{0, 1\}$. For $\Phi \in S$ let $C(\Phi)$ denote the set of $\Theta \in S$ with $\Theta \cdot \Phi = 1$. We will first prove the following statements.

(A) For all $\Phi \in S$ we have $\Phi^2 = -2$.

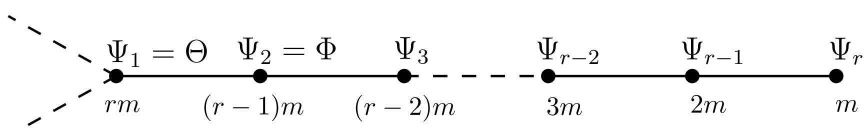
(B) For all $\Phi \in S$ we have $2n_\Phi = \sum_{\Psi \in C(\Phi)} n_\Psi$.

(C) For all $\Phi \in S$ and $\Theta \in C(\Phi)$ we have $n_\Phi \geq \frac{1}{2} n_\Theta$ with equality if and only if $C(\Phi) = \{\Theta\}$.

(D) For all $\Phi \in S$ and $\Theta \in C(\Phi)$ with $n_\Phi = n_\Theta$ we have either $C(\Phi) = \{\Theta, \Psi\}$ for some Ψ with $n_\Psi = n_\Phi$ or $C(\Phi) = \{\Theta, \Psi_1, \Psi_2\}$ for some Ψ_1, Ψ_2 with $n_{\Psi_1} = n_{\Psi_2} = \frac{1}{2} n_\Phi$. In the latter case we have $C(\Psi_i) = \{\Phi\}$ for $i = 1, 2$.

(E) For all $\Phi \in S$ and $\Theta \in C(\Phi)$ with $n_\Phi < n_\Theta < 2n_\Phi$ we have $C(\Phi) = \{\Theta, \Psi\}$ for some $\Psi \neq \Theta$ with $n_\Psi = 2n_\Phi - n_\Theta$.

(F) For all $\Phi \in S$ and $\Theta \in C(\Phi)$ with $n_\Phi < n_\Theta$ the integer $m = n_\Theta - n_\Phi$ divides n_Θ and there is a sequence $\Psi_1 = \Theta, \Psi_2 = \Phi, \Psi_3, \ldots, \Psi_r$ of $r = n_\Theta / m$ elements of S, such that $C(\Psi_j) = \{\Psi_{j-1}, \Psi_{j+1}\}$ for $j = 2, \ldots, r-1$ and $C(\Psi_r) = \{\Psi_{r-1}\}$, and $n_{\Psi_j} = (r + 1 - j)m$ for $j = 1, \ldots, r$.



To prove (A), note that by Lemma 2.1.22 we have $\Phi^2 \leq 0$ with equality if and only if $a\Phi = bF$ for some $a, b \in \mathbb{Z}$ with $a \neq 0$. From $\#S \geq 2$ and the inequality $n_\Psi > 0$ for all $\Psi \in S$, we conclude that equality does not hold, so $\Phi^2 < 0$. As we have $\Phi^2 \geq -2$ and Φ^2 is even, we get $\Phi^2 = -2$. From $F \cdot \Phi = 0$ we find $-n_\Phi \Phi^2 = \sum_{\Psi \neq \Phi} n_\Psi \Psi \cdot \Phi$, which implies the equality in (B). The statement (C) follows from (B) as all the n_Ψ are positive. For (D) and (E), suppose that we have $\Phi \in S$ and $\Theta \in C(\Phi)$ with $n_\Phi \leq n_\Theta < 2n_\Phi$. Then we find

$$2n_\Phi = n_\Theta + \sum_{\substack{\Psi \in C(\Phi) \\ \Psi \neq \Theta}} n_\Psi \geq n_\Phi + \sum_{\substack{\Psi \in C(\Phi) \\ \Psi \neq \Theta}} n_\Psi.$$

As we have $n_\Psi \geq \frac{1}{2} n_\Phi > 0$ for all $\Psi \in C(\Phi)$, there is room for at most two terms in this summation, so $\#C(\Phi) \leq 3$. If we have strict inequality $n_\Phi < n_\Theta$, then there is in fact only room for one term, which proves (E). If there is equality, then we find the two cases described in (D). The last part of (D) follows from (C).

For (F), suppose we have $\Phi \in S$ and $\Theta \in C(\Phi)$ with $n_\Phi < n_\Theta$. Set $m = n_\Theta - n_\Phi > 0$ and set $\Psi_1 = \Theta$ and $\Psi_2 = \Phi$. For notational convenience, we will write $n_j = n_{\Psi_j}$ for any j, so we have $n_1 = n_\Theta$ and $n_2 = n_\Phi$. By (C) we have $n_1 \leq 2n_2$ with equality if and only if $m = n_2$. If we have strict inequality, then by (E) there exists $\Psi_3 \in S$ such that $C(\Psi_2) = \{\Psi_1, \Psi_3\}$ and $n_3 = 2n_2 - n_1 = n_2 - m < n_2$. Repeating this argument we find that either $m = n_3$, or there exists $\Psi_4 \in S$ such that $C(\Psi_3) = \{\Psi_2, \Psi_4\}$ and $n_4 = 2n_3 - n_2 = n_3 - m < n_3$. As the n_Ψ are positive, this argument can be repeated only a finite number of times and we find a sequence $\Psi_1, \ldots, \Psi_r$ such that $C(\Psi_j) = \{\Psi_{j-1}, \Psi_{j+1}\}$ for $j = 2, \ldots, r-1$, and $n_j = n_{j-1} - m$ for $j = 2, \ldots, r$ and $n_r = m$. It follows that $m = n_r = n_1 - (r-1)m$, so $n_1 = rm$ and $n_j = (r+1-j)m$. From the equality $n_{r-1} = 2m = 2n_r$ we find $C(\Psi_r) = \{\Psi_{r-1}\}$ by (C), which proves (F).

We now continue our proof using statements (A)–(F). Set $N = \max_{\Theta \in S} n_\Theta$ and $T = \{\Theta \in S \mid n_\Theta = N\}$. Let Γ denote the full subgraph of Δ on T. Suppose we have $\Theta, \Phi \in T$. As Δ is connected by the connectedness hypothesis, there is a path $\Theta = \Psi_1, \ldots, \Psi_t = \Phi$ in Δ. Again we will write $n_j = n_{\Psi_j}$. Suppose that for some i with $1 \leq i < t$ we have $n_i \neq n_{i+1}$. By reversing the path if necessary, we may assume $n_i > n_{i+1}$. Then by (F) we find that for $j = i+2, \ldots, t$ the element Ψ_j is the unique element in $C(\Psi_{j-1}) \setminus \{\Psi_{j-2}\}$ and that we have $n_i > n_{i+1} > n_{i+2} > \ldots > n_t$, which contradicts the maximality of $n_t = n_\Phi = N$. We conclude $n_i = n_t = N$ for all i, so $\Psi_i \in T$ for all i and thus Γ is connected. From (B) it follows that the valency of any vertex in Γ is at most 2. This implies that Γ is either a cycle, or Γ is a linear graph, i.e., we can write $T = \{\Psi_1, \ldots, \Psi_n\}$ such that $\Psi_i \cdot \Psi_j = 1$ if and only if $|i - j| = 1$ for $i, j \in \{1, \ldots, n\}$. If $\Theta \in T$ has valency 2 in Γ, then by (B) the valency of Θ in Δ is also 2. Because Δ is connected, this implies that if Γ is a cycle, then Δ is a cycle as well and by the simplicity hypothesis, G is of type I_n for $n = \#S$. If Γ is a linear graph consisting of $n > 1$ vertices, then only its two endpoints can be connected to elements of $S \setminus T$. Applying (D) to these endpoints we find that G is of type I_{n-1}^*.

It remains to consider the case that Γ consists of one vertex, say Θ. Then for every $\Phi \in C(\Theta)$ we find from (F) that $m_\Phi = n_\Theta - n_\Phi > 0$ is a divisor of n_Θ. Set $r_\Phi = n_\Theta / m_\Phi \in \mathbb{Z}_{\geq 2}$ for all $\Phi \in C(\Theta)$. Then we get $n_\Phi / n_\Theta = 1 - (r_\Phi)^{-1}$ and (B) yields $2 = \sum_{\Phi \in C(\Theta)} (1 - r_\Phi^{-1})$. The only solutions to this equation with $r_\Phi \in \mathbb{Z}_{\geq 2}$ are

$$(r_\Phi)_\Phi \in \{(2,3,6), (2,4,4), (3,3,3), (2,2,2,2)\}.$$

Suppose we have $(r_\Phi)_\Phi = (2,3,6)$. Then by (F) there are three paths starting at Θ of length 2, 3, and 6 respectively. Furthermore, it follows that no vertex outside these paths is connected by an edge in Δ to a vertex in these paths, except perhaps to Θ. As $C(\Theta)$ is contained in these paths and Δ is connected, we find that there are no vertices in Δ outside these paths. From the simplicity hypothesis we find that G is uniquely determined and of type II^*. The other three solutions yield type III^*, IV^*, and I_0^* respectively. $\square$

Remark 2.1.25 Let G be the free abelian group on a finite set S with a map $G \times G \to \mathbb{Z}$ satisfying all assumptions and statements (i)–(iv) of Lemma 2.1.22. Let $F \in G$ be the element as described in statement (ii) of that lemma. Then by Lemma 2.1.22 the group $G/\langle F\rangle$ inherits the structure of a negative definite lattice. Assume moreover that for all $\Theta \in S$ we have $\Theta^2 \geq -2$ and Θ^2 is even. Then by Proposition 2.1.24 the lattice $G/\langle F\rangle$ is either 0 or all $\Theta \in S$ satisfy $\Theta^2 = -2$. Suppose the latter case holds. Then for every $\Theta \in S$ the reflection $x \mapsto x - 2\frac{x\cdot\Theta}{\Theta^2}\Theta$ of $G_{\mathbb{Q}}$ in the hyperplane orthogonal to Θ takes G to G. It induces an automorphism of $G/\langle F\rangle$ and thus Θ is a root of $G/\langle F\rangle$. Therefore, $G/\langle F\rangle$ is generated by roots and so is its opposite lattice (see Definition 2.1.6), which is positive definite. By definition this means that this opposite lattice is a root lattice, so it is not a coincidence that all lattices in the fourth column of Table 2.1 are opposites of root lattices. The fact that these lattices are root lattices also explains the relation between the graphs in the third column of Table 2.1 and extended Dynkin diagrams. Root lattices and (extended) Dynkin diagrams have been classified and studied extensively, see for instance [CS], § 4.2 and 21.3, and [Bo], Chapter VI. For more about the relation between these groups G as in Lemma 2.1.22 and root lattices and extended Dynkin diagrams, see [Mir], § I.6.

2.2 Algebraic geometry prerequisites

In this section we will recall the definitions of the divisor group, the Picard group, and the Néron-Severi group of an algebraic variety. We will state a few results that will be of use later.

Definition 2.2.1 *For any scheme X, the* Picard group $\operatorname{Pic} X$ *is the group of isomorphism classes of line bundles on X.*

As in [Ha2], Section II.6, denote the following condition by (*).

(*) X is a noetherian integral separated scheme which is regular in codimension one.

Definition 2.2.2 *Let X satisfy (*) and let $K(X)$ denote the function field of X. Then as in* [Ha2]*, Section* II.6*, the* divisor group $\operatorname{Div} X$ *is the free abelian group generated by prime Weil divisors. The group of* principal Weil divisors *on X is the image of the map $K(X)^* \to \operatorname{Div} X$ sending a function f to the divisor $(f) = \sum_Y v_Y(f)Y$, where the sum is over all prime Weil divisors Y and $v_Y(f)$ is the valuation of f in the discrete valuation ring associated to the generic point of Y. The cokernel* $\operatorname{Cl} X \cong \operatorname{Div} X/(\operatorname{im} K(X)^*)$ *is the* divisor class group *of X. Also as in* [Ha2]*, Section* II.6*, the* Cartier divisor group $\operatorname{Div}_{\mathrm{Ca}} X$ *is the group $H^0(X, \mathcal{K}_X^*/\mathcal{O}_X^*)$, where $\mathcal{K}_X$ is the constant sheaf associated to $K(X)$. The group of* principal Cartier divisors *on X is the image of the map $H^0(X, \mathcal{K}^*) \to H^0(X, \mathcal{K}_X^*/\mathcal{O}_X^*)$. The cokernel is denoted* $\operatorname{Cl}_{\mathrm{Ca}} X$ *and called the* Cartier divisor class group *of X.*

Proposition 2.2.3 *If X satisfies (*) and X is also locally factorial, then there are natural isomorphisms* $\operatorname{Div} X \cong \operatorname{Div}_{\mathrm{Ca}} X$ *and* $\operatorname{Cl} X \cong \operatorname{Cl}_{\mathrm{Ca}} X \cong \operatorname{Pic} X$.

Proof. See [Ha2], Prop. II.6.11 and II.6.15 and Cor. II.6.16. □

Remark 2.2.4 Note that any regular scheme is locally factorial, so Proposition 2.2.3 applies in particular to regular noetherian integral separated schemes. In this case, we will just talk about divisors without specifying 'Weil' or 'Cartier'. In general, if we leave out this specification, a divisor will mean a Weil divisor.

For more details about the Picard group and the divisor class groups, see [Ha2], Section II.6. We will now focus on the case that X is a variety. Note that we don't require a variety to be irreducible or reduced.

Definition 2.2.5 *Let k be a field. A* variety *over k is a separated scheme X that is of finite type over* $\operatorname{Spec} k$. *We say that X is* smooth *if the morphism $X \to \operatorname{Spec} k$ is smooth. A variety has* pure dimension d *if all its irreducible components have dimension d. A* curve *or a* surface *is a variety of pure dimension* 1 *or* 2 *respectively.*

Remark 2.2.6 Note that this definition is different from the definition in [Ha2], p. 105, where varieties are also assumed to be integral.

The following definition, proposition and corollary are copied from Bjorn Poonen's notes on rational points on varieties. For equivalent definitions, see [FJ], § 9.2.

Definition 2.2.7 *A field extension L of k is* separable *if the ring $L \otimes_k k'$ is reduced for all field extensions k' of k. A field extension L of k is* primary *if the largest separable algebraic extension of k contained in L is k itself.*

Proposition 2.2.8 *Let X be a variety over k with function field $K(X)$. Then the following statements hold.*

(i) *The variety X is geometrically irreducible if and only if X is irreducible and the field extension $K(X)$ of k is primary.*
(ii) *The variety X is geometrically reduced if and only if X is reduced and for each irreducible component Z of X, the field extension $K(Z)$ of k is separable.*

Proof. For (i), see [EGA IV(2)], Prop. 4.5.9. For (ii), see [EGA IV(2)], Prop. 4.6.1. □

Corollary 2.2.9 *Let X be an integral variety over a field k and let k' denote the maximal algebraic extension of k inside $K(X)$. Then the following conditions hold.*

(i) *If X is geometrically integral, then $k' = k$.*
(ii) *If X is proper, then $\mathcal{O}_X(X) \subset k'$.*
(iii) *If X is regular, then $k' \subset \mathcal{O}_X(X)$.*

Proof. Assume X is geometrically integral. By Proposition 2.2.8, part (i), the extension $K(X)$ of k is primary. Therefore, so is the subextension k' of k. By part (ii) of the same proposition, the extension k' of k is also separable. Any primary separable algebraic extension of a field is trivial, which proves (i). Suppose X is proper. Then every element $f \in \mathcal{O}_X(X)$ is algebraic over k, see [Ha2], Thm. I.3.4. This proves (ii). Suppose X is regular. As any regular local ring is integrally closed, we find that $\mathcal{O}_X(X) = \bigcap_{x \in X} \mathcal{O}_{X,x}$ (see [Ha2], Prop. II.6.3A) is integrally closed as well. As we have $k \subset \mathcal{O}_X(X)$, we also have $k' \subset \mathcal{O}_X(X)$. □

Corollary 2.2.10 *Let X be a projective, geometrically integral, regular variety over a field k with function field $K(X)$. Then we have an exact sequence*

$$0 \to k^* \to K(X)^* \to \operatorname{Div} X \to \operatorname{Pic} X \to 0.$$

Proof. By Proposition 2.2.3, all that needs to be checked is exactness at $K(X)^*$. Let k' denote the algebraic closure of k within $K(X)$. For any $f \in K(X)^*$, the divisor (f) is 0 if and only if we have $f \in \mathcal{O}_{X,x}^*$ for all generic points $x \in X$ associated to prime divisors. Hence, we find $f \in \bigcap_{x \in X} \mathcal{O}_{X,x}^* = \mathcal{O}_X(X)^*$, see [Ha2], Prop. II.6.3A. From Corollary 2.2.9 we find $\mathcal{O}_X(X) = k$. □

For the remainder of this section, let X be a smooth, projective, geometrically integral variety over a field k.

Definition 2.2.11 *The group* $\operatorname{Div}^0 X$ *is the subgroup of* $\operatorname{Div} X$ *generated by all divisors that become algebraically equivalent to* 0 *after a base change to the algebraic closure* $\overline{k}$. *The image of* $\operatorname{Div}^0 X$ *in* $\operatorname{Pic} X$ *is denoted by* $\operatorname{Pic}^0 X$. *The* Néron-Severi group $\operatorname{NS}(X)$ *of* X *is the quotient* $\operatorname{Pic} X / \operatorname{Pic}^0 X$.

For a precise definition of algebraic equivalence, see [Ha2], exc. V.1.7, which is stated only for smooth surfaces, but holds in any dimension, see [SGA 6], Exp. XIII, p. 644, 4.4. We will write $D \sim D'$ and $D \approx D'$ to indicate that two divisors D and D' are linearly and algebraically equivalent respectively.

Proposition 2.2.12 *The Néron-Severi group* $\operatorname{NS}(X)$ *of* X *is a finitely generated abelian group.*

Proof. See [Ha2], exc. V.1.7–8, or [Mi2], Thm. V.3.25 for surfaces, or [SGA 6], Exp. XIII, Thm. 5.1 in general. □

Definition 2.2.13 *The rank* $\rho = \operatorname{rk} \operatorname{NS}(X) = \dim_{\mathbb{Q}} \operatorname{NS}(X) \otimes \mathbb{Q}$ *is called the* Picard number *of* X. *The rank of* $\operatorname{NS}(X_{\overline{k}})$ *is called the* geometric Picard number *of* X.

Remark 2.2.14 For a smooth, projective, geometrically integral curve Y the group $\operatorname{Pic}^0(Y)$ coincides with the group of divisor classes of degree 0, so then $\operatorname{NS}(Y) \cong \mathbb{Z}$.

Remark 2.2.15 Let $f\colon Z \to Y$ be a morphism between varieties over a field k. Then there is an induced homomorphism $\operatorname{Pic} Y \to \operatorname{Pic} Z$. Suppose that f is dominant and that Z and Y are geometrically integral. Let $\mathcal{K}_Z$ and $\mathcal{K}_Y$ denote the constant sheaves associated to the function fields $K(Z)$ and $K(Y)$ on Z and Y respectively. Then we have an injection of function fields $K(Y) \hookrightarrow K(Z)$, which induces another homomorphism $\operatorname{Div}_{\mathrm{Ca}} Y = H^0(Y, \mathcal{K}_Y^*/\mathcal{O}_Y^*) \to H^0(Z, \mathcal{K}_Z^*/\mathcal{O}_Z^*) = \operatorname{Div}_{\mathrm{Ca}} Z$. Suppose finally that Z and Y are smooth and projective as well. Then by Remark 2.2.4 this last homomorphism yields a homomorphism $\operatorname{Div} Y \to \operatorname{Div} Z$. It restricts to a homomorphism $\operatorname{Div}^0 Y \to \operatorname{Div}^0 Z$. It also sends effective divisors to effective divisors. All these homomorphisms are compatible with each other and thus we also obtain homomorphisms $\operatorname{Pic}^0 Y \to \operatorname{Pic}^0 Z$ and $\operatorname{NS}(Y) \to \operatorname{NS}(Z)$. By abuse of notation, all these homomorphisms are denoted by f^*.

For the next definition, see also [SGA 6], Exp. XIII, p. 644, 4.4.

Definition 2.2.16 *Let* $\operatorname{Pic}^{\mathrm{n}} X$ *denote the subgroup of all divisor classes numerically equivalent to* 0*, i.e., represented by a divisor* D *with* $D \cdot C = 0$ *for all irreducible curves on* X*. Also set*

$$\operatorname{Pic}^t X = \{z \in \operatorname{Pic} X \ : \ mz \in \operatorname{Pic}^0 X \text{ for some } m \in \mathbb{Z}_{>0}\}.$$

Proposition 2.2.17 *Algebraic equivalence implies numerical equivalence. We have*

$$\operatorname{Pic}^0 X \subset \operatorname{Pic}^t X = \operatorname{Pic}^{\mathrm{n}} X.$$

The group $\operatorname{Pic} X / \operatorname{Pic}^{\mathrm{n}} X$ *of divisor classes modulo numerical equivalence is a finitely generated free abelian group, isomorphic to* $\operatorname{NS}(X)/\operatorname{NS}(X)_{\mathrm{tors}}$.

Proof. For the first statement, see [SGA 6], Exp. X, p. 537, Déf. 2.4.1, and p. 546, Cor. 4.5.3. Hence we get a series of inclusions $\operatorname{Pic}^0 X \subset \operatorname{Pic}^t X \subset \operatorname{Pic}^{\mathrm{n}} X$. For the fact that the second inclusion is an equality, see [Ha1], Prop. 3.1, and [Mu], Thm. 4. The last statement now follows from Proposition 2.2.12. □

Now assume $k = \mathbb{C}$. Then we can consider the complex analytic space X_h associated to X. Its topological space has underlying set $X(\mathbb{C})$. Together with its structure sheaf $\mathcal{O}_{X_h}$ it forms a ringed space. The exponential function gives an exact sequence

$$0 \to \mathbb{Z} \to \mathcal{O}_{X_h} \to \mathcal{O}_{X_h}^* \to 0$$

of sheaves. Serre (see [GAGA]) showed that there are isomorphisms $H^i(X_h, \mathcal{O}_{X_h}) \cong H^i(X, \mathcal{O}_X)$ for all i and similar isomorphisms for $\mathcal{O}_X^*$. As we have an isomorphism $H^1(X, \mathcal{O}_X^*) \cong \operatorname{Pic} X$, the long exact sequence yields

$$0 \to H^1(X_h, \mathbb{Z}) \to H^1(X, \mathcal{O}_X) \to \operatorname{Pic} X \to H^2(X_h, \mathbb{Z}) \to H^2(X, \mathcal{O}_X) \to \cdots . \tag{2.1}$$

The image of $H^1(X, \mathcal{O}_X)$ in $\operatorname{Pic} X$ is exactly $\operatorname{Pic}^0 X$, see [Ha2], App. B, p. 447. The elements of $\operatorname{Pic}^0 X \cong H^1(X, \mathcal{O}_X)/H^1(X_h, \mathbb{Z})$ correspond to the $\mathbb{C}$-points on the Picard variety of X, which is an abelian variety.

Proposition 2.2.18 *The Néron-Severi group* $\mathrm{NS}(X)$ *is isomorphic to a subgroup of* $H^2(X_h,\mathbb{Z})$ *and the second Betti number* $b_2 = \dim_{\mathbb{Q}} H^2(X_h,\mathbb{Z}) \otimes \mathbb{Q} = \dim H^2(X_h,\mathbb{C})$ *is an upper bound for the Picard number of* X*.*

Proof. This follows directly from (2.1) and the fact that $\mathrm{Pic}^0 X$ is the image of the map $H^1(X,\mathcal{O}_X) \to \mathrm{Pic}\, X$. $\square$

Remark 2.2.19 For smooth projective varieties in characteristic p there is a result similar to Proposition 2.2.18, where we use étale cohomology instead, see section 2.6.

The next proposition gives a sharper upper bound for the Picard number of X, still defined over $\mathbb{C}$. Note that we have the Hodge decomposition

$$H^2(X_h,\mathbb{C}) \cong \bigoplus_{p+q=2} H^q(X_h, \bigwedge^p \Omega_{X_h}),$$

where complex conjugation induces an isomorphism $H^q(X_h, \bigwedge^p \Omega_{X_h}) \cong H^p(X_h, \bigwedge^q \Omega_{X_h})$, see [BPV], Cor. I.13.3, for surfaces and [GH], p. 116, for any dimension.

Proposition 2.2.20 *The homomorphism* $\mathrm{Pic}\, X \to H^2(X_h,\mathbb{Z})$ *in* (2.1) *induces a natural homomorphism* $\varphi\colon \mathrm{NS}(X) \to H^2(X_h,\mathbb{C})$*. The kernel of* φ *is finite and the image of* φ *is contained in* $H^1(X_h,\Omega_{X_h})$*.*

Proof. The map φ is the composition of the injection $\mathrm{NS}(X) \hookrightarrow H^2(X_h,\mathbb{Z})$ and the homomorphism $H^2(X_h,\mathbb{Z}) \to H^2(X_h,\mathbb{C})$, which has kernel $H^2(X_h,\mathbb{Z})_{\mathrm{tors}}$. As $H^2(X_h,\mathbb{Z})$ is finitely generated, its torsion subgroup is finite and hence φ has finite kernel. From the long exact sequence (2.1) we find that the image of $\mathrm{Pic}\, X$ in $H^2(X_h,\mathbb{Z})$ is the kernel of the homomorphism $H^2(X_h,\mathbb{Z}) \to H^2(X,\mathcal{O}_X)$. This map factors as

$$H^2(X_h,\mathbb{Z}) \to H^2(X_h,\mathbb{C}) \to H^2(X_h, \bigwedge^0 \Omega_{X_h}) \cong H^2(X,\mathcal{O}_X),$$

where the second map is the natural projection coming from the Hodge decomposition. It follows that the image of $\mathrm{Pic}\, X$ in $H^2(X_h,\mathbb{C})$, i.e., the image of φ, is contained in $H^2(X_h, \bigwedge^2 \Omega_{X_h}) \oplus H^1(X_h,\Omega_{X_h})$. As the image of φ is invariant under complex conjugation acting on the coefficients $\mathbb{C}$ in $H^2(X_h,\mathbb{C})$, we find that the image of φ is in fact contained in $H^1(X_h,\Omega_{X_h})$. $\square$

Corollary 2.2.21 *The Picard number of* X *is at most* $\dim H^1(X_h,\Omega_{X_h})$*.*

Proof. As the kernel of φ in Proposition 2.2.20 is finite, we find

$$\dim_{\mathbb{Q}} \mathrm{NS}(X) \otimes \mathbb{Q} = \dim_{\mathbb{Q}} \mathrm{im}\,(\varphi) \otimes \mathbb{Q} = \dim_{\mathbb{C}} \mathrm{im}\,(\varphi) \otimes \mathbb{C}.$$

By Proposition 2.2.20 this dimension is at most $\dim H^1(X_h,\Omega_{X_h})$. $\square$

We will no longer assume $k = \mathbb{C}$ and restrict our attention to surfaces. Let X be a smooth, projective, geometrically integral surface. In that case we can define the intersection number $D \cdot D'$ of two divisors D and D', see [Ha2], Thm. V.1.1. It gives a symmetric bilinear map $\operatorname{Pic} X \times \operatorname{Pic} X \to \mathbb{Z}$. As any two algebraically equivalent divisors are also numerically equivalent, this pairing induces a symmetric bilinear map $\mathrm{NS}(X) \times \mathrm{NS}(X) \to \mathbb{Z}$. If X is defined over $\mathbb{C}$, then this map commutes with the cup-product $H^2(X_h, \mathbb{Z}) \times H^2(X_h, \mathbb{Z}) \to \mathbb{Z}$.

Definition 2.2.22 *A* K3 surface *is a smooth, projective, geometrically integral surface X with irregularity $q = \dim H^1(X, \mathcal{O}_X) = 0$ on which the canonical sheaf is trivial.*

Remark 2.2.23 Note that by our definition all surfaces, in particular K3 surfaces, are algebraic.

Remark 2.2.24 As the second Betti number b_2 of a K3 surface X equals $b_2 = 22$ (see [BPV], Prop. VIII.3.2 for characteristic 0 and [BM], Thm. 5, for characteristic $p > 0$), we find from Proposition 2.2.18 and Remark 2.2.19 that the Picard number $\rho = \operatorname{rk} \mathrm{NS}(X)$ of a K3 surface is at most 22. In characteristic 0, we even have $\rho \leq \dim H^1(X_h, \Omega) = 20$ by Corollary 2.2.21. If this maximum 20 is met, we call X a *singular K3 surface*.

Definition 2.2.25 *We define the* K3 lattice L_{K3} *to be the even unimodular lattice* $L_{\mathrm{K3}} = E_8(-1) \oplus E_8(-1) \oplus U \oplus U \oplus U$*, where* $E_8(-1)$ *is the opposite of the standard root lattice* E_8 *(see Definition* 2.1.6 *and* [CS], § 4.8.1*, or* [Bo], § VI.4*), and* U *is the* 2*-dimensional lattice with Gram matrix*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Lemma 2.2.26 *Let X be a K3 surface over $\mathbb{C}$. Then the group $H^2(X_h, \mathbb{Z})$ together with the cup-product $H^2(X_h, \mathbb{Z}) \times H^2(X_h, \mathbb{Z}) \to \mathbb{Z}$ has the structure of an even lattice isomorphic to L_{K3}. The embedding $\mathrm{NS}(X) \hookrightarrow H^2(X_h, \mathbb{Z})$ makes $\mathrm{NS}(X)$ into a primitive sublattice of $H^2(X_h, \mathbb{Z})$.*

Proof. For the fact that $H^2(X_h, \mathbb{Z})$ is torsion-free and isomorphic to L_{K3}, see [BPV], Prop. VIII.3.2. Because $H^2(X_h, \mathbb{Z})$ is torsion-free, the map $H^2(X_h, \mathbb{Z}) \to H^2(X_h, \mathbb{C})$ is injective and the Néron-Severi group $\mathrm{NS}(X)$ is isomorphic to its image in $H^2(X_h, \mathbb{C})$. This image is equal to $H^1(X_h, \Omega) \cap H^2(X_h, \mathbb{Z})$, where the intersection is taken in $H^2(X_h, \mathbb{C})$, see [BPV], p. 120. Hence, $\mathrm{NS}(X)$ is a primitive sublattice of $H^2(X_h, \mathbb{Z})$. □

Remark 2.2.27 Let X be a K3 surface over $\mathbb{C}$. By lemma 2.2.26 the group $H^2(X_h, \mathbb{Z})$ is torsion-free and thus, so is the Néron-Severi group $\mathrm{NS}(X)$. By Proposition 2.2.17 this implies that algebraic equivalence is the same as numerical equivalence. As we have $\dim H^1(X, \mathcal{O}_X) = 0$, we also find that $\operatorname{Pic}^0 X$ is trivial. Therefore, there is an isomorphism $\operatorname{Pic} X \cong \mathrm{NS}(X)$ and algebraic and numerical equivalence are in fact the same as linear equivalence on complex K3 surfaces. The same holds for K3 surfaces in positive characteristic, see [BM], Thm. 5.

2.3 Definition of elliptic surfaces

Before going into the theory of elliptic surfaces in the next section, we will elaborate on the definition. In this section, we will also state a few preliminary results and a theorem that gives equivalent conditions for an elliptic fibration to be relatively minimal.

Throughout this section, k will denote an algebraically closed field. All varieties, unless stated otherwise, are k-varieties.

Definition 2.3.1 *A* fibration *of a variety* Y over *a regular integral curve* Z *over* k *is a dominant morphism* $g\colon Y \to Z$.

Remark 2.3.2 If Y is integral in the definition above, then g is flat, see [Ha2], Prop. III.9.7. If also the characteristic of k equals 0 and the singular locus of Y is contained in finitely many fibers, then almost all fibers are nonsingular, see [Ha2], Thm. III.10.7. If Y is projective, then g is surjective, as projective morphisms are closed.

Lemma 2.3.3 *Let* $g\colon Y \to Z$ *be a fibration of a proper surface* Y *over a regular, proper, integral curve* Z. *Let* D *be a prime divisor of* Y. *Then the induced morphism* $g|_D\colon D \to Z$ *is either constant or surjective.*

Proof. Since Y and Z are proper over k, the morphism g is proper, and therefore g a closed map. As D is an irreducible closed subscheme of Y, this means that $g(D)$ is an irreducible closed subset of Z. Since Z is a curve, this implies that $g(D)$ is equal to just a closed point or to Z. □

Definition 2.3.4 *Let* $g\colon Y \to Z$ *be as in Lemma* 2.3.3. *Then a divisor* D *on* Y *is called* fibral *or* vertical *if for all its irreducible components* D' *the restriction* $g|_{D'}$ *is constant. If* $g|_{D'}$ *is surjective for all irreducible components* D' *of* D, *then* D *is called* horizontal. *The subgroup of* $\operatorname{Div} Y$ *generated by vertical (resp. horizontal) divisors is denoted* $\operatorname{Div}_{\mathrm{vert}} S$ *(resp.* $\operatorname{Div}_{\mathrm{hor}} S$*).*

Remark 2.3.5 It follows from Lemma 2.3.3 that $\operatorname{Div} S$ is the direct sum of $\operatorname{Div}_{\mathrm{vert}} S$ and $\operatorname{Div}_{\mathrm{hor}} S$.

Definition 2.3.6 *Let* Z *be a smooth, projective, irreducible curve. A fibration of a smooth, projective, irreducible surface* Y *over* Z *is called* relatively minimal *if for every fibration of a smooth, projective, irreducible surface* Y' *over* Z, *every* Z*-birational morphism* $Y \to Y'$ *is necessarily an isomorphism.*

Theorem 2.3.7 *Let* Y *be a smooth, projective, irreducible surface,* Z *a smooth, projective, irreducible curve, and let* $g\colon Y \to Z$ *be a fibration such that no fiber contains an exceptional prime divisor* E, *i.e., a prime divisor with self-intersection number* $E^2 = -1$ *and* $H^1(E, \mathcal{O}_E) = 0$. *Then* g *is a relatively minimal fibration.*

Proof. This is a direct corollary of the Castelnuovo Criterion ([Ch], Thm. 3.1) and the Minimal Models Theorem ([Ch], Thm. 1.2). See also Lichtenbaum [Lic] and Shafarevich [Sha]. □

Lemma 2.3.8 *Let $g\colon X \to Y$ be a projective morphism of noetherian schemes. Assume that X is integral and that g has a section. Then there is an isomorphism $g_*\mathcal{O}_X \cong \mathcal{O}_Y$ if and only if for every $y \in Y$ the fiber X_y is connected.*

Proof. Set $Y' = \mathbf{Spec}\, g_*\mathcal{O}_X$. By Stein factorization (see [Ha2], Cor. III.11.5) the morphism g factors naturally as $g = h \circ f$, where $f\colon X \to Y'$ is projective with connected fibers and $h\colon Y' \to Y$ is finite. If we have $g_*\mathcal{O}_X \cong \mathcal{O}_Y$, then h is an isomorphism, so g has connected fibers. Conversely, suppose g has connected fibers. As f is projective, it is closed. If f were not surjective, then there would be a nonempty open affine $V \subset Y'$ with $f^{-1}(V) = \emptyset$. This implies $(f_*\mathcal{O}_X)(V) = 0$, contradicting the equality $f_*\mathcal{O}_X = \mathcal{O}_{Y'}$. We conclude that f is surjective, so h also has connected fibers. As h is finite, its fibers are also totally disconnected (see [Ha2], exc. II.3.5), so h is injective on topological spaces. Let $\varphi\colon Y \to X$ be a section of g. Then $\psi = f \circ \varphi$ is a section of h. Every injective continuous map between topological spaces that has a continuous section is a homeomorphism, so h is a homeomorphism. Therefore, to prove that h is an isomorphism, it suffices to show this locally, so we may assume $Y' = \operatorname{Spec} B$ and $Y = \operatorname{Spec} A$. The composition $\psi^\# \circ h^\#\colon A \to B \to A$ is the identity, so $\psi^\#$ is surjective. As X is integral, so is Y'. Hence, the ideal $(0) \subset B$ is prime. Since ψ is surjective, there is a prime ideal $\mathfrak{p} \subset A$ such that $(0) = \psi(\mathfrak{p}) = (\psi^\#)^{-1}\mathfrak{p}$, so $\psi^\#$ is injective. We find that $\psi^\#$ is an isomorphism. Hence, so are ψ and h, so there is an isomorphism $g_*\mathcal{O}_X \cong \mathcal{O}_Y$. □

Definition 2.3.9 *A fibration is called* elliptic *if all but finitely many fibers are smooth, geometrically irreducible curves of genus* 1.

Theorem 2.3.10 *Let C be a smooth, irreducible, projective curve of genus $g(C)$ over an algebraically closed field k. Let S be a smooth, irreducible, projective surface over k with Euler characteristic $\chi = \chi(\mathcal{O}_S)$ and let $g\colon S \to C$ be an elliptic fibration that has a section. Then the following are equivalent.*

(i) *The morphism g is a relatively minimal fibration,*
(ii) *There is a divisor L on C of degree χ, such that any canonical divisor K_S on S is linearly equivalent to $g^*(K_C + L)$, where K_C is a canonical divisor on C.*
(iii) *Any canonical divisor K_S on S is algebraically equivalent to $(2g(C) - 2 + \chi)F$, where F is any fiber of g,*
(iv) *We have $K_S^2 = 0$.*

Proof. (i) ⇒ (ii). Almost all fibers are irreducible and thus connected. By Remark 2.3.2 the morphism g is flat, so by the principle of connectedness, *all* fibers are connected, see [Ha2], exc. III.11.4. From Lemma 2.3.8 we find that $g_*\mathcal{O}_S \cong \mathcal{O}_C$. Under that assumption, an explicit expression for K_S can be given, see [Ko1], § 12, for base fields of characteristic 0, and [BM], § 1, for characteristic $p > 0$. Since g has a section, say $\mathcal{O}$, every fiber of g will have intersection multiplicity 1 with the horizontal divisor $\mathcal{O}(C)$, so there are no multiple fibers. In that case, the expression mentioned above implies that K_S is linearly equivalent to $g^*(K_C + L)$ for some divisor L on C of degree χ.

(ii) $\Rightarrow$ (iii). The divisor $K_C + L$ has degree $2g(C) - 2 + \chi$, so it is algebraically equivalent to $(2g(C) - 2 + \chi)P$ for any point P on C. Hence, the divisor $g^*(K_C + L)$ is algebraically equivalent to $(2g(C) - 2 + \chi)F$ for any fiber F.

(iii) $\Rightarrow$ (iv). Since F is algebraically equivalent to any other fiber F', it is also numerically equivalent to any other fiber F'. Thus we get $F^2 = F \cdot F' = 0$, so $K_S^2 = 0$.

(iv) $\Rightarrow$ (i). Suppose g were not relatively minimal. Then the Minimal Models Theorem (see [Ch], Thm. 1.2) tells us that there would be a relatively minimal fibration $g' \colon S' \to C$ of a smooth, irreducible, projective surface S' and a C-morphism $\gamma \colon S \to S'$ which consists of a nonempty sequence of blow-ups of points. Then g' is an elliptic fibration as well. The composition $\gamma \circ \mathcal{O}$ is a section of g'. By the proven implication (i) $\Rightarrow$ (iii), we find that $K_{S'}^2 = 0$. This implies $K_S^2 < 0$, because for any blow-up $Z \to Z'$ of a nonsingular projective surface Z' in a point P, we have $K_Z^2 = K_{Z'}^2 - 1$, see [Ha2], Prop. V.3.3. From this contradiction, we conclude that g is relatively minimal. $\square$

The following definition states that if the fibration g as described in Theorem 2.3.10 is not smooth, then we call the quadruple $(S, C, g, \mathcal{O})$ an *elliptic surface*. Recall that throughout this section k is assumed to be algebraically closed.

Definition 2.3.11 *Let C be a smooth, irreducible, projective curve over k. An* elliptic surface *over C is a smooth, irreducible, projective surface S over k together with a relatively minimal elliptic fibration $g \colon S \to C$ that is* **not smooth***, and a section $\mathcal{O} \colon C \to S$ of g.*

Remark 2.3.12 In order to rephrase what it means for g not to be smooth, note that by [EGA IV(2)], Déf. 6.8.1, a morphism of schemes $g \colon X \to Y$ is smooth if and only if g is flat, g is locally of finite presentation, and for all $y \in Y$ the fiber $X_y = X \times_Y \operatorname{Spec} k(y)$ over the residue field $k(y)$ is geometrically regular. See also [Ha2], Thm. III.10.2.

In the case that g is a fibration of an integral variety X over a smooth, irreducible, projective curve over an algebraically closed field k, it follows from Remark 2.3.2 that g is flat. As X is noetherian and of finite type over k, it also follows that g is locally of finite presentation. Hence g not being smooth is then equivalent to the existence of a singular fiber.

For the rest of this section, let S be an elliptic surface over a smooth, irreducible, projective curve C over k, fibered by $g \colon S \to C$ with a section $\mathcal{O}$. Let $K = k(C)$ denote the function field of C and let $\eta \colon \operatorname{Spec} K \to C$ be its generic point. Then the generic fiber $E = S \times_C \operatorname{Spec} K$ of g is a curve over K of genus 1. The curve E/K is smooth because g is flat and projective, see [Ha2], exercise III.10.2. The curve E/K is projective because being projective is stable under base extension, see [Ha2], exercise II.4.9. Let ξ denote the natural map $E \to S$.

$$\begin{tikzcd} E \arrow[r, "\xi"] \arrow[d] & S \arrow[d, "g"] \\ \operatorname{Spec} K \arrow[r, "\eta"'] & C \end{tikzcd} \tag{2.2}$$

Lemma 2.3.13 *Both maps ξ_* and η^* in*

$$E(K) = \operatorname{Hom}_K(\operatorname{Spec} K, E) \xrightarrow{\xi_*} \operatorname{Hom}_C(\operatorname{Spec} K, S) \xleftarrow{\eta^*} \operatorname{Hom}_C(C, S) = S(C)$$

are bijective.

Proof. By the universal property of fibered products, we find that every morphism $\sigma\colon \operatorname{Spec} K \to S$ with $g \circ \sigma = \eta$ comes from a unique section of the morphism $E \to \operatorname{Spec} K$. Hence, the map ξ_* is bijective. As C is a smooth curve and S is projective, any morphism from a dense open subset of C to S extends uniquely to a morphism from C, see [Ha2], Prop. I.6.8. As $\operatorname{Spec} K$ is dense in C, the map η^* is bijective as well. □

Whenever we implicitly identify the two sets $E(K)$ and $S(C)$, it will be done using the bijection $\xi_*^{-1} \circ \eta^*$ of Lemma 2.3.13. The section $\mathcal{O}$ of g corresponds to a point on E, which we will also denote by $\mathcal{O}$. It gives E the structure of an elliptic curve. This endows $E(K)$ with a group structure, which carries over to $S(C)$, see [Si1], Prop. III.3.4.

For any $P \in E(K) \cong S(C)$, let $(P)_E$ and $(P)_S$ denote the prime divisor corresponding to the image of P on E and S respectively. We will leave out the indices E and S if it is clear from the context which is meant. We will now deduce some useful intersection multiplicities on S. By definition any two fibers F and F' of g are algebraically equivalent. Hence, if F is any fiber and Θ is any irreducible component of a fiber, then we have $F \cdot \Theta = 0$, as we may replace F by any fiber F' that is disjoint from Θ. Let $P \in S(C)$ be any section of g. As the divisor $(P) = (P)_S$ meets all fibers of g only once, we find $(P) \cdot F = 1$ for any fiber F. For any irreducible component Θ of a fiber we have $(P) \cdot \Theta = 1$ or 0 depending on whether (P) does or does not intersect Θ. If D is a divisor on C of degree d, then we have $g^*(D) \cdot (P) = d$, as every point on C pulls back under g^* to a whole fiber on S. If $g(C)$ denotes the genus of $C \cong P(C)$ and $\chi = \chi(\mathcal{O}_S)$ denotes the Euler characteristic of S, then according to Theorem 2.3.10, the adjunction formula (see [Ha2], Prop. V.1.5) gives

$$2g(C) - 2 = (P) \cdot ((P) + K) = (P)^2 + (2g(C) - 2 + \chi)(P) \cdot F = (P)^2 + 2g(C) - 2 + \chi,$$

so we find $(P)^2 = -\chi$. The following proposition tells us that this number $(P)^2$ is negative.

Proposition 2.3.14 *The Euler characteristic $\chi = \chi(\mathcal{O}_S)$ of an elliptic surface is positive.*

Proof. See [Og]. □

2.4 Shioda's theory of elliptic surfaces

We will phrase Shioda's theory of elliptic surfaces [Shi3] in a scheme-theoretic language. We will show that the Néron-Severi group of an elliptic surface is a free abelian group that can be given the structure of a lattice by the intersection pairing. We will then prove the following main theorem which implies that the Mordell-Weil group of the generic fiber of an elliptic surface is finitely generated.

As in the previous section, let S denote an elliptic surface over a smooth, irreducible, projective curve C over an algebraically closed field k, fibered by $g\colon S \to C$ with a section $\mathcal{O}$. Let $K = k(C)$ denote the function field of C and let $\eta\colon \operatorname{Spec} K \to C$ be its generic point. Let $E = S \times_C \operatorname{Spec} K$ be the generic fiber of g and let $\xi\colon E \to S$ denote the natural projection.

One of our main goals is to prove the following theorem.

Theorem 2.4.1 *The intersection pairing gives the Néron-Severi group* $\mathrm{NS}(S)$ *the structure of a lattice. The subgroup* T *generated by the vertical divisors and the section* $(\mathcal{O})$ *is a sublattice of* $\mathrm{NS}(S)$ *that fits in a natural short exact sequence*

$$0 \to T \to \mathrm{NS}(S) \to E(K) \to 0.$$

There are two main differences between Shioda's setup and ours. First of all, we will define our homomorphisms between various groups in a functorial way. This allows us to prove various statements using for instance the snake lemma instead of explicit formulas. Second, Shioda works with the generic fiber E of an elliptic surface S as if it is a curve on the surface just like the special fibers, i.e., fibers above closed points of the base curve C. Even though E is technically not a curve on S, Shioda thinks of the restriction of a divisor D on S to E as "intersecting" D and E. This gives a map from $\operatorname{Div} S$ to $\operatorname{Div} E$, which induces a homomorphism from $\operatorname{Pic} S$ to $\operatorname{Pic} E$. We will introduce this map as coming from the contravariant functor Pic. Even though Shioda's way of working with the generic fiber is justified by Weil [We], our way avoids the danger of using results about the generic fiber that only hold for special fibers. Whenever a statement is due to Shioda, we will mention this in its proof.

To better understand the structure of the Néron-Severi group of an elliptic surface, we first focus on the part that comes from the vertical divisors. Recall (Definition 2.3.4) that $\operatorname{Div}_{\mathrm{vert}} S$ denotes the free abelian group generated by the vertical prime divisors. For any closed point $v \in C$ let $\Lambda(v)$ denote the free abelian group generated by the irreducible components of the fiber $g^{-1}(v)$. Then we have an isomorphism $\operatorname{Div}_{\mathrm{vert}} S = \bigoplus_{v \in C} \Lambda(v)$. Because g is dominant, by Remark 2.2.15 there is a homomorphism $g^*\colon \operatorname{Div} C \to \operatorname{Div} S$, whose image is obviously contained in $\operatorname{Div}_{\mathrm{vert}} S$. For $v \in C$, let F_v denote the fiber $g^*(v) = \sum n_\Theta \Theta$ where the sum is taken over the irreducible components Θ of $g^{-1}(v)$ and we have $n_\Theta = \operatorname{ord}_\Theta(u_v \circ g)$ for a uniformizer u_v of the local ring at $v \in C$. Then we have $F_v \in \Lambda(v)$ and as F_v is algebraically equivalent to $F_{v'}$ for any other $v' \in C$, we have $F_v \cdot \Theta = F_{v'} \cdot \Theta = 0$ for all $\Theta \in \Lambda(v)$. This implies that the intersection pairing is well-defined on the quotient $\Lambda_1(v) = \Lambda(v)/\langle F_v \rangle$.

Let $\Theta_{v,0}$ denote the irreducible component of F_v that intersects the section $(\mathcal{O})$. Since $\mathcal{O}$ is a section, it intersects F_v only once, so we find $1 = F_v \cdot (\mathcal{O}) = \sum_\Theta n_\Theta \Theta \cdot (\mathcal{O}) = n_{\Theta_{v,0}} \Theta_{v,0} \cdot (\mathcal{O})$. Thus we have $n_{\Theta_{v,0}} = 1$. The map $\mathbb{Z} \to \Lambda(v)$ sending 1 to F_v is a section of the homomorphism $\Lambda(v) \to \mathbb{Z}$ that sends D to $D \cdot (\mathcal{O})$. Hence the short exact sequence

$$0 \to \mathbb{Z} \to \Lambda(v) \to \Lambda_1(v) \to 0$$

splits. The induced section of $\Lambda(v) \to \Lambda_1(v)$ sends $D \bmod F_v$ to $D - (D \cdot (\mathcal{O}))F_v$, which is the unique element D' in $\Lambda(v)$ such that $D' - D$ is a multiple of F_v and the coefficient of $\Theta_{v,0}$ in D' is zero. This shows that $\Lambda_1(v)$ is isomorphic to the free abelian group generated by all irreducible components of $g^{-1}(v)$ except $\Theta_{v,0}$.

Remark 2.4.2 Let ζ_v denote the composition of the injection $\Lambda(v) \to \mathrm{Div}_{\mathrm{vert}}\, S$ with the described section $\Lambda_1(v) \to \Lambda(v)$ sending $D \bmod F_v$ to $D - (D \cdot (\mathcal{O}))F_v$. Then σ_v identifies $\Lambda_1(v)$ with the free subgroup of $\mathrm{Div}_{\mathrm{vert}}\, S$ generated by those irreducible components of $g^{-1}(v)$ that do not intersect $(\mathcal{O})$. Whenever we identify $\Lambda_1(v)$ with a subgroup of $\mathrm{Div}_{\mathrm{vert}}\, S$ in this section, it will be through ζ_v.

Lemma 2.4.3 *The group $\Lambda(v)$ together with the intersection pairing and the element $F_v = \sum_\Theta n_\Theta \Theta$ satisfies all conditions and statements* (i)–(iv) *of Lemma* 2.1.22*. Furthermore, for any irreducible component Θ of $g^{-1}(v)$ we have $\Theta^2 \geq -2$ and Θ^2 is even.*

Proof. The number of components of $g^{-1}(v)$ is finite and nonzero and the intersection pairing $(D, D') \mapsto D \cdot D'$ is symmetric and bilinear. For any two irreducible components Θ, Φ we have $\Theta \cdot \Phi \geq 0$ because Θ and Φ are effective. The element F in statement (ii)$'$ is the whole fiber F_v. By Remark 2.3.2 the morphism g is flat, so by the principle of connectedness, all fibers are connected, see [Ha2], exc. III.11.4. This gives statement (iii). As (i), (ii)$'$, and (iii) together imply (ii), we also have (ii). Statement (iv) follows from the fact that we have $n_{\Theta_{v,0}} = 1$. Since the canonical divisor K_S is numerically equivalent to a multiple of F_v (Theorem 2.3.10) and we have $F_v \cdot y = 0$ for all $y \in \Lambda(v)$, the adjunction formula gives $2g(\Theta) - 2 = \Theta \cdot (\Theta + K_S) = \Theta^2$ for any irreducible component of $g^{-1}(v)$, where $g(\Theta)$ is the genus of Θ. Hence we find $\Theta \geq -2$ and Θ^2 is even. □

Let m_v denote the number of irreducible components of $g^{-1}(v)$ and let $m_v^{(1)}$ denote the number of irreducible components Θ of multiplicity $n_\Theta = 1$. Note that we have $n_{\Theta_{v,0}} = 1$, so we get $m_v^{(1)} \geq 1$.

Proposition 2.4.4 *For any $v \in C$ the group $\Lambda(v)$ together with the intersection pairing is isomorphic to one of the groups described in Table* 2.1*. The intersection pairing makes $\Lambda_1(v)$ into a negative definite lattice of rank $m_v - 1$ and discriminant $(-1)^{m_v - 1} m_v^{(1)}$.*

Proof. By Lemma 2.4.3 the group $\Lambda(v)$ together with the intersection pairing satisfies all hypotheses of Proposition 2.1.24, so $\Lambda(v)$ is isomorphic to one of the examples in Table 2.1. Therefore $\Lambda_1(v)$ is isomorphic to one of the negative definite lattices in the fourth column of that table. The rank of $\Lambda_1(v)$ follows from the fact that $\Lambda(v)$ is free of rank m_v and we have $\operatorname{rk}\Lambda_1(v) = \operatorname{rk}\Lambda(v) - 1$. The discriminant follows from Remark 2.1.23 and the fact that $\Lambda_1(v)$ is negative definite. □

Proposition 2.4.4 tells us what the group structure of $\Lambda(v)$ together with the intersection pairing can be. This does not tell us everything about the geometric structure of the fiber above any $v \in C$, as for instance the irreducible components may or may not be singular, or three components may intersect in one point. Table 2.2 shows several possible fibers with a more detailed description given in Table 2.3. Table 2.2 is almost exactly copied from [Si2], Fig. 4.4. The first two columns of Table 2.2 and 2.3 contain the name or type of the singular fiber and the number of irreducible components. Note that many of the names in Table 2.2 and 2.3 were also used in Table 2.1, where they denoted certain groups together with a symmetric pairing. The names in Table 2.1 were chosen such that for every type N in Table 2.1, if $g^{-1}(v)$ is a singular fiber of type N as in Table 2.2, then $\Lambda(v)$ together with the intersection pairing is isomorphic to the example in Table 2.1 of type N. For a singular fiber at v of type $I_0(j)$ or $I_0^*(j)$, the group $\Lambda(v)$ is of type I_0 or I_0^* respectively. The types I_0, II, III, and IV in Table 2.2 and 2.3 do not occur in Table 2.1. If $g^{-1}(v)$ is a singular fiber of one of these types, then $\Lambda(v)$ is of type I_1, I_1, I_2, or I_3 respectively.

The third column of Table 2.2 contains a picture. Each (possibly curved) line segment corresponds to an irreducible component of the singular fiber. The number of intersection points of two line segments equals the number of intersection points of the corresponding irreducible components. All these intersections are transversal, except for type III, where two nonsingular rational curves intersect in one point with multiplicity 2. A short description in words is provided in the third column of Table 2.3. The fibers of type $I_0(j)$ and $I_0^*(j)$ come with an extra parameter j in the moduli space of four distinct points on the projective line. For type $I_0(j)$ the fiber is an elliptic curve, and thus a double cover of $\mathbb{P}^1$ with four ramification points. The parameter j corresponds to these four points. As the ground field is algebraically closed, this parameter j can be identified with the j-invariant of the fiber. For singular fibers of type $I_0^*(j)$ the parameter j describes the four intersection points of the component of multiplicity 2 with the other components. We will see in Remark 2.4.18 that over any ground field (also not algebraically closed) at least one of these intersection points is rational, so that the component of multiplicity 2 is indeed isomorphic with the projective line. We will see in the same remark why this parameter is also called j. The fourth column of Table 2.2 gives the opposite of a standard root lattice that $\Lambda_1(v)$ is isomorphic to, see also Table 2.1. The fifth column states $m_v^{(1)}$, which also equals the absolute value of the discriminant of $\Lambda_1(v)$, see Proposition 2.4.4.

We will see that after reducing, any two fibers X and Y of an elliptic fibration that are of the same type, are in fact isomorphic. In Proposition 2.4.10 we will prove something stronger by assuming only that X and Y satisfy the *description* of the same

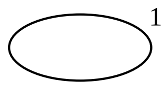
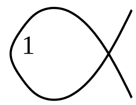
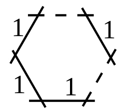
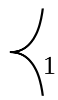
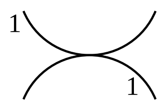
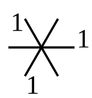
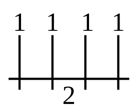
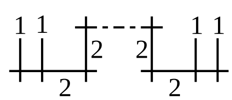
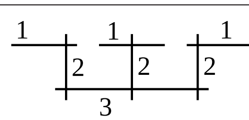
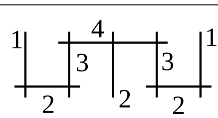
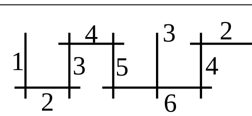
Type	m_v	Configuration	$\Lambda_1(v)$	$m_v^{(1)}$
$I_0(j)$	1		0	1
I_1	1		0	1
$I_n(n \geq 2)$	n		$A_{n-1}(-1)$	n
II	1		0	1
III	2		$A_1(-1)$	2
IV	3		$A_2(-1)$	3
$I_0^*(j)$	5		$D_4(-1)$	4
$I_n^*(n \geq 1)$	$n+5$		$D_{n+4}(-1)$	4
IV^*	7		$E_6(-1)$	3
III^*	8		$E_7(-1)$	2
II^*	9		$E_8(-1)$	1

Table 2.2: fibers of elliptic surfaces

type	m_v	description (all fibers are projective)
$I_0(j)$	1	nonsingular curve of genus 1 with j-invariant j
I_1	1	singular rational curve with one node
I_2	2	two nonsingular rational curves intersecting in two different points
$I_n (n \geq 3)$	n	n nonsingular rational curves intersecting in a cycle, i.e., $\Theta_i \cdot \Theta_j = 1$ if $i - j \equiv \pm 1 \bmod n$, $\Theta_i \cdot \Theta_j = 0$ otherwise
II	1	singular rational curve with one cusp
III	2	two nonsingular rational curves intersecting in one point with multiplicity 2
IV	3	three nonsingular rational curves intersecting in one point P with $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 2$, where $\mathfrak{m}$ is the maximal ideal of the local ring at P
$I_0^*(j)$	5	nonsingular rational curves with only transversal intersections, no three components intersect in one point, the intersection numbers are as suggested by Table 2.2, and the parameter j is the element in the moduli space of four points on $\mathbb{P}^1$ corresponding to the four intersection points.
$I_n^*(n \geq 1)$ IV^* III^* II^*	$n+5$ 7 8 9	$\left.\right\}$ nonsingular rational curves with only transversal intersections, no three components intersect in one point, and the intersection numbers are as suggested by Table 2.2.

Table 2.3: description of fibers

type of fiber, not that they are actually fibers of an elliptic fibration. This requires that we generalize the notion of intersection number of two curves on a smooth surface to the case of two components of an abstract curve. For curves on a smooth surface we have the following definition, see [Ha2], p. 360.

Definition 2.4.5 *Let X be a smooth surface over a field k and let C and D be two geometrically integral curves on X intersecting at the point P. Let $\mathfrak{p}$ and $\mathfrak{q}$ denote the prime ideals in the local ring $\mathcal{O}_{X,P}$ corresponding to C and D respectively. Then the intersection number $(C \cdot D)_P$ of C and D at P equals $\dim_k \mathcal{O}_{X,P}/(\mathfrak{p}+\mathfrak{q})$.*

Remark 2.4.6 Suppose $X, C, D, P, \mathfrak{p}$, and $\mathfrak{q}$ are as in Definition 2.4.5. Let Z denote the scheme-theoretic union $Z = C \cup D$, i.e., the ideal sheaf of Z in X is the intersection of the ideal sheaves of C and D in X. Let $\mathcal{O}_{Z,P}$ denote the local ring of P in Z. Then we have an isomorphism $\mathcal{O}_{Z,P} \cong \mathcal{O}_{X,P}/(\mathfrak{p} \cap \mathfrak{q})$. Let $\mathfrak{p}$ and $\mathfrak{q}$ also denote the image in $\mathcal{O}_{Z,P}$ of $\mathfrak{p}$ and $\mathfrak{q}$ respectively. Then we have $\dim_k \mathcal{O}_{Z,P}/(\mathfrak{p}+\mathfrak{q}) = \dim_k \mathcal{O}_{X,P}/(\mathfrak{p}+\mathfrak{q})$.

According to Remark 2.4.6, the following definition is a generalization of the notion of intersection number of two curves on a smooth surface.

Definition 2.4.7 *Let Z be a geometrically reduced curve over a field k and let $P \in Z$ be a closed point of degree 1 where two different irreducible components C and D of Z intersect. Let $\mathfrak{p}$ and $\mathfrak{q}$ denote the prime ideals in the local ring $\mathcal{O}_{Z,P}$ corresponding to C and D respectively. Then the intersection number $(C \cdot D)_P$ of C and D at P equals $\dim_k \mathcal{O}_{Z,P}/(\mathfrak{p}+\mathfrak{q})$. We say that C and D meet* transversally *if we have $(C \cdot D)_P = 1$.*

Lemma 2.4.8 *Let $Z, C, D, P, \mathfrak{p}$, and $\mathfrak{q}$ be as in Definition 2.4.7, and let $\mathfrak{m}$ denote the maximal ideal of the local ring $\mathcal{O}_{Z,P}$. Then for $r = (C \cdot D)_P$ we have $\mathfrak{m}^r \subset \mathfrak{p}+\mathfrak{q}$.*

Proof. Let $\mathfrak{n}$ be the maximal ideal of the artinian ring $\mathcal{O}_{Z,P}/(\mathfrak{p}+\mathfrak{q})$ and let t be the smallest integer such that $\mathfrak{n}^t/\mathfrak{n}^{t+1} = 0$. Then by Nakayama's lemma we have $\mathfrak{n}^t = 0$, so $\mathfrak{m}^t \subset \mathfrak{p}+\mathfrak{q}$. We also have $r = \dim_k R/(\mathfrak{p}+\mathfrak{q}) \geq t$, so $\mathfrak{m}^r \subset \mathfrak{m}^t \subset \mathfrak{p}+\mathfrak{q}$. □

Lemma 2.4.9 *Let the notation be as in Lemma 2.4.8. Then C and D intersect transversally at P if and only if we have $\mathfrak{p}+\mathfrak{q} = \mathfrak{m}$.*

Proof. Suppose C and D intersect transversally, so $r = 1$. Then we find $\mathfrak{m} \subset \mathfrak{p}+\mathfrak{q}$ from Lemma 2.4.8. Since we also have $\mathfrak{p}+\mathfrak{q} \subset \mathfrak{m}$, we get $\mathfrak{m} = \mathfrak{p}+\mathfrak{q}$. Conversely, suppose $\mathfrak{m} = \mathfrak{p}+\mathfrak{q}$. Then we have an isomorphism $\mathcal{O}_{Z,P}/(\mathfrak{p}+\mathfrak{q}) \cong \mathcal{O}_{Z,P}/\mathfrak{m} \cong k$, so $(C \cdot D)_P = \dim_k k = 1$. □

Proposition 2.4.10 *Let N be a type of fiber described in Tables 2.2 and 2.3. Let X and Y be curves over the algebraically closed field k, both fitting the description of N. Then X_{red} and Y_{red} are isomorphic to each other.*

To prove Proposition 2.4.10 we will use the following lemmas.

Lemma 2.4.11 *Let k be any field and let R and S be commutative local k-algebras with maximal ideals $\mathfrak{m}$ and $\mathfrak{n}$ respectively. Assume that $k \to S/\mathfrak{n}$ is an isomorphism. Assume also that R contains ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subset \mathfrak{m}$ with $r \geq 2$ and with $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r = (0)$ and that there exists a positive integer t with $\mathfrak{m}^t \subset \mathfrak{p}_i + \mathfrak{p}_j$ for $i \neq j$. Suppose that there are local homomorphisms of k-algebras $\varphi_i \colon S \to R/\mathfrak{p}_i$ such that the induced homomorphism $\mathfrak{n}/\mathfrak{n}^{t(r-1)} \to \bigoplus_{i=1}^r \mathfrak{m}/(\mathfrak{m}^{t(r-1)} + \mathfrak{p}_i)$ has image contained in the image of the natural homomorphism $\mathfrak{m}/\mathfrak{m}^{t(r-1)} \to \bigoplus_{i=1}^r \mathfrak{m}/(\mathfrak{m}^{t(r-1)} + \mathfrak{p}_i)$. Then there is a unique local homomorphism of k-algebras $\psi \colon S \to R$ such that φ_i is the composition of ψ and the homomorphism $R \to R/\mathfrak{p}_i$ for all i.*

$$\begin{tikzcd}
S \arrow[rrrr, dashed, "\psi"] \arrow[dr, "\varphi_1"'] \arrow[drr, "\varphi_2"] \arrow[drrrr, "\varphi_r"] & & & & R \arrow[dlll] \arrow[dll] \arrow[d] \\
& R/\mathfrak{p}_1 & R/\mathfrak{p}_2 & \cdots & R/\mathfrak{p}_r
\end{tikzcd}$$

Proof. We show that for each $x \in S$ there is a unique $y \in R$ such that $\varphi_i(x) \equiv y \bmod \mathfrak{p}_i$ for all i. First we show existence. For $x \in k \subset S$ this is obvious, as φ_i is a homomorphism of k-algebras. Suppose $x \in \mathfrak{n}$. Then by the last hypothesis, there exists $z \in \mathfrak{m}$ such that for all i we have $z \equiv \varphi_i(x) \bmod (\mathfrak{m}^{t(r-1)} + \mathfrak{p}_i)$. Hence for all i there are $a_i \in \mathfrak{m}^{t(r-1)}$ and $b_i \in \mathfrak{p}_i$ such that $\varphi_i(x) - z = a_i + b_i$. From the inclusions

$$\begin{aligned}
\mathfrak{m}^{t(r-1)} = (\mathfrak{m}^t)^{r-1} &\subset (\mathfrak{p}_1 + \mathfrak{p}_i) \cdots (\mathfrak{p}_{i-1} + \mathfrak{p}_i)(\mathfrak{p}_{i+1} + \mathfrak{p}_i) \cdots (\mathfrak{p}_r + \mathfrak{p}_i) \\
&\subset (\mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_r) + \mathfrak{p}_i
\end{aligned}$$

we deduce that we can write $a_i = c_i + d_i$ with $c_i \in \mathfrak{p}_1 \cdots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \cdots \mathfrak{p}_r$ and $d_i \in \mathfrak{p}_i$. Set $y = z + \sum_{j=1}^r c_j$. Then we have $y \equiv z + c_i = \varphi_i(x) - b_i - d_i \equiv \varphi_i(x) \bmod \mathfrak{p}_i$ for all i, just as was needed. For general $x \in S$, we write x as $x = x_1 + x_2$ with $x_1 \in k$ and $x_2 \in \mathfrak{n}$ to obtain y_1 and y_2 such that $y_l \equiv \varphi_i(x_l) \bmod \mathfrak{p}_i$ for all i and $l = 1, 2$. Then $y = y_1 + y_2$ satisfies $\varphi_i(x) \equiv y \bmod \mathfrak{p}_i$ for all i. To show that y is unique, suppose that there are y and y' with $y \equiv \varphi_i(x) \equiv y' \bmod \mathfrak{p}_i$. Then we have $y - y' \in \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r = (0)$, so $y = y'$. Define $\psi \colon S \to R$ by sending $x \in S$ to the unique element $y \in R$ that satisfies $\varphi_i(x) \equiv y \bmod \mathfrak{p}_i$ for all i. Then φ_i is the composition of ψ and the homomorphism $R \to R/\mathfrak{p}_i$ for all i. This implies that the homomorphism $\prod \varphi_i \colon S \to \prod R/\mathfrak{p}_i$ is the composition of ψ and the natural homomorphism $R \to \prod R/\mathfrak{p}_i$. As we have $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r = (0)$, this last homomorphism is injective, so ψ is a homomorphism as well. As ψ is the identity on k and sends $\mathfrak{n}$ to $\mathfrak{m}$, we conclude that ψ is a local homomorphism of k-algebras. $\square$

Remark 2.4.12 As one can see in the proof, the exponent $t(r-1)$ in the last hypothesis of Lemma 2.4.11 can be replaced by any integer q with $\mathfrak{n}^q \subset \mathfrak{p}_i + (\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_{i-1} \cap \mathfrak{p}_{i+1} \cap \ldots \cap$

$\mathfrak{p}_r$) for all i. Also, R and S may be assumed to be just local rings instead of k-algebras, as long as the last hypothesis is replaced by the assumption that for q as above, the image of $S/\mathfrak{n}^q \to \bigoplus_{i=1}^r R/(\mathfrak{m}^q + \mathfrak{p}_i)$ is contained in the image of $R/\mathfrak{m}^q \to \bigoplus_{i=1}^r R/(\mathfrak{m}^q + \mathfrak{p}_i)$.

Lemma 2.4.13 *Let V and W be vector spaces over a field k and let $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ be vector spaces over k of dimension 1. Suppose that there are nonsurjective homomorphisms $\varphi\colon V \to \bigoplus_{i=1}^n X_i$ and $\psi\colon W \to \bigoplus_{i=1}^n Y_i$ such that for each j the induced homomorphisms $V \to \bigoplus_{i\neq j} X_i$ and $W \to \bigoplus_{i \neq j} Y_i$ are surjective. Assume that $\alpha_1\colon X_1 \to Y_1$ is an isomorphism. Then there are isomorphisms $\alpha_i\colon X_i \to Y_i$ for $i = 2, \ldots, n$ such that the isomorphism $\alpha = (\alpha_i)_i\colon \bigoplus_{i=1}^n X_i \to \bigoplus_{i=1}^n Y_i$ induces an isomorphism between the images of φ and ψ.*

Proof. Suppose $1 \leq j \leq n$ and let $\pi_j\colon \bigoplus_{i=1}^n X_i \to \bigoplus_{i\neq j} X_i$ be the natural projection. Since $\pi_j \circ \varphi$ is surjective, the homomorphism $X_j = \ker \pi_j \to \operatorname{coker} \varphi$ is surjective as well. Since X_j has dimension 1 and $\operatorname{coker}\varphi$ is nontrivial, we find that this homomorphism is an isomorphism for all j. Similarly we get an isomorphism $Y_j \to \operatorname{coker}\psi$ for all j. Thus the isomorphism α_1 induces an isomorphism $\gamma\colon \operatorname{coker}\varphi \to \operatorname{coker}\psi$, which induces isomorphisms $\alpha_i\colon X_i \to Y_i$ such that the diagram

$$\begin{tikzcd} \bigoplus_{i=1}^n X_i \arrow[r] \arrow[d, "(\alpha_i)_i"'] & \operatorname{coker}\varphi \arrow[d, "\gamma"', "\cong"] \\ \bigoplus_{i=1}^n Y_i \arrow[r] & \operatorname{coker}\psi \end{tikzcd}$$

commutes. This induces an isomorphism between the kernels of the horizontal arrows. These kernels are the images of φ and ψ. $\square$

Lemma 2.4.14 *Let k be any field. Let X and Y be geometrically reduced curves over k with closed points Q and R of degree 1 on X and Y respectively. Suppose that X and Y both consist of $n \geq 2$ irreducible components, say $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$, such that for all $i \neq j$ the components X_i and X_j intersect only at Q and Y_i and Y_j intersect only at R. Suppose also that the X_i and Y_i are regular and that for $i = 1, \ldots, n$ there is an isomorphism $\varphi_i\colon X_i \to Y_i$ that sends Q to R. Let $\mathfrak{m}$ and $\mathfrak{n}$ denote the maximal ideals of the local rings $\mathcal{O}_{X,Q}$ and $\mathcal{O}_{Y,R}$ respectively. Then the following statements hold.*

(i) *Suppose we have $n = 2$, the components X_1 and X_2 intersect transversally at Q, and Y_1 and Y_2 intersect transversally at R. Then there is an isomorphism $X \to Y$ that restrict to φ_i on X_i for $i = 1, 2$.*

(ii) *Suppose we have $n = 2$, the components X_1 and X_2 intersect each other with multiplicity 2, the same holds for Y_1 and Y_2, one of the components has genus 0, and X and Y are projective. Then there exists an isomorphism $X \to Y$.*

(iii) *Suppose we have $n = 3$, the X_i intersect each other pairwise transversally, so do the Y_i, and X and Y are projective. Suppose also that two of the X_i have genus*

0 *and we have* $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim_k \mathfrak{n}/\mathfrak{n}^2 = 2$. *Then there exists an isomorphism* $X \to Y$.

Proof. For (i), define the open subsets $U_i = X_i - \{Q\}$. Then the isomorphisms $\varphi_i|_{U_i}$ glue to a morphism $\rho\colon X - \{Q\} \to Y$. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ denote the only two minimal primes of $\mathcal{O}_{X,Q}$, corresponding to the components X_1 and X_2 respectively. Since X is reduced, they satisfy $\mathfrak{p}_1 \cap \mathfrak{p}_2 = (0)$. As the intersection at Q is transversal, we find $\mathfrak{m} \subset \mathfrak{p}_1 + \mathfrak{p}_2$ from Lemma 2.4.8. Applying Lemma 2.4.11 to the local rings $\mathcal{O}_{X,Q}$ and $\mathcal{O}_{Y,R}$, we find that the local homomorphisms $\mathcal{O}_{Y,R} \to \mathcal{O}_{X,Q}/\mathfrak{p}_i$ corresponding to φ_i come from a unique local homomorphism $\mathcal{O}_{Y,R} \to \mathcal{O}_{X,Q}$. This means that we can extend ρ uniquely to a morphism $\psi\colon X \to Y$. By symmetry we also have a unique morphism $\psi'\colon Y \to X$ that restricts to φ_i^{-1} on Y_i. By uniqueness, the composition $\psi' \circ \psi$ is equal to the identity, so ψ is an isomorphism.

For (ii), say that X_2 has genus 0. As X_2 contains the k-point Q, we find that X_2 is isomorphic to $\mathbb{P}^1_k$ and hence, so is Y_2. Let $\varphi_i^\#$ denote the local homomorphism $\mathcal{O}_{Y_i,R} \to \mathcal{O}_{X_i,Q}$ induced by φ_i between the local rings at R and Q on Y_i and X_i respectively. As X_2 and Y_2 are isomorphic to $\mathbb{P}^1$, there are isomorphisms $\mathcal{O}_{X_2,Q} \cong k[s]_{(s)}$ and $\mathcal{O}_{Y_2,R} \cong k[t]_{(t)}$. Then we get the following diagram and we want to know if there exists a local isomorphism $\sigma\colon \mathcal{O}_{Y,R} \to \mathcal{O}_{X,Q}$ that makes the diagram commutative.

$$\begin{tikzcd}
\mathcal{O}_{Y_1,R} \arrow[d, "\cong"', "\varphi_1^\#"] & \mathcal{O}_{Y,R} \arrow[l] \arrow[r] \arrow[d, dashed, "\exists ?"', "\sigma"] & \mathcal{O}_{Y_2,R} \arrow[r, "\cong"] \arrow[d, "\cong"', "\varphi_2^\#"] & k[t]_{(t)} \\
\mathcal{O}_{X_1,Q} & \mathcal{O}_{X,Q} \arrow[l] \arrow[r] & \mathcal{O}_{X_2,Q} \arrow[r, "\cong"'] & k[s]_{(s)}
\end{tikzcd} \tag{2.3}$$

The problem is that such σ may not exist. We will replace $\varphi_2^\#$ by another isomorphism for which such a σ does exist. For $i = 1, 2$, let $\mathfrak{m}_i$ and $\mathfrak{n}_i$ denote the maximal ideals of $\mathcal{O}_{X_i,Q}$ and $\mathcal{O}_{Y_i,R}$ respectively. Then the $\varphi_i^\#$ induce an isomorphism $\mathfrak{n}_1/\mathfrak{n}_1^2 \oplus \mathfrak{n}_2/\mathfrak{n}_2^2 \cong \mathfrak{m}_1/\mathfrak{m}_1^2 \oplus \mathfrak{m}_2/\mathfrak{m}_2^2$. In order for σ to exist, this isomorphism has to identify the image of the map $\beta\colon \mathfrak{n}/\mathfrak{n}^2 \to \mathfrak{n}_1/\mathfrak{n}_1^2 \oplus \mathfrak{n}_2/\mathfrak{n}_2^2$ with the image of $\alpha\colon \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}_1/\mathfrak{m}_1^2 \oplus \mathfrak{m}_2/\mathfrak{m}_2^2$.

$$\begin{tikzcd}
\mathfrak{n}/\mathfrak{n}^2 \arrow[r, "\beta"] \arrow[d, dashed, "\exists ?"'] & \mathfrak{n}_1/\mathfrak{n}_1^2 \oplus \mathfrak{n}_2/\mathfrak{n}_2^2 \arrow[d, "\cong"] \\
\mathfrak{m}/\mathfrak{m}^2 \arrow[r, "\alpha"'] & \mathfrak{m}_1/\mathfrak{m}_1^2 \oplus \mathfrak{m}_2/\mathfrak{m}_2^2
\end{tikzcd}$$

For any $\lambda \in k^*$ consider the composition δ_λ of local isomorphisms of k-algebras

$$\begin{tikzcd}
\mathcal{O}_{Y_2,R} \arrow[r, "\cong"'] \arrow[rrr, bend left, "\delta_\lambda"] & k[t]_{(t)} \arrow[r, "\cong", "t \mapsto \lambda s"'] & k[s]_{(s)} \arrow[r, "\cong"'] & \mathcal{O}_{X_2,Q}.
\end{tikzcd}$$

When λ runs through k^*, the homomorphism $\mathfrak{n}_2/\mathfrak{n}_2^2 \to \mathfrak{m}_2/\mathfrak{m}_2^2$ induced by δ_λ runs through all isomorphisms between $\mathfrak{n}_2/\mathfrak{n}_2^2$ and $\mathfrak{m}_2/\mathfrak{m}_2^2$ as both are 1-dimensional. We will see that there is a $\lambda \in k^*$ such that if we replace $\varphi_2^\#$ by δ_λ in diagram (2.3), then there does exist an isomorphism σ as mentioned above.

Note that we have $\mathfrak{m}_i/\mathfrak{m}_i^2 = \mathfrak{m}/(\mathfrak{m}^2 + \mathfrak{p}_i)$, where $\mathfrak{p}_i$ is the prime in $\mathcal{O}_{X,Q}$ corresponding to X_i. Hence the maps $\mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}_i/\mathfrak{m}_i^2$ are surjective for $i = 1, 2$. Similarly, we find that the maps $\mathfrak{n}/\mathfrak{n}^2 \to \mathfrak{n}_i/\mathfrak{n}_i^2$ are surjective. We will show that α is not surjective. Note that for $i = 1, 2$ there is a short exact sequence

$$0 \to \frac{\mathfrak{m}^2 + \mathfrak{p}_1 + \mathfrak{p}_2}{\mathfrak{m}^2 + \mathfrak{p}_i} \to \frac{\mathfrak{m}}{\mathfrak{m}^2 + \mathfrak{p}_i} \to \frac{\mathfrak{m}}{\mathfrak{m}^2 + \mathfrak{p}_1 + \mathfrak{p}_2} \to 0 \tag{2.4}$$

of vector spaces over k. As the intersection number $X_1 \cdot X_2$ equals 2, we have $\mathfrak{m}^2 \subset \mathfrak{p}_1 + \mathfrak{p}_2$ by Lemma 2.4.8. This implies $\mathfrak{m}^2 + \mathfrak{p}_1 + \mathfrak{p}_2 = \mathfrak{p}_1 + \mathfrak{p}_2$. As X_1 and X_2 do not intersect transversally, we have $\mathfrak{p}_1 + \mathfrak{p}_2 \subsetneq \mathfrak{m}$ by Lemma 2.4.9, so the dimension of the right-most vector space in (2.4) is at least 1. As the X_i are regular, the vector space in the middle has dimension 1. Together this implies that the left-most vector space is 0, so we have $\mathfrak{m}^2 + \mathfrak{p}_i = \mathfrak{m}^2 + \mathfrak{p}_1 + \mathfrak{p}_2 = \mathfrak{p}_1 + \mathfrak{p}_2$. This implies that α is the natural map $\alpha\colon \mathfrak{m}/\mathfrak{m}^2 \to \big(\mathfrak{m}/(\mathfrak{p}_1 + \mathfrak{p}_2)\big)^2$, which is obviously not surjective. A similar argument shows that β is not surjective. By Lemma 2.4.13 there is an isomorphism $\eta\colon \mathfrak{n}_2/\mathfrak{n}_2^2 \to \mathfrak{m}_2/\mathfrak{m}_2^2$ such that $\varphi_1^\#$ and η induce an isomorphism $\mathfrak{n}_1/\mathfrak{n}_1^2 \oplus \mathfrak{n}_2/\mathfrak{n}_2^2 \to \mathfrak{m}_1/\mathfrak{m}_1^2 \oplus \mathfrak{m}_2/\mathfrak{m}_2^2$ that identifies the images of α and β. This map η is induced by δ_λ for some $\lambda \in k^*$. As we have $\mathfrak{m}^2 \subset \mathfrak{p}_1 + \mathfrak{p}_2$, we find from Lemma 2.4.11 that there is a unique homomorphism $\sigma\colon \mathcal{O}_{Y,R} \to \mathcal{O}_{X,Q}$ making the following diagram commutative.

$$\begin{tikzcd}
\mathcal{O}_{Y_1,R} \arrow[d, "\varphi_1^\#", "\cong"'] & \mathcal{O}_{Y,R} \arrow[l] \arrow[r] \arrow[d, "\sigma"] & \mathcal{O}_{Y_2,R} \arrow[d, "\delta_\lambda", "\cong"'] \\
\mathcal{O}_{X_1,Q} & \mathcal{O}_{X,Q} \arrow[l] \arrow[r] & \mathcal{O}_{X_2,Q}
\end{tikzcd}$$

By symmetry there is also a unique homomorphism $\sigma'\colon \mathcal{O}_{X,Q} \to \mathcal{O}_{Y,R}$ that is compatible with the inverses of $\varphi_1^\#$ and δ_λ. By uniqueness, the compositions $\sigma' \circ \sigma$ and $\sigma \circ \sigma'$ are the identity, so σ is an isomorphism. This implies that there are open neighborhoods U and V of Q and R in X and Y respectively, such that σ induces an isomorphism from U to V. Since X and Y are projective and regular outside Q and R, this isomorphism extends to an isomorphism $X \to Y$, see [Ha2], Prop. I.6.8.

For (iii) we proceed similarly. Assume X_1 and X_2 have genus 0. Then for $i = 1, 2$ there are isomorphisms $\mathcal{O}_{X_i,Q} \cong k[s_i]_{(s_i)}$ and $\mathcal{O}_{Y_i,R} \cong k[t_i]_{(t_i)}$. We get the following diagram.

$$\begin{tikzcd}
\mathcal{O}_{Y_1,R} \arrow[d, "\cong"] \arrow[ddd, bend right, "\varphi_1^{\#}"'] & \mathcal{O}_{Y,R} \arrow[l] \arrow[r] \arrow[d] \arrow[ddd, dashed, bend right=15, "\exists?\ \sigma"'] & \mathcal{O}_{Y_2,R} \arrow[d, "\cong"'] \arrow[ddd, bend left, "\varphi_2^{\#}"] \\
k[t_1]_{(t_1)} & \mathcal{O}_{Y_3,R} \arrow[d, "\cong"', "\varphi_3^{\#}"] & k[t_2]_{(t_2)} \\
k[s_1]_{(s_1)} & \mathcal{O}_{X_3,Q} & k[s_2]_{(s_2)} \\
\mathcal{O}_{X_1,Q} \arrow[u, "\cong"'] & \mathcal{O}_{X,Q} \arrow[l] \arrow[r] \arrow[u] & \mathcal{O}_{X_2,Q} \arrow[u, "\cong"]
\end{tikzcd} \tag{2.5}$$

We will again replace $\varphi_i^{\#}$ by another isomorphism for $i = 1, 2$, such that there exists an isomorphism $\sigma\colon \mathcal{O}_{Y,R} \to \mathcal{O}_{X,Q}$ making the diagram commutative. For $i = 1, 2, 3$, let $\mathfrak{m}_i$ and $\mathfrak{n}_i$ denote the maximal ideals of $\mathcal{O}_{X_i,Q}$ and $\mathcal{O}_{Y_i,R}$ respectively. Then the $\varphi_i^{\#}$ induce an isomorphism $\bigoplus_{i=1}^3 \mathfrak{n}_i/\mathfrak{n}_i^2 \cong \bigoplus_{i=1}^3 \mathfrak{m}_i/\mathfrak{m}_i^2$. Consider $\alpha\colon \mathfrak{m}/\mathfrak{m}^2 \to \bigoplus_{i=1}^3 \mathfrak{m}_i/\mathfrak{m}_i^2$ and $\beta\colon \mathfrak{n}/\mathfrak{n}^2 \to \bigoplus_{i=1}^3 \mathfrak{n}_i/\mathfrak{n}_i^2$. Because we have $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim \mathfrak{n}/\mathfrak{n}^2 = 2$, we find that α and β are not surjective. Suppose we have $i, j \in \{1, 2, 3\}$ with $i \neq j$. Since X_i and X_j intersect transversally, we have $\mathfrak{p}_i + \mathfrak{p}_j = \mathfrak{m}$, where $\mathfrak{p}_l$ denotes the minimal prime in $\mathcal{O}_{X,Q}$ corresponding to X_l. Hence, for every $x, y \in \mathfrak{m}$ there are $a, b \in \mathfrak{p}_i$ and $c, d \in \mathfrak{p}_j$ such that $x = a + c$ and $y = b + d$. Then for $z = b + c$ we have $z \equiv x \bmod \mathfrak{p}_i$ and $z \equiv y \bmod \mathfrak{p}_j$. This implies that the homomorphism $\mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}_i/\mathfrak{m}_i^2 \oplus \mathfrak{m}_j/\mathfrak{m}_j^2$ is surjective. Similarly, the homomorphism $\mathfrak{n}/\mathfrak{n}^2 \to \mathfrak{n}_i/\mathfrak{n}_i^2 \oplus \mathfrak{n}_j/\mathfrak{n}_j^2$ is surjective. By Lemma 2.4.13 this implies that there are isomorphisms $\eta_i\colon \mathfrak{n}_i/\mathfrak{n}_i^2 \to \mathfrak{m}_i/\mathfrak{m}_i^2$ for $i = 1, 2$ such that these η_i together with $\varphi_3^{\#}$ induce an isomorphism $\bigoplus_{i=1}^3 \mathfrak{n}_i/\mathfrak{n}_i^2 \to \bigoplus_{i=1}^3 \mathfrak{m}_i/\mathfrak{m}_i^2$ that identifies the image of β with the image of α. As in the proof of (ii), there are $\lambda_i \in k^*$ for $i = 1, 2$ such that η_i is induced by δ_i, where δ_i is the composition

$$\begin{tikzcd}
\mathcal{O}_{Y_i,R} \arrow[r, "\cong"'] \arrow[rrr, bend left=15, "\delta_i"] & k[t_i]_{(t_i)} \arrow[r, "\cong", "t_i \mapsto \lambda_i s_i"'] & k[s_i]_{(s_i)} \arrow[r, "\cong"'] & \mathcal{O}_{X_i,Q}
\end{tikzcd}$$

of isomorphisms of local k-algebras. As we have $\mathfrak{m} \subset \mathfrak{p}_i + \mathfrak{p}_j$ for $i \neq j$ by transversality, we find from Lemma 2.4.11 that there is a unique $\sigma\colon \mathcal{O}_{Y,R} \to \mathcal{O}_{X,Q}$ such that σ makes diagram (2.5) commute if we replace $\varphi_i^{\#}$ by δ_i for $i = 1, 2$. As in the proof of (ii), it follows from symmetry and uniqueness of σ that σ is an isomorphism. Therefore, there is an isomorphism of open neighborhoods of Q and R in X and Y respectively, which extends to an isomorphism from X to Y. □

Remark 2.4.15 Note that statements (ii) and (iii) of Lemma 2.4.14 are false without the assumption on the genus of some of the components. Suppose for instance that $C_1, C_2 \subset \operatorname{Spec} k[x, y]$ are regular curves without nontrivial automorphisms, given by

$f_1(x,y), f_2(x,y) \in k[x,y]$ and assume that both curves go through the origin and have the y-axis as tangent line at the origin. Let C_2' be the curve given by $f_2(x,2y)=0$. Set $X = C_1 \cup C_2$ and $Y = C_1 \cup C_2'$. Then the components of X and Y are isomorphic, but by considering the maps on tangent spaces, one can show that locally around the origin X and Y are not isomorphic.

Proof of Proposition 2.4.10. If both X and Y satisfy the description of type $I_0(j)$ for some j then they are isomorphic because over an algebraically closed field two elliptic curves are isomorphic if and only if they have the same j-invariant. If they were of type I_1 or II, it follows from the fact that any two rational curves with one node are isomorphic, and the same holds for rational curves with one cusp. In all other cases the irreducible components are nonsingular rational curves, and thus isomorphic to $\mathbb{P}^1$. Suppose that in X and Y each of these irreducible components intersects at most three other components, all intersections are transversal, and there are no points where more than two components intersect. Since any curve of genus 0 with at most three different fixed points is isomorphic to any other curve of genus 0 with as many fixed points (over an algebraically closed field), there is an isomorphism from the open subset of smooth points on X to the open subset of smooth points on Y. As the irreducible components of X and Y are smooth and projective, this isomorphism extends to an isomorphism between components. Applying Lemma 2.4.14, statement (i), to any two intersecting components, we find that it extends to an isomorphism between X and Y. Similarly, the proposition follows for type $I_0^*(j)$ as any two curves of genus 0 with four points corresponding to the same element j in the moduli space of four points on the projective line are by definition isomorphic. This leaves types III, IV. These two cases follow from Lemma 2.4.14, statements (ii) and (iii) respectively. □

Remark 2.4.16 Without the extra parameter for types $I_0(j)$ and $I_0^*(j)$ the conclusion of Proposition 2.4.10 would be wrong. However, this extra parameter appears not to be used anywhere in the literature in the context of the singular fibers of type $I_0^*(j)$.

Question 1 *Proposition* 2.4.10 *is no longer true if we replace* X_{red} *and* Y_{red} *by* X *and* Y *respectively. Suppose we add the assumption that* X *and* Y *are both fibers of an elliptic surface. Is it then possible to divide some of the types of singular fibers into additional continuous families such that Proposition* 2.4.10 *is still true if we replace* X_{red} *and* Y_{red} *by* X *and* Y *respectively?*

The next theorem tells us that the types of fibers in table 2.2 are all possible types of fibers of elliptic surfaces. Note that the ground field k is still assumed to be algebraically closed.

Theorem 2.4.17 *Let* $F = F_v = g^*(v)$ *be the fiber of* g *above a point* $v \in C$. *Let* A *be the set of irreducible components of* $g^{-1}(v)$. *Then we can write* $F = \sum_{\Theta \in A} n_\Theta \Theta$ *with* $n_\Theta > 0$ *and the fiber* F *is of one of the types described in Table* 2.3 *and* 2.2.

Proof. The fiber is a closed subscheme of the smooth surface S, so at any point P in the fiber, the local ring $\mathcal{O}_{F,P}$ is a quotient of the local ring $\mathcal{O}_{S,P}$ in S. Since S is regular of dimension 2, we have $\dim \mathfrak{m}/\mathfrak{m}^2 = 2$, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{O}_{S,P}$. This implies $\dim \mathfrak{n}/\mathfrak{n}^2 \leq 2$ for the maximal ideal $\mathfrak{n}$ of $\mathcal{O}_{F,P}$ with equality if and only if P is a singular point of F. See also [Ha2], Prop. II.8.12.

By Lemma 2.4.3 the group $\Lambda(v)$ together with the intersection pairing satisfies all hypotheses of Proposition 2.1.24, so $\Lambda(v)$ is isomorphic to one of the examples in Table 2.1. Set $r = \#A$. Suppose $r = 1$ and write $\Theta = \Theta_1$. Then $F = n_\Theta \Theta$, so $\Theta^2 = 0$. As the canonical divisor K_S is numerically equivalent to a multiple of any fiber, we have $K_S \cdot \Psi = 0$ for any vertical divisor Ψ. Therefore, the adjunction formula gives $2p_a(\Theta) - 2 = \Theta \cdot (\Theta + K_S) = \Theta^2 = 0$, so the arithmetic genus $p_a(\Theta)$ of Θ equals 1. If Θ is nonsingular, then the fiber is of type $I_0(j)$ for some j. It is a general fact that a geometrically integral curve with arithmetic genus 1 has at most one singular point, and if it does have one, then it is a double point, see [Ha2], Cor. V.3.7. Thus, if Θ is singular, then $F = \Theta$ is of type I_1 or II. Now suppose $r \geq 2$. Then by Proposition 2.1.24 we have $\Theta_i^2 = -2$ for all i. By the adjunction formula this implies that the arithmetic genus of Θ_i equals 0, which implies that Θ_i is a nonsingular rational curve.

If there are Θ_i and Θ_j with $\Theta_i \cdot \Theta_j \geq 2$, then according to Proposition 2.1.24 the fiber F contains only two components with intersection number 2. They intersect in either one or two points and F is thus of type III or I_2 respectively. If there are three components that intersect in one point, then by Proposition 2.1.24 these are all components, so F is of type IV.

We may now assume that all intersections are transversal, no three components intersect in one point, and any two components intersect at most once. These cases are classified according to the isomorphism class of $\Lambda(v)$ together with the intersection pairing. Their isomorphism classes have been classified in Proposition 2.1.24. The elliptic fibers F_v for which $\Lambda(v)$ is of type I_0^* contain a component that intersects four other components. These fibers are separated into a continuous family of types $I_0^*(j)$, where the parameter j describes the isomorphism class of the four intersection points on the projective line. □

Remark 2.4.18 Tate's algorithm (see [Ta3] and [Si2], IV.9) gives an easy way to decide which type of singular fiber lies above a point $v \in C$. It is based on the valuation at v of both the j-invariant of the generic fiber E/K and the discriminant of a Weierstrass model of E. From the proof of Tate's algorithm (see [Si2], p. 373) one can also deduce the parameter j if the fiber is of type $I_0^*(j)$ as follows. Let R be a discrete valuation ring with uniformizer π, fraction field K, and algebraically closed residue field k. Let $\mathcal{E}$ be a minimal, smooth, integral model over R of an elliptic curve E over K. Suppose that the special fiber of $\mathcal{E}$ over the residue field k of R has type $I_0^*(j_0)$ for some $j_0 \in k$. Then according to [Si2], p. 373, the characteristic of k is not equal to 2, and there exists a Weierstrass model of E given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in R$ and $\pi|a_1, a_2$, $\pi^2|a_3, a_4$, and $\pi^3|a_6$, such that the polynomial $P(T) = T^3 + a_{2,1}T^2 + a_{4,2}T + a_{6,3} \in R[T]$ with $a_{i,j} \equiv \pi^{-j}a_i$ has distinct roots modulo (π). The parameter j_0 corresponds to the isomorphism class of the projective line with these three roots in $R/(\pi) = k$ and the point at infinity.

A way to interpret this is as follows. Over an algebraically closed field, the moduli space of four distinct points on the projective line is exactly the j-line, where four points P_1, P_2, P_3, P_4 on $\mathbb{P}^1$ correspond to the j-invariant of an elliptic curve for which the x-coordinate gives a map to $\mathbb{P}^1$ that ramifies above the P_i. Let $j \in K$ be the j-invariant of our elliptic curve E/K. By [Si2], p. 373, we have $j \in R$. Set $u = \pi^{-1}x$ and $v = \pi^{-2}y$. Then E/K can be given by

$$\pi(v^2 + a_{1,1}uv + a_{3,2}v) = u^3 + a_{2,1}u^2 + a_{4,2}u + a_{6,3}.$$

The coordinate u determines a map $E \to \mathbb{P}^1_K$ and j corresponds to $\mathbb{P}^1_K$ with the four ramification points of u. By the quadratic formula these are the three points given by

$$\pi(a_{1,1}u + a_{3,2})^2 + 4(u^3 + a_{2,1}u^2 + a_{4,2}u + a_{6,3}) = 0$$

and the point at infinity. The reduction of these points modulo π are exactly the roots of $P(T) \bmod (\pi)$ and the point at infinity. These four points on $\mathbb{P}^1_k$ correspond to j_0, so the image of $j \in R$ in the residue field k is exactly j_0. Considering for instance the elliptic surface S_λ over $\mathbb{P}^1(t)$ given by

$$y^2 = x(x-t)(x-\lambda t),$$

with $\lambda \in k \setminus \{0,1\}$, we get a singular fiber of type $I_0^*(j_0)$ at $t = 0$, where j_0 is the j-invariant of the elliptic curve given by $y^2 = x(x-1)(x-\lambda)$.

Recall that we still have a fixed elliptic surface S over a curve C with function field $K = k(C)$. The generic fiber is denoted E, which is an elliptic curve over K, whose function field $K(E)$ is isomorphic to the function field $k(S)$ of S.

Lemma 2.4.19 *The homomorphism* $\operatorname{Div}_{\mathrm{vert}} S \cong \bigoplus_{v\in C} \Lambda(v) \to \mathbb{Z}F \oplus \bigoplus_{v\in C} \Lambda_1(v)$ *sending* D *to* $\big((D\cdot(\mathcal{O}))F, \overline{D}\big)$ *has kernel* $g^*\operatorname{Div}^0 C$ *and induces a split short exact sequence*

$$0 \longrightarrow \operatorname{Div}^0 C \xrightarrow{g^*} \operatorname{Div}_{\mathrm{vert}} S \longrightarrow \mathbb{Z}F \oplus \bigoplus_{v\in C} \Lambda_1(v) \longrightarrow 0. \tag{2.6}$$

Proof. Let φ denote the homomorphism in question. The composition of φ with the projection to $\bigoplus_{v\in C}\Lambda_1(v)$ is clearly surjective. As any fiber maps to $F \oplus 0$, we find that φ itself is also surjective. The inclusion $g^*\operatorname{Div}^0(C) \subset \ker\varphi$ is clear from the fact that $\deg D' = (g^*D')\cdot(\mathcal{O})$ for any divisor $D' \in \operatorname{Div} C$. Conversely, any divisor $D \in \ker\varphi$ consists of whole fibers and is therefore of the form $D = g^*(D')$ for some divisor $D' \in \operatorname{Div} C$. From the equality $\deg D' = (g^*D')\cdot(\mathcal{O}) = D\cdot(\mathcal{O}) = (\text{coefficient of } F) = 0$ we find $D' \in \operatorname{Div}^0 C$. The sequence splits because it is a sequence of free abelian groups. $\square$

Let T_1 denote the group $\mathbb{Z}F \oplus \bigoplus_{v\in C}\Lambda_1(v)$ from Lemma 2.4.19.

Remark 2.4.20 An explicit splitting of the sequence (2.6) can be given by choosing a point $v_0 \in C$ and setting $F_0 = g^*(v_0)$ (in fact, it is enough for v_0 to be a divisor of degree 1). The map $\mathbb{Z}F \to \mathrm{Div}_{\mathrm{vert}}\, S$ sending F to F_0 and the maps ζ_v from Remark 2.4.2 together induce a homomorphism $\zeta\colon T_1 \to \mathrm{Div}_{\mathrm{vert}}\, S$ that sends F to F_0 and $D \bmod \langle F_v\rangle \in \Lambda_1(v)$ to $D - (D\cdot(\mathcal{O}))F_v$. This gives a section for (2.6). The associated homomorphism $\mathrm{Div}_{\mathrm{vert}}\, S \to \mathrm{Div}^0 C$ sends $D \in \Lambda(v)$ to $(D\cdot(\mathcal{O}))((v)-(v_0))$. Note that this splitting depends on both $\mathcal{O}$ and the choice of v_0. Whenever we implicitly embed T_1 in $\mathrm{Div}_{\mathrm{vert}}\, S$ in this section, it will be through ζ.

Remark 2.4.21 Because the divisors in $g^*\,\mathrm{Div}^0 C$ are algebraically equivalent to 0, the map $\mathrm{Div}_{\mathrm{vert}}\, S \to \mathrm{NS}(S)$ factors through T_1, so we get a natural map $T_1 \to \mathrm{NS}(S)$, which depends on the choice of the section $\mathcal{O}$. We will see in Proposition 2.4.29 that this map is injective. We can also think of this as map as the composition of ζ from Remark 2.4.20 with the map $\mathrm{Div}_{\mathrm{vert}}\, S \to \mathrm{NS}(S)$. This composition does not depend anymore on the choice of v_0. The intersection pairing gives a well defined map $T_1 \times \mathrm{NS}(S) \to \mathbb{Z}$, which also depends on $\mathcal{O}$. This can be given explicitly through the section ζ of $\mathrm{Div}_{\mathrm{vert}}\, S \to T_1$ given in Remark 2.4.20. Note that for any $v \in C$ and any $D \in \Lambda_1(v) \subset T_1$ we have $(R)\cdot D = (\mathcal{O})\cdot D = F\cdot D = 0$ for every section $R \in S(C)$ for which the divisor (R) intersects every fiber in the same irreducible component as $(\mathcal{O})$. It follows from Proposition 2.4.4 that the intersection pairing on $\bigoplus_{v\in C}\Lambda_1(v) \subset T_1$ (which does not depends on $\mathcal{O}$) is negative definite, so we already see that the map $\bigoplus_{v\in C}\Lambda_1(v) \to \mathrm{NS}(S)$ is injective.

We will now state and prove a proposition that is a slight generalization of a theorem by Shioda ([Shi3], Theorem 3.1). Our proof is practically the same as Shioda's. By phrasing a generalization, we will also be able to deduce another theorem, for which Shioda gives a more complicated proof.

Proposition 2.4.22 *On an elliptic surface S, fibered by g over a curve C, the following conditions on a divisor D of S are equivalent.*

(i) *The divisor D is linearly equivalent to a divisor in the image of $g^*\colon \mathrm{Div}^0 C \to \mathrm{Div}^0 S$.*

(ii) *The divisor D is algebraically equivalent to* 0.

(iii) *For some integer $n > 0$ the divisor nD is algebraically equivalent to* 0.

(iv) *The divisor D is numerically equivalent to* 0.

Proof. The implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) are obvious. Shioda proves only the equivalence of (ii), (iii), and (iv), see [Shi3], Thm. 3.1. To prove the implication (iv) $\Rightarrow$ (i) we will follow closely Shioda's proof of the implication (iv) $\Rightarrow$ (ii). Shioda credits the idea to Inoue. Let D be a divisor on S that is numerically equivalent to 0. Let K_S denote a canonical divisor on S. According to Proposition 2.3.14 the Euler characteristic

$\chi = \chi(\mathcal{O}_S)$ of S is positive, so the Riemann-Roch theorem for surfaces (see [Ha2], Thm. V.1.6) gives

$$h^0(S, \mathcal{O}(D)) - h^1(S, \mathcal{O}(D)) + h^0(S, \mathcal{O}(K_S - D)) = \frac{1}{2} D \cdot (D - K_S) + \chi = \chi > 0.$$

Hence, we have $h^0(S, \mathcal{O}(D)) > 0$ or $h^0(S, \mathcal{O}(K_S - D)) > 0$, which implies that either D or $K_S - D$ is linearly equivalent to an effective divisor D'. In the first case ($D' \sim D$) we are done. Indeed, in this case we find $D' = 0$, because if D' were nonzero and effective, then there would exist some curve Γ on S with $D' \cdot \Gamma > 0$ (take any prime divisor C in the support of D', take any point P on C, and take Γ to be any curve through P that is not C).

In the second case we find $D' \cdot \Theta = K_S \cdot \Theta - D \cdot \Theta = 0$ for any vertical divisor Θ. This follows from the fact that K_S is numerically equivalent to a multiple of any fiber (see Theorem 2.3.10), so we find $K_S \cdot \Theta = 0$ for any vertical divisor Θ. As D' is effective, this implies that D' contains no horizontal components. By Lemma 2.4.19 this implies that D' can be written as

$$D' = g^*(\Delta) + nF + D''$$

for some divisor Δ on C of degree 0, some integer n, any fiber F, and some $D'' \in \bigoplus_{v \in C} \Lambda_1(v)$. Note that here we view $T_1 = \mathbb{Z}F \oplus \bigoplus_{v \in C} \Lambda_1(v)$ as a subgroup of $\mathrm{Div}_{\mathrm{vert}}\, S$ through ζ, see Remark 2.4.20. The equation $D' \cdot \Theta = 0$ implies $D'' \cdot \Theta = 0$ for any vertical divisor Θ. By Proposition 2.4.4 the intersection pairing on $\bigoplus_{v \in C} \Lambda_1(v)$ is negative definite, so we find $D'' = 0$ and thus $D \sim K_S - D' = K_S - g^*(\Delta) - nF$. By Theorem 2.3.10 this implies that D is linearly equivalent to $g^*(\Gamma)$ for some divisor Γ on C. From the equality $\deg \Gamma = g^*(\Gamma) \cdot (\mathcal{O}) = D \cdot (\mathcal{O}) = 0$, we conclude $\Gamma \in \mathrm{Div}^0 C$. $\square$

Proposition 2.4.23 *The group* $\mathrm{NS}(S)$ *is finitely generated and free. The intersection pairing induces a symmetric, nondegenerate, bilinear pairing on* $\mathrm{NS}(S)$*, making it into a lattice of signature* $(1, \rho - 1)$*. If the Euler characteristic* $\chi = \chi(\mathcal{O}_S)$ *of* S *is even, then* $\mathrm{NS}(S)$ *is an even lattice.*

Proof. The group $\mathrm{NS}(S)$ is finitely generated by Proposition 2.2.12. The fact that $\mathrm{NS}(S)$ is free follows immediately from Proposition 2.4.22 and the fact that the Néron-Severi group modulo numerical equivalence is free, see Proposition 2.2.17. It also follows immediately that the bilinear intersection pairing is nondegenerate on $\mathrm{NS}(S)$, see [Shi3], Thm. 2.1 or [Ha2], example V.1.9.1. The signature is given by the Hodge Index Theorem ([Ha2], Thm. V.1.9). From the adjunction formula ([Ha2], Prop. V.1.5) we find $2g(D) - 2 = D \cdot (D + (2g(C) - 2 + \chi)F) = D^2 + (2g(C) - 2 + \chi)(D \cdot F)$ for any irreducible curve D on S with genus $g(D)$. Therefore, if χ is even, we find that D^2 is even for all prime divisors D. As these divisors generate $\mathrm{NS}(S)$, the lattice $\mathrm{NS}(S)$ is even. $\square$

Theorem 2.4.24 *The map* $g^* \colon \mathrm{Pic}^0 C \to \mathrm{Pic}^0 S$ *is an isomorphism.*

Proof. This is Theorem 4.1 in [Shi3]. Instead of the relatively involved proof given there, we will deduce this from Proposition 2.4.22. The homomorphism g^* is injective, because it is a section of $\mathcal{O}^*\colon \operatorname{Pic}^0 S \to \operatorname{Pic}^0 C$. The surjectivity of g^* follows immediately from the implication (ii) $\Rightarrow$ (i) of Proposition 2.4.22. $\square$

Remark 2.4.25 The Jacobian of $\mathbb{P}^1$ is zero, so if the base curve C is isomorphic to $\mathbb{P}^1$, then $\operatorname{Pic}^0(S) = 0$ and the Néron-Severi group $\operatorname{NS}(S)$ is isomorphic to the Picard group $\operatorname{Pic}(S)$. In general any elliptic fibration $S \to C'$ with section and at least one singular fiber has a base curve of genus $g(C') = \dim \operatorname{Jac}(C) = \dim \operatorname{Pic}^0(S)$. Over $\mathbb{C}$, this number equals the irregularity $q = q(S) = \dim H^1(S, \mathcal{O}_S)$. If S is for instance a complex K3 surface, the irregularity satisfies $q = 0$, so then we get $g(C') = 0$.

The morphism $\xi\colon E \to S$ induces homomorphisms ξ^* on the level of Pic, Pic^0 and hence also on the level of NS. Because ξ is dominant, it induces an injection $\xi^*\colon k(S) \to k(E)$ of function fields, too. This injection is an isomorphism because it comes from the fibered product with the function field $k(C)$ of C over $k(C)$ itself. Since ξ is dominant, by Remark 2.2.15 there is an induced homomorphism $\xi^*\colon \operatorname{Div} S \to \operatorname{Div} E$ as well. All these homomorphisms denoted by ξ^* are compatible with each other. Shioda describes $\xi^*(D)$ as "the intersection of the horizontal part of the divisor D with the generic fiber E" and denotes it $D \cdot E$.

Remark 2.4.26 There are a few other ways to think about this homomorphism. Suppose D is an effective divisor of S and Y is its associated closed subscheme of S (see [Ha2], p. 145). Then the closed subscheme Z associated to the divisor $\xi^*(D)$ on E is $Z = Y \times_C \operatorname{Spec} K$, where $K = k(C)$ is the function field of C. In particular this implies that if $P \in S(C)$ is a section of g, then ξ^* sends the divisor $P(C)$ on S to the divisor $P(C) \times_C \operatorname{Spec} K$ on E, which gives a section in $E(K)$. By the universal property of fibered products, this yields exactly the correspondence between $S(C)$ and $E(K)$ as described in Lemma 2.3.13. If D has no vertical components, then Y is the closure of $\xi(Z)$ in S.

Lemma 2.4.27 *The homomorphism ξ^* induces a short exact sequence*

$$0 \to \operatorname{Div}_{\mathrm{vert}}(S) \to \operatorname{Div} S \xrightarrow{\xi^*} \operatorname{Div} E \to 0,$$

where $\operatorname{Div}_{\mathrm{vert}}(S)$ is the subgroup of $\operatorname{Div} S$ generated by vertical divisors. Furthermore, we have an equality $\deg(\xi^* D) = D \cdot F$ for any fiber F.

Proof. Clearly, we have a containment $\operatorname{Div}_{\mathrm{vert}}(S) \subset \ker \xi^*$. As $\operatorname{Div} S$ is isomorphic to $\operatorname{Div}_{\mathrm{vert}}(S) \oplus \operatorname{Div}_{\mathrm{hor}}(S)$ (see Remark 2.3.5), it suffices to show that $\xi^*\colon \operatorname{Div}_{\mathrm{hor}}(S) \to \operatorname{Div} E$ is an isomorphism. This follows from last statement of Remark 2.4.26, but we will use a different argument that will also be useful for the last equality of this Lemma. The horizontal prime divisors of S correspond with the discrete valuation rings of $k(S)$ containing $g^*k(C) \cong K$. As $k(S)$ is isomorphic to $K(E)$, these are the discrete valuation rings of $K(E)$ containing K, which correspond exactly with the K-rational points of E. The last equality follows from the fact that for a horizontal prime divisor D, both sides equal the degree of the residue field of its local ring over K. For vertical divisors, both sides equal 0. $\square$

Lemma 2.4.28 *The homomorphism $g^*\colon \operatorname{Div}^0 C \to \operatorname{Div}^0 S$ is injective and the cokernel is naturally isomorphic to $K(E)^*/K^*$.*

Proof. We consider the short exact sequences $0 \to k(C)^*/k^* \to \operatorname{Div}^0 C \to \operatorname{Pic}^0 C \to 0$ and $0 \to k(S)^*/k^* \to \operatorname{Div}^0 S \to \operatorname{Pic}^0 S \to 0$ and apply the snake lemma to the map g^* from the former to the latter exact sequence. The kernels are trivial because g^* is a section of $\mathcal{O}^*$. The cokernels on the outside are $k(S)^*/k(C)^*$ and 0 (by Theorem 2.4.24), so the snake lemma tells us that the cokernel in the middle is also isomorphic to $k(S)^*/k(C)^*$, which is isomorphic to $K(E)^*/K^*$.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & k(C)^*/k^* \arrow[r] \arrow[d, "g^*"'] & \operatorname{Div}^0 C \arrow[r] \arrow[d, "g^*"'] & \operatorname{Pic}^0 C \arrow[r] \arrow[d, "g^*"'] & 0 \\
0 \arrow[r] & k(S)^*/k^* \arrow[r] \arrow[d] & \operatorname{Div}^0 S \arrow[r] \arrow[d] & \operatorname{Pic}^0 S \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & k(S)^*/k(C)^* \arrow[r] \arrow[d] & K(E)^*/K^* \arrow[r] \arrow[d] & 0 & \\
 & 0 & 0 & &
\end{tikzcd}$$

$\square$

Recall that T_1 denotes the group $\mathbb{Z}F \oplus \bigoplus_{v\in C} \Lambda_1(v)$ from Lemma 2.4.19.

Proposition 2.4.29 *There is a natural short exact sequence*

$$0 \to T_1 \to \operatorname{NS}(S) \xrightarrow{\varphi} \operatorname{Pic} E \to 0,$$

where the first map is induced by the natural map from $\operatorname{Div}_{\mathrm{vert}} S$ to $\operatorname{NS}(S)$ and the map φ is induced by the composition of the maps $\xi^*\colon \operatorname{Div} S \to \operatorname{Div} E$ and $\operatorname{Div} E \to \operatorname{Pic} E$.

Proof. We have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Div}^0 C \arrow[r, "g^*"] \arrow[d, "g^*"'] & \mathrm{Div}_{\mathrm{vert}} S \arrow[d] \\
0 \arrow[r] & \mathrm{Div}^0 S \arrow[r] & \mathrm{Div}\, S
\end{tikzcd}$$

which induces a homomorphism between the cokernels of the horizontal maps, i.e., a homomorphism $T_1 \to \mathrm{NS}(S)$. Now we apply the snake lemma. The left vertical map is injective and has cokernel $K(E)^*/K^*$ by Lemma 2.4.28. The second vertical map is injective and has cokernel $\mathrm{Div}\, E$ by Lemma 2.4.27. Tracing arrows we find that the homomorphism $K(E)^*/K^* \to \mathrm{Div}\, E$ between these two cokernels is exactly the well known map that sends a rational function to the principal divisor associated to it. Thus, this map is injective with cokernel $\mathrm{Pic}\, E$. The snake lemma gives us the following commutative diagram in which all horizontal and vertical sequences are exact.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathrm{Div}^0 C \arrow[r, "g^*"] \arrow[d, "g^*"'] & \mathrm{Div}_{\mathrm{vert}} S \arrow[r] \arrow[d] & T_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Div}^0 S \arrow[r] \arrow[d] & \mathrm{Div}\, S \arrow[r] \arrow[d] & \mathrm{NS}(S) \arrow[r] \arrow[d, "\varphi"] & 0 \\
0 \arrow[r] & K(E)^*/K^* \arrow[r] \arrow[d] & \mathrm{Div}\, E \arrow[r] \arrow[d] & \mathrm{Pic}\, E \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

□

The two 3×3 diagrams from the proofs of Lemma 2.4.28 and Proposition 2.4.29 fit together in the following big commutative cube.

$$\begin{tikzcd}
& & \operatorname{Pic}^0 C \arrow[rrr, "g^*"] \arrow[ddd, "g^*"'] & & & \operatorname{Pic}_{\mathrm{vert}} S \arrow[rrr] \arrow[ddd] & & & T_1 \arrow[ddd] \\
& \operatorname{Div}^0 C \arrow[ur] \arrow[rrr, "g^*"] \arrow[ddd, "g^*"'] & & & \operatorname{Div}_{\mathrm{vert}} S \arrow[ur] \arrow[rrr] \arrow[ddd] & & & T_1 \arrow[ur] \arrow[ddd] & \\
k(C)^*/k^* \arrow[ur] \arrow[rrr] \arrow[ddd] & & & k(C)^*/k^* \arrow[ur] \arrow[rrr] \arrow[ddd] & & & 0 \arrow[ur] \arrow[ddd] & & \\
& & \operatorname{Pic}^0 S \arrow[rrr] \arrow[ddd] & & & \operatorname{Pic} S \arrow[rrr] \arrow[ddd, "\xi^*"] & & & \mathrm{NS}(S) \arrow[ddd, "\varphi"] \\
& \operatorname{Div}^0 S \arrow[ur] \arrow[rrr] \arrow[ddd] & & & \operatorname{Div} S \arrow[ur] \arrow[rrr] \arrow[ddd, "\xi^*"] & & & \mathrm{NS}(S) \arrow[ur] \arrow[ddd, "\varphi"] & \\
k(S)^*/k^* \arrow[ur] \arrow[rrr] \arrow[ddd] & & & k(S)^*/k^* \arrow[ur] \arrow[rrr] \arrow[ddd, "\xi^*"] & & & 0 \arrow[ur] \arrow[ddd] & & \\
& & 0 \arrow[rrr] & & & \operatorname{Pic} E \arrow[rrr] & & & \operatorname{Pic} E \\
& K(E)^*/K^* \arrow[ur] \arrow[rrr] & & & \operatorname{Div} E \arrow[ur] \arrow[rrr] & & & \operatorname{Pic} E \arrow[ur] & \\
k(S)^*/k(C)^* \arrow[ur] \arrow[rrr] & & & K(E)^*/K^* \arrow[ur] \arrow[rrr] & & & 0 \arrow[ur] & &
\end{tikzcd}$$

Proposition 2.4.30 *All sequences in the cube above are short exact sequences (with the zeros left out).*

Proof. The two 3×3 diagrams from the proofs of Lemma 2.4.28 and Proposition 2.4.29 make up the left face and the plane between the front and back face respectively. Consider the 3×3 diagram between the left and the right face. Its bottom two rows are exact by definition. Exactness of the front vertical sequence in this subdiagram follows from the isomorphism $K(E) \cong k(S)$ and the equality $K = k(C)$. Exactness of the second vertical sequence is exactly Lemma 2.4.27. From the snake lemma it then follows that the kernel of $\xi^* \colon \operatorname{Pic} S \to \operatorname{Pic} E$ is equal to the image of $\operatorname{Div}_{\mathrm{vert}} S$ in $\operatorname{Pic} S$, i.e., $\ker \xi^* = \operatorname{Pic}_{\mathrm{vert}} S$. Now consider the top face of the cube. We already know the left two sequences are exact. The snake lemma then shows that the cokernel of $g^* \colon \operatorname{Pic}^0 C \to \operatorname{Pic}_{\mathrm{vert}} S$ is isomorphic to the cokernel of $g^*\colon \operatorname{Div}^0 C \to \operatorname{Div}_{\text{vert}} S$, i.e., to T_1. The exactness of all other sequences is now obvious. $\square$

Remark 2.4.31 The homomorphism $\varphi\colon \mathrm{NS}(S) \to \operatorname{Pic} E$ can also be constructed as follows. By (2.2) the composition $g \circ \xi\colon E \to S \to C$ factors through $\operatorname{Spec} K$, so the homomorphism $\xi^* \circ g^*\colon \operatorname{Pic} C \to \operatorname{Pic} S \to \operatorname{Pic} E$ factors through $\operatorname{Pic}(\operatorname{Spec} K) = 0$. Hence we get an inclusion $g^* \operatorname{Pic}^0 C \subset g^* \operatorname{Pic} C \subset \ker \xi^*$, so ξ^* factors through $\operatorname{Pic} S/g^*(\operatorname{Pic}^0 C)$, which is isomorphic to $\mathrm{NS}(S)$ by Theorem 2.4.24.

Let Σ denote the homomorphism $\operatorname{Pic} E \to E(K)$ that sends the prime divisor (P) to P for any $P \in E(K)$. Let $\psi\colon \mathrm{NS}(S) \to E(K)$ be the composition of φ and Σ and set $T = \ker \psi$. Let ρ and r denote the rank of $\mathrm{NS}(S)$ and $E(K)$ respectively. Let $U \subset \mathrm{NS}(S)$ be the group generated by divisor classes of any fiber F and the section $(\mathcal{O})$.

$$\begin{tikzcd}
 & & \operatorname{Pic} S \arrow[r, "\xi^*"] \arrow[d] & \operatorname{Pic} E \arrow[d, "\Sigma"] \\
0 \arrow[r] & T \arrow[r] & \mathrm{NS}(S) \arrow[r, "\psi"'] \arrow[ur, "\varphi"] & E(K)
\end{tikzcd}$$

Theorem 2.4.32 *The homomorphism ψ is surjective and maps (P) to P. The kernel T is a sublattice of $\mathrm{NS}(S)$ of signature $(1, \operatorname{rk} T - 1)$. It is generated by $(\mathcal{O})$ and the irreducible components of the singular fibers of g, and it is isomorphic to the orthogonal direct sum of the unimodular lattice U and $\bigoplus_{v \in C} \Lambda_1(v)$. The rank of T equals $\operatorname{rk} T = 2 + \sum_v (m_v - 1)$. We have $\rho = r + 2 + \sum_v (m_v - 1)$.*

Proof. Most of this is in [Shi3], Thm. 1.3. Let $P \in E(K)$ be any K-point on E. By Lemma 2.3.13 it corresponds to a section in $S(C)$. By Remark 2.4.26 the homomorphism $\xi^*\colon \operatorname{Pic} S \to \operatorname{Pic} E$ sends the associated divisor $(P)_S$ on S to the associated divisor $(P)_E$ on E, which gets mapped to P by Σ. This proves the first statement.

The homomorphism $\deg\colon \operatorname{Pic} E \to \mathbb{Z}$ sending a divisor class D to its degree yields a split short exact sequence

$$0 \to \operatorname{Pic}^0 E \to \operatorname{Pic} E \to \mathbb{Z} \to 0.$$

A section $\mathbb{Z} \to \operatorname{Pic} E$ of the map deg is given by sending 1 to $(\mathcal{O})$. The associated homomorphism $\pi\colon \operatorname{Pic} E \to \operatorname{Pic}^0 E$ maps D to $D - (\deg D)(\mathcal{O})$. The map $\Sigma\colon \operatorname{Pic} E \to E(K)$ factors as the composition of π and the usual isomorphism $\operatorname{Pic}^0 E \to E(K)$ sending $(P) - (\mathcal{O})$ to P (see [Si1], Prop. III.3.4). Thus T is also the kernel of the composition $\sigma = \pi \circ \varphi$.

$$\begin{tikzcd}
 & & \operatorname{Pic} S \arrow[r, "\xi^*"] \arrow[d] & \operatorname{Pic} E \arrow[d, "\pi"] \arrow[dr, "\Sigma"] & \\
0 \arrow[r] & T \arrow[r] & \mathrm{NS}(S) \arrow[ur, "\varphi"] \arrow[r, "\sigma"] \arrow[rr, bend right, "\psi"'] & \operatorname{Pic}^0 E \arrow[r, "\cong"] & E(K)
\end{tikzcd}$$

Now we apply the snake lemma to the following diagram.

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & & 0 \arrow[d] & \mathbb{Z} \arrow[d] & \\
0 \arrow[r] & T_1 \arrow[r] \arrow[d] & \mathrm{NS}(S) \arrow[r, "\varphi"] \arrow[d, equal] & \operatorname{Pic} E \arrow[r] \arrow[d, "\pi"] & 0 \\
0 \arrow[r] & T \arrow[r] & \mathrm{NS}(S) \arrow[r, "\sigma"'] \arrow[d] & \operatorname{Pic}^0 E \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 &
\end{tikzcd}$$

The snake lemma implies that the map $T_1 \to T$ is injective with cokernel $\mathbb{Z}$. Hence we get a short exact sequence

$$0 \to T_1 \to T \to \mathbb{Z} \to 0.$$

A simple tracing of arrows shows that a section of the cokernel map $T \to \mathbb{Z}$ can be given by sending 1 to $(\mathcal{O}) \in T$. Hence we find an isomorphism

$$T \cong \mathbb{Z}(\mathcal{O}) \oplus T_1 \cong \mathbb{Z}(\mathcal{O}) \oplus \mathbb{Z}F \oplus \bigoplus_{v \in C} \Lambda_1(v) \cong U \oplus \bigoplus_{v \in C} \Lambda_1(v).$$

From Remark 2.4.21 we find that the lattice U is orthogonal to $\bigoplus_{v \in C} \Lambda_1(v)$. From the intersection numbers $F^2 = 0$, $(\mathcal{O})^2 = -\chi$, and $F \cdot (\mathcal{O}) = 1$, we find that U is unimodular with Gram matrix associated to the basis $\{(\mathcal{O}), F\}$ equal to

$$\begin{pmatrix} -\chi & 1 \\ 1 & 0 \end{pmatrix}.$$

The signature of T follows from the fact that $\bigoplus_{v \in C} \Lambda_1(v)$ is negative definite (see Proposition 2.4.4) and U has signature $(1, 1)$. From Proposition 2.4.4 we also conclude $\operatorname{rk} T_1 = 1 + \sum_{v \in C}(m_v - 1)$. The rank of $T \cong T_1 \oplus \mathbb{Z}$ follows immediately. From the short exact sequence

$$0 \to T \to \mathrm{NS}(S) \to E(K) \to 0 \qquad (2.7)$$

we conclude $\rho = \operatorname{rk} \mathrm{NS}(S) = \operatorname{rk} T + \operatorname{rk} E(K) = 2 + \sum_{v \in C}(m_v - 1) + r$. □

Proof of Theorem 2.4.1. This follows immediately from Theorem 2.4.32. □

We will now take a closer look at the lattice structure of the Néron-Severi group $\mathrm{NS}(S)$ and deduce that we can give the group $E(K)/E(K)_{\mathrm{tors}}$ the structure of a positive definite lattice. Set $W = U^{\perp}$ and $L = T^{\perp}$, where the orthogonal complements are taken in $\mathrm{NS}(S)$.

Lemma 2.4.33 *The lattice W is an even, negative definite lattice. The Néron-Severi group $\mathrm{NS}(S)$ is the orthogonal direct sum of U and W. The sublattice L is the orthogonal complement of $\bigoplus_{v \in C} \Lambda_1(v)$ in W. We have the following ranks and discriminants.*

lattice	*rank*	*discriminant*
W	$\rho - 2$	$-\operatorname{disc} \mathrm{NS}(S)$
$\bigoplus_{v \in C} \Lambda_1(v)$	$\sum_{v \in C}(m_v - 1)$	$(-1)^{\sum(m_v - 1)} \prod_{v \in C} m_v^{(1)}$
T	$2 + \sum_{v \in C}(m_v - 1)$	$(-1)^{\operatorname{rk} T - 1} \prod_{v \in C} m_v^{(1)}$
L	r	$\operatorname{disc} \mathrm{NS}(S)[\mathrm{NS}(S) : L \oplus T]^2 / \operatorname{disc} T =$ $\pm \operatorname{disc} W [W : L \oplus \bigoplus_{v \in C} \Lambda_1(v)]^2 / \prod_{v \in C} m_v^{(1)}$

Proof. See [Shi3], § 7. Since U has signature $(1, 1)$ and $\mathrm{NS}(S)$ has signature $(1, \rho - 1)$, we find that W is negative definite. To prove that W is even we follow Shioda's proof, see [Shi3], Thm. 7.4. Let D be an effective divisor with equivalence class in W. Then in particular we have $D \cdot F = 0$, so by Theorem 2.3.10 we have $D \cdot K_S = 0$, where K_S is a canonical divisor on S. Hence from the adjunction formula $2p_a(D) - 2 = D \cdot (D + K_S)$, we find that D^2 is even. Here $p_a(D)$ denotes the arithmetic genus of the closed subscheme associated to D. As W is generated by divisor classes of effective divisors, we conclude that W is even. Since U is unimodular, the second statement follows from Lemma 2.1.14. Then the formulas for the rank and discriminant of W follow from the fact that we have $\operatorname{rk} U = 2$ and $\operatorname{disc} U = -1$.

Let T_0 denote the lattice $\bigoplus_{v \in C} \Lambda_1(v)$. Theorem 2.4.32 tells us that T is isomorphic to the orthogonal direct sum of T_0 and U. Hence the orthogonal complement $L = T^{\perp}$ of $T = T_0 \oplus U$ in $\mathrm{NS}(S) = W \oplus U$ is equal to the orthogonal complement of T_0 in W. Proposition 2.4.4 gives the rank and discriminant of T_0, from which we find those of T. Since L is the orthogonal complement of T in $\mathrm{NS}(S)$, we find $\operatorname{rk} L = \operatorname{rk} \mathrm{NS}(S) - \operatorname{rk} T$, which equals r by Theorem 2.4.32. The formula for the discriminant of L follows from Lemma 2.1.15 by considering L as the orthogonal complement either of T in $\mathrm{NS}(S)$ or of T_0 in W. □

Set

$$m = \operatorname{lcm}\{m_v^{(1)} \mid v \in C\} \tag{2.8}$$

and write

$$E(K)^0 = \left\{ P \in E(K) \;\middle|\; \begin{array}{l} (P) \text{ intersects all fibers in the same} \\ \text{irreducible component as } (\mathcal{O}) \end{array} \right\}.$$

Theorem 2.4.34 *Let m be as in* (2.8)*. The projection* $\mathrm{NS}(S) \to L_{\mathbb{Q}}$ *induces a homomorphism* $\gamma\colon E(K) \cong \mathrm{NS}(S)/T \to \frac{1}{m}L \cap L^*$ *with kernel* $E(K)_{\mathrm{tors}}$*. The set* $E(K)^0$ *is a torsion-free subgroup of* $E(K)$ *of finite index. The map* γ *sends* $E(K)^0$ *isomorphically to* L*.*

Proof. This is slightly stronger than [Shi3], Thm. 8.9. First we will show $mT'^* \subset T'$. As $\mathrm{NS}(S)$ is integral, we have a series of inclusions $T^* \subset T'^* \subset T' \subset T$, so it suffices to show $mT^* \subset T$. By Theorem 2.4.32 it is enough to show $mU^* \subset U$ and $m\Lambda_1(v)^* \subset \Lambda_1(v)$ for all $v \in C$. For U this follows from the fact that U is unimodular, so $U^* = U$. By Lemma 2.1.13 and Proposition 2.4.4 we have $[\Lambda_1(v)^* : \Lambda_1(v)] = m_v^{(1)}|m$, so m annihilates $\Lambda_1(v)^*/\Lambda_1(v)$. This shows that we can apply Lemma 2.1.20. For Λ and T in Lemma 2.1.20 take $\mathrm{NS}(S)$ and T respectively. Then the lattice denoted by L in Lemma 2.1.20 corresponds to our L, and the group A in Lemma 2.1.20 corresponds to $E(K)$. As in Lemma 2.1.20, let M denote the kernel of the homomorphism $E(K) \cong \mathrm{NS}(S)/T \to T'^*/T$ induced by the projection $\mathrm{NS}(S) \to T_{\mathbb{Q}}$. Everything follows from Lemma 2.1.20 if we show $M = E(K)^0$. Shioda's proof of the inclusion $M \subset E(K)^0$ is fairly imprecise.

Take $P \in E(K)^0 \subset \mathrm{NS}(S)/T$. By Theorem 2.4.32 the element P is represented by the divisor $(P) \in \mathrm{NS}(S)$. By Remark 2.4.21 we find $(P) \cdot D = 0$ for every $D \in \Lambda_1(v)$. As $\Lambda_1(v)$ is negative definite, the projection of (P) to $\Lambda_1(v)$ vanishes and we find that under the projection $\mathrm{NS}(S) \to T_{\mathbb{Q}} \cong U_{\mathbb{Q}} \oplus (\bigoplus_{v \in C} \Lambda_1(v))_{\mathbb{Q}}$ the divisor (P) maps to $U^* = U \subset T$, so we get $P \in M$. Conversely, take $P \in M$. Again P is represented by the divisor (P). Take any $v \in C$. By definition of M, the orthogonal projection of (P) to $T_{\mathbb{Q}}$ is contained in T, so in particular the projection Γ of (P) to $(U \oplus \Lambda_1(v))_{\mathbb{Q}} \subset T_{\mathbb{Q}}$ is contained in $U \oplus \Lambda_1(v) \cong \mathbb{Z}(\mathcal{O}) \oplus \Lambda(v)$. We have $\Gamma \cdot z = (P) \cdot z$ for every $z \in \mathbb{Z}(\mathcal{O}) \oplus \Lambda(v)$. From $(P) \cdot F = 1$ we can compute the coefficient of $(\mathcal{O})$ and we find that we can write $\Gamma = (\mathcal{O}) + \Gamma_v$ with $\Gamma_v \in \Lambda(v)$. Let $\Theta_{\mathcal{O}}$ and Θ_P denote the irreducible components of F_v that intersect $(\mathcal{O})$ and (P) respectively. Suppose $\Theta_{\mathcal{O}} \neq \Theta_P$. Then for every irreducible component Θ of $g^{-1}(v)$ we get

$$\Gamma_v \cdot \Theta = \Gamma \cdot \Theta - (\mathcal{O}) \cdot \Theta = ((P) - (\mathcal{O})) \cdot \Theta = \begin{cases} 1 & \text{if } \Theta = \Theta_P, \\ -1 & \text{if } \Theta = \Theta_{\mathcal{O}}, \\ 0 & \text{otherwise.} \end{cases}$$

However, from the classification of singular fibers in Theorem 2.4.17 we easily verify that such a Γ_v does not exist. We conclude $\Theta_P = \Theta_{\mathcal{O}}$, and thus $P \in E(K)^0$. □

By considering $L(-1)$ instead, i.e., the lattice L but with the opposite of its pairing, we can embed $E(K)/E(K)_{\mathrm{tors}}$ in a positive definite lattice, as stated in the following corollary.

Corollary 2.4.35 *Let m be as in* (2.8)*. The homomorphism γ induces a natural homomorphism $\overline{\gamma}\colon E(K) \to \frac{1}{m}L(-1) \cap L(-1)^*$ inducing the following commutative diagram.*

$$\begin{tikzcd} E(K)/E(K)_{\mathrm{tors}} \arrow[r, hook, "\overline{\gamma}"] & \frac{1}{m}L(-1) \cap L(-1)^* \\ E(K)^0 \arrow[u, hook] \arrow[r, "\overline{\gamma}", "\cong"'] & L(-1) \arrow[u, hook] \end{tikzcd}$$

This induces a symmetric bilinear pairing on $E(K)$ and it induces the structure of a positive definite lattice on $E(K)/E(K)_{\mathrm{tors}}$ with an even sublattice $E(K)^0$. The corresponding pairing is equal to the canonical height pairing $(P,Q) \mapsto h(P+Q) - h(P) - h(Q)$, where h is height associated to the ample divisor $(\mathcal{O})$.

Proof. The diagram follows immediately from Theorem 2.4.34. Since L is negative definite, $L(-1)$ is positive definite. By Lemma 2.4.33 the lattice $L \subset W$ is even. For the last statement, see [Si2], Theorem III.9.3. □

Remark 2.4.36 The lattice $E(K)/E(K)_{\mathrm{tors}}$ together with the positive definite pairing described in Corollary 2.4.35 is called the *Mordell-Weil lattice*. The pairing itself is called the *height pairing*. By tracing down the maps that define it, Shioda ([Shi3], Thm 8.6) gives an explicit formula for the height pairing of two sections P and Q. It is based only on the intersection numbers $(P) \cdot (Q)$, $(P) \cdot (\mathcal{O})$, $(Q) \cdot (\mathcal{O})$, and $((P) - (\mathcal{O})) \cdot \Theta$ for any irreducible component Θ of a singular fiber.

Lemma 2.4.37 *The discriminant of the Néron-Severi group and the Mordell-Weil lattice $E(K)/E(K)_{\mathrm{tors}}$ are related by the equation*

$$\operatorname{disc} \mathrm{NS}(S) = \frac{\operatorname{disc}\left(E(K)/E(K)_{\mathrm{tors}}\right) \cdot \prod_v m_v(1)}{|E(K)_{\mathrm{tors}}|^2}.$$

Proof. This follows immediately from Lemma 2.1.21 and 2.4.33. See also [Shi1], Cor. 1.7. □

Proposition 2.4.38 *Let m be as in* (2.8)*. The values of the height pairing are contained in $\frac{1}{m}\mathbb{Z}$.*

Proof. Let M denote the intersection $\frac{1}{m}L(-1) \cap L^*(-1)$. Then the height pairing factors through the pairing $M \times M \to \mathbb{Q}$ by Corollary 2.4.35. For $x, y \in M$ we get $m\langle x, y\rangle = \langle mx, y\rangle \in \mathbb{Z}$ as we have $mx \in L(-1)$ and $y \in L(-1)^*$. □

2.5 Two constructions of elliptic surfaces

In this section we will prove that under mild conditions a fan of hyperplane sections of a degree 3 surface in $\mathbb{P}^3$ gives rise to an elliptic surface. This statement is well known, at least for nonsingular surfaces in characteristic 0, but details such as the existence of singular fibers are often overlooked. Also under mild conditions a base extension of an elliptic surface gives rise again to an elliptic surface. Both statements appear to lack proofs in the literature, so we include them here.

Definition 2.5.1 *A surface X over an algebraically closed field k has a* rational singularity *at a point x if there exist a surface Y and a projective, birational morphism $f: Y \to X$ that is an isomorphism from $f^{-1}(X - \{x\})$ to $X - \{x\}$ and such that we have $R^1 f_* \mathcal{O}_Y = 0$ and $f^{-1}(U)$ is smooth over k for some open neighborhood U of x.*

Remark 2.5.2 Let $f: Y \to X$ be a resolution of a singularity at x on X with exceptional curve (possibly reducible) E. Then x is a rational singularity if and only if for every positive divisor Z on Y with support in E the arithmetic genus $p_a(Z)$ satisfies $p_a(Z) \leq 0$, see [Ar], Prop. 1.

Proposition 2.5.3 *Let k be any field of characteristic not equal to 2 or 3, contained in an algebraically closed field k'. Let X be a projective, irreducible surface in $\mathbb{P}^3_k$ of degree 3, such that $X_{k'}$ is regular outside a finite number of rational singularities. Let L be a line that intersects X in three different nonsingular points M_1, M_2, and M_3. Identify $\mathbb{P}^1$ with the family of hyperplanes in $\mathbb{P}^3$ through L and let $f: X \dashrightarrow \mathbb{P}^1$ be the rational map that sends every point of X to the hyperplane it lies in. Let $\pi: \widetilde{X} \to X$ be a minimal desingularization of the blow-up of X at the M_i. For $i = 1, 2, 3$, let $\widetilde{M_i}$ denote the exceptional curve above M_i on $\widetilde{X}$. Then $f \circ \pi$ extends to a morphism $\widetilde{f}$. It maps the $\widetilde{M_i}$ isomorphically to $\mathbb{P}^1$, yielding at least three sections. Together with any of its sections, $\widetilde{f}$ makes $\widetilde{X}_{k'}$ into a rational elliptic surface over $\mathbb{P}^1_{k'}$.*

Remark 2.5.4 O'Sullivan ([O'Su], Prop. VI.1.1) shows that any normal cubic surface in $\mathbb{P}^3$ that is not a cone has only rational double points. He excludes characteristics 2, 3, and 5, but describes how his results could be extended to any characteristic using results from Lipman [Lip]. For a published reference, see [BW] (characteristic 0).

The proof of Proposition 2.5.3 consists of several steps. For clarity, we will prove them in separate lemmas. Let $k, k', L, X, \widetilde{X}, \pi, M_i, \widetilde{M_i}, f$, and $\widetilde{f}$ be as in Proposition 2.5.3. First we will show that $\widetilde{X}$ is rational, smooth, and irreducible. Then we show that $\widetilde{f}$ is a morphism that has a section. We proceed by showing that almost all fibers are nonsingular of genus 1. After that, we see that $\widetilde{f}$ is not smooth and finally, we will show that $\widetilde{f}$ is a relatively minimal fibration. Note that if L is defined over k, then so is f. If M_i is a k-point, then the section $\mathcal{O}$ corresponding to $\widetilde{M_i}$ is defined over k as well. All other statements are geometric, so without loss of generality we will assume that $k = k'$.

Lemma 2.5.5 *Under the assumptions of Proposition* 2.5.3 *the surface* $\widetilde{X}$ *is rational, smooth, and irreducible.*

Proof. By construction, $\widetilde{X}$ is smooth. It is irreducible because X is, and $\pi\colon \widetilde{X} \to X$ is birational. Obviously, to show that $\widetilde{X}$ is rational, it suffices to show that X is rational. It is a classical result that nonsingular cubics are obtained by blowing up 6 points in general position in $\mathbb{P}^2$, whence they are rational. For this statement, see [Ha2], § V.4, in particular Rem. V.4.7.1. Proofs are given in [Man], § 24 or [Na], I, Thm. 8, p. 366.

For the singular case, note that X is not a cone. Indeed, the exceptional curve E of the desingularization of a cone over a plane cubic is isomorphic to that cubic, see [Ha2], exc. II.5.7. Hence, it would satisfy $p(E) = 1$, which contradicts Remark 2.5.2. As X is not a cone, projection from any singular point x will give a dominant rational map from X to $\mathbb{P}^2$. It is birational because every line through x that is not contained in X intersects X by Bézout's Theorem in only one more point. □

Lemma 2.5.6 *The rational map* $\widetilde{f}$ *extends to a morphism, mapping* $\widetilde{M_i}$ *isomorphically to* $\mathbb{P}^1$*.*

Proof. The rational map f is defined everywhere, except at the M_i, whence the composition $f \circ \pi$ is well-defined outside the $\widetilde{M_i}$. Any point P on $\widetilde{M_i}$ corresponds to a direction at M_i on X. Since L intersects X in three different points and the total intersection $L \cdot X$ has degree 3 by Bézout's Theorem, it follows that L is not tangent to X, so these directions at M_i are cut out by the planes through L. The map $f \circ \pi$ extends to a morphism $\widetilde{f}$ by sending $P \in \widetilde{M_i}$ to the plane that cuts out the direction at M_i that P corresponds to. Thus, it induces an isomorphism from the $\widetilde{M_i}$ to $\mathbb{P}^1$. □

Note that if a hyperplane H does not contain any singular points of X, then the fiber of $\widetilde{f}$ above H is isomorphic to $H \cap X$. Here the missing points M_i in $f^{-1}(H) = (H \cap X) \setminus \{M_1, M_2, M_3\}$ are filled in by the appropriate points on $\widetilde{M_i}$. To prove that almost all fibers are nonsingular curves of genus 1 we will use Proposition 2.5.8. Its proof was suggested by B. Poonen.

Lemma 2.5.7 *Any connected, regular variety is integral.*

Proof. Let Z be such a variety. Then Z is reduced, so it suffices to show that Z is irreducible. The minimal primes of the local ring of a point on Z correspond to the components it lies on. As a regular local ring has only one minimal prime ideal, we conclude that every point of Z lies on exactly one component. As Z is connected, Z is irreducible. □

Proposition 2.5.8 *Let* Y *be a geometrically connected, regular variety over a field* l*. If* Y *contains a closed point of which the residue field is separable over* l*, then* Y *is geometrically integral.*

Proof. Let l^{sep} denote a separable closure of l. As separable extensions preserve regularity (see [EGA IV(2)], Prop. 6.7.4), we find that $Y_{l^{\mathrm{sep}}}$ is regular. As it is connected as well, $Y_{l^{\mathrm{sep}}}$ is integral by Lemma 2.5.7, whence irreducible. Over a separably closed field, irreducibility implies geometric irreducibility, see Proposition 2.2.8, part (i). Therefore $Y_{\bar{l}}$ is irreducible.

Let c be the closed point mentioned. Then the local ring $\mathcal{O}_{Y,c}$ is regular, with residue field separable over l. From [EGA IV(1)], Thm. 19.6.4, we find that the ring $\mathcal{O}_{Y,c}$ is formally smooth over l. By [EGA IV(2)], Thm. 6.8.6, this implies that Y is smooth (over l) at c. As smoothness is an open condition (see [EGA IV(2)], Cor. 6.8.7), there is a nonempty open subset $U \subset Y$ such that Y is smooth at all $x \in U$. As smoothness is a local condition, U is smooth, whence geometrically regular.

As $Y_{\bar{l}}$ is irreducible, the subset $U_{\bar{l}}$ is dense and also irreducible, whence connected. It is also regular, so it is integral by Lemma 2.5.7. Therefore, U is geometrically integral, which for an integral scheme over l is equivalent to the fact that its function field is a primary and separable field extension of l, see [EGA IV(2)], Cor. 4.6.3. As Y is integral and the function field $k(Y)$ of Y is isomorphic to the function field $k(U)$ of U, it follows that Y is geometrically integral as well. □

Lemma 2.5.9 *Under the assumptions of Proposition* 2.5.3 *almost all fibers are nonsingular curves of genus* 1*.*

Proof. It follows from Remark 2.3.2 that almost all fibers are nonsingular if char $k = 0$. Suppose char $k = p > 3$. We will first show that the generic fiber $E = \widetilde{X} \times_{\mathbb{P}^1} \operatorname{Spec} k(t)$ above the generic point $\eta : \operatorname{Spec} k(t) \to \mathbb{P}^1$ of $\mathbb{P}^1$ is regular. Then we will show E is geometrically integral of genus 1 and finally we will conclude it is smooth over $\operatorname{Spec} k(t)$.

Take a point $P \in E$ and let $x \in \widetilde{X}$ be the image of P under the projection $\varphi\colon E \to \widetilde{X}$. On every open $U = \operatorname{Spec} A \subset \mathbb{P}^1$, the map η is given by the localization map $\psi\colon A \hookrightarrow k(t)$. As fibered products of affine spaces come from tensor products, which commute with localization, the map $\varphi^{\#}\colon \mathcal{O}_{\widetilde{X},x} \to \mathcal{O}_{E,P}$ on local A-algebras is induced by ψ. The maximal ideal of $\mathcal{O}_{\widetilde{X},x}$ pulls back under $\widetilde{f}^{\#}|_A\colon A \to \mathcal{O}_{\widetilde{X},x}$ to the prime ideal of A corresponding to $\widetilde{f}(x) = \operatorname{im} \eta$, i.e., to (0). Hence, all nonzero elements of A are already invertible in $\mathcal{O}_{\widetilde{X},x}$, so the map $\mathcal{O}_{\widetilde{X},x} \to \mathcal{O}_{E,P}$ is in fact an isomorphism. Since $\widetilde{X}$ is regular by Lemma 2.5.5, we conclude that $\mathcal{O}_{\widetilde{X},x} \cong \mathcal{O}_{E,P}$ is a regular local ring, so E is regular.

Also, for any extension field F of $k(t)$ the scheme $E \times_{k(t)} F$ is a cubic in $\mathbb{P}^2_F$, so it is connected. Thus, E is geometrically connected. As in Lemma 2.3.13, the sections $\widetilde{M}_i$ determine $k(t)$-points on E. From Proposition 2.5.8 we find that E is geometrically integral. As E is a regular, geometrically integral, plane cubic curve, it has genus $g(E) = 1$. Here we define the genus $g(C)$ of a regular (but possibly not smooth), projective, and geometrically integral curve C by the common value of its arithmetic genus $p_a(C)$ and its geometric genus $p_g(C) = \dim H^0(C, \omega_C^\circ)$, where ω_C° is the dualizing sheaf of C, see [Ha2], III.7.

Now, if E were not smooth over $k(t)$, then there would be a finite extension $F/k(t)$ such that $E_F = E \times_{k(t)} F$ is not regular. Any nonregular plane cubic has genus 0, so $g(E_F) = 0$. Let $K/k(t)$ be the subfield of F such that $K/k(t)$ is separable and F/K is purely inseparable. Then by [EGA IV(2)], Prop. 6.7.4, the curve $E_K = E \times_{k(t)} K$ is regular, so $g(E_K) = 1$. By [Ta1], Cor. 1, the difference $g(E_K) - g(E_F) = 1$ is an integral multiple of $(p-1)/2$, so we find $p = 2$ or $p = 3$. Since we have $p > 0$, we conclude that E is smooth over η. As $\widetilde{f}$ is flat and projective, by [Ha2], exc. III.10.2, there is a dense open subset $U \subset \mathbb{P}^1$ on which $\widetilde{f}\colon \widetilde{f}^{-1}(U) \to U$ is smooth. By Remark 2.3.12 almost all fibers are then nonsingular. As they are plane cubics, they have genus 1. $\square$

Lemma 2.5.10 *Under the assumptions of Proposition* 2.5.3 *the morphism* $\widetilde{f}$ *is not smooth.*

Proof. By Remark 2.3.12, it suffices to prove that there exists a singular fiber. As there are only finitely many singular points on X, for almost all planes H through L the fiber $\widetilde{X}_H$ is isomorphic to $X \cap H$. As any two projective curves in $H \cong \mathbb{P}^2$ intersect, it follows that $\widetilde{X}_H$ is connected for all but finitely many H. Since $\widetilde{f}$ is flat (see Remark 2.3.2), it follows from the principle of connectedness (see [Ha2], exc. III.11.4) that the fiber $\widetilde{X}_H$ is connected for all H.

If X contains a singular point, then the fiber $\widetilde{X}_H$ of $\widetilde{f}$ above the plane H that it lies in contains an exceptional curve, so it is reducible and connected. From Lemma 2.5.7 we conclude that $\widetilde{X}_H$ is singular.

Hence, to prove the existence of a singular fiber we may assume that X is nonsingular. After a linear transformation, we may assume that $L \subset \mathbb{P}^3$ is given by $w = z = 0$ and X is given by $F = 0$ for some homogeneous polynomial $F \in k[x, y, z, w]$ of degree 3. Let $P \in X \subset \mathbb{P}^3$ be a point where both $\partial F/\partial x$ and $\partial F/\partial y$ vanish (the existence of P follows from the Projective Dimension Theorem, see [Ha2], Thm. I.7.2). Set $t_0 = (\partial F/\partial z)(P)$ and $t_1 = (\partial F/\partial w)(P)$. Then t_0 and t_1 are not both zero because P is nonsingular. The tangent plane T_P to X at P is then given by $t_0 z + t_1 w = 0$, so it contains L. The fiber $T_P \cap X$ above T_P is singular, as T_P is tangent at P. $\square$

Lemma 2.5.11 *Under the assumptions of Proposition* 2.5.3 *the morphism* $\widetilde{f}$ *is a relatively minimal fibration.*

Proof. By Lemmas 2.5.5, 2.5.6, and 2.5.9, the hypotheses of Theorem 2.3.10 are satisfied, so it suffices to show that $K_{\widetilde{X}}^2 = 0$. Let $\rho\colon X' \to X$ be the blow-up of X at the three points M_i, and let $\sigma\colon \widetilde{X} \to X'$ be the minimal desingularization of X'.

For any projective variety Z, let K_Z° denote the divisor associated to the dualizing sheaf ω_Z°, see [Ha2], § III.7. If Z is nonsingular, then K_Z° is linearly equivalent to the canonical divisor K_Z, see [Ha2], Cor. III.7.12. From [Ha2], Thm. III.7.11, we find that $\omega_X^\circ \cong \mathcal{O}_X(d-4)$ with $d = \deg X = 3$. Hence, if H is a hyperplane that does not meet any of the M_i or the singular points of X, then K_X° is linearly equivalent to $-(H \cap X)$.

Let U be the maximal smooth open subset of X, and set $V = \rho^{-1}(U)$. As V is isomorphic to U, blown up at three nonsingular points, we find by [Ha2], Prop. V.3.3, that $K_V = \rho^* K_U + \widetilde{M_1} + \widetilde{M_2} + \widetilde{M_3}$. Since ρ is an isomorphism outside the M_i, we find that $K^\circ_{X'} = \rho^* K^\circ_X + \widetilde{M}_1 + \widetilde{M}_2 + \widetilde{M}_3$. As K°_X does not meet the M_i, and $\widetilde{M}_i^2 = -1$ (see [Ha2], Prop. V.3.2) we get

$$(K^\circ_{X'})^2 = (\rho^* K^\circ_X)^2 + \widetilde{M}_1^2 + \widetilde{M}_2^2 + \widetilde{M}_3^2 = (K^\circ_X)^2 - 3 = (H \cap X)^2 - 3 = \deg X - 3 = 0.$$

Du Val [Du] proves that rational singularities do not affect adjunction, i.e., there is an isomorphism $\omega^\circ_{\widetilde{X}} \cong \sigma^* \omega^\circ_{X'}$, see also [Pi], § 15, Prop. 2, and § 17. Hence, we get $K_{\widetilde{X}} \sim K^\circ_{\widetilde{X}} \sim \sigma^* K^\circ_{X'}$. As σ is an isomorphism on $\sigma^{-1}(V)$, we get $K^2_{\widetilde{X}} = (\sigma^* K^\circ_{X'})^2 = (K^\circ_{X'})^2 = 0$. □

Proof of Proposition 2.5.3. This follows immediately from Lemmas 2.5.5, 2.5.6, 2.5.9, 2.5.10, and 2.5.11. □

Remark 2.5.12 If L intersects X in one of its singular points, then one could still define a fibration $\widetilde{X} \to \mathbb{P}^1$ in the same way as in Proposition 2.5.3. For almost all hyperplanes H the fiber above H will be the normalization of the singular cubic curve $H \cap X$. Hence this will not be an elliptic fibration.

Remark 2.5.13 In characteristic 3, all fibers might be singular, as is the case when X is given by $y^2z + yz^2 + wxy + wxz + xz^2 + wy^2 = 0$ and L is given by $x = w = 0$. The intersection of X with the plane H_t given by $w = tx$ is singular at the point $[x : y : z : w] = [1 : t^{1/3} : t^{2/3} : t]$ on the twisted cubic curve in $\mathbb{P}^3$. The plane H_t is tangent to X at that point. The only singular points of X are three ordinary double points at $[1 : 0 : 0 : 0]$, $[0 : 0 : 0 : 1]$, and $[1 : 1 : 1 : 1]$.

In characteristic 2, we can also get all fibers to be singular, as one easily checks in case X is given by $x^3 + x^2z + x^2w + y^3 + yzw = 0$ and L is given by $w = z = 0$. The only singular points on X are the ordinary double points $[0 : 0 : 0 : 1]$ and $[0 : 0 : 1 : 0]$.

In the proof of Proposition 2.5.3 the fact that the characteristic of k is not equal to 2 or 3 is only used in Lemma 2.5.9. Hence the conclusion of the proposition is also true in characteristic 2 and 3 if we add to the hypotheses that almost all planes through L are not tangent to X. By Bertini's Theorem, the set of planes that intersect X in a nonsingular curve is open (see [Ha2], Thm. II.8.18), so it suffices to require that there is at least one plane through L that is not tangent to X.

Remark 2.5.14 The singular points on X as in Proposition 2.5.3 can be used to find sections of $\widetilde{f}$. If X has two singular points P and Q, then the line l through P and Q lies on X, for if it did not, it would have intersection multiplicity at least 4 with X, but by Bézout's Theorem the intersection multiplicity should be 3. Therefore, either l intersects L and thus l is contained in the fiber above the plane that L, P, and Q all lie in, or l gives a section of $\widetilde{f}$.

The next proposition describes how to construct an elliptic surface by base extension of another elliptic surface. This construction will also be used in the proof of Theorem 4.1.1.

Proposition 2.5.15 *Let S be an elliptic surface over a smooth, irreducible, projective curve C over an algebraically closed field k, with fibration g and section $\mathcal{O}$ of g. Let $\gamma\colon C' \to C$ be a nonconstant map of curves from a smooth, irreducible, projective curve C', which is unramified above those points in C where g has singular fibers. Put $S' = S \times_C C'$, let g' be the projection $S' \to C'$, and let $\mathcal{O}'\colon C' \to S'$ denote the morphism induced by the identity on C' and the composition $\mathcal{O} \circ \gamma$. Then $\mathcal{O}'$ is a section of g' and they make S' into an elliptic surface over C'. The Euler characteristics $\chi_S = \chi(\mathcal{O}_S)$ and $\chi_{S'} = \chi(\mathcal{O}_{S'})$ are related by $\chi_{S'} = (\deg\gamma)\chi_S$.*

$$\begin{tikzcd}
S' \arrow[r] \arrow[d, "g'"] & S \arrow[d, "g"] \\
C' \arrow[u, bend left, "\mathcal{O}'"] \arrow[r, "\gamma"'] & C \arrow[u, bend left, "\mathcal{O}"]
\end{tikzcd}$$

Proof. Since projective morphisms are stable under base extension (see [Ha2], exc. II.4.9), we find that S' is projective over C', which is projective over $\operatorname{Spec} k$, so S' is projective. The composition $g' \circ \mathcal{O}'$ is by construction the identity on C', so $\mathcal{O}'$ is a section of g'.

As k is algebraically closed, the residue field $k(x)$ of a closed point $x \in C'$ is isomorphic to the residue field $k(\gamma(x))$. Hence the fiber above x is isomorphic to the fiber above $\gamma(x)$, as we have

$$\operatorname{Spec} k(x) \times_{C'} S' \cong \operatorname{Spec} k(x) \times_{C'} C' \times_C S \cong \operatorname{Spec} k(x) \times_C S \cong \operatorname{Spec} k(\gamma(x)) \times_C S.$$

Therefore, as for g, all fibers of g' are connected. As g is elliptic, all but finitely many fibers of g' will be smooth curves of genus 1. Since g has a singular fiber, so does g'. From Lemma 2.3.8 we find that $g'_*\mathcal{O}_{S'} \cong \mathcal{O}_{C'}$. As C' is irreducible and projective, this implies $\dim H^0(S', \mathcal{O}_{S'}) = \dim H^0(C', g'_*\mathcal{O}_{S'}) = \dim H^0(C', \mathcal{O}'_C) = 1$. We conclude that S' is connected.

To prove that S' is smooth and irreducible, set $h = \gamma \circ g'$. By assumption there are open $U, V \subset C$ with $U \cup V = C$, such that $\gamma|_{\gamma^{-1}(U)}$ is unramified, whence smooth, and $g|_{g^{-1}(V)}$ has no singular fibers, which implies it is smooth by Remark 2.3.12. As smooth morphisms are stable under base extension and composition (see [Ha2], Prop. II.10.1), we find first that $h^{-1}(U) = g^{-1}(U) \times_U \gamma^{-1}(U)$ is smooth over $g^{-1}(U) \subset S$. As S is smooth over k and $g^{-1}(U)$ is open in S, we conclude that $h^{-1}(U)$ is smooth over k. Similarly, $h^{-1}(V)$ is smooth over k, whence so is their union S'. As S' is also connected, we find that S' is irreducible from Lemma 2.5.7.

To prove that g' is relatively minimal, it suffices by Theorem 2.3.7 to show that no fiber S'_x above $x \in C'$ contains an exceptional prime divisor. Let D' be an irreducible component of the fiber S'_x, mapping isomorphically to the irreducible component D of $S_{\gamma(x)} \cong S'_x$ under the induced morphism $\gamma' \colon S' \to S$. Suppose that D' is an exceptional divisor, i.e., $D' \cong \mathbb{P}^1$ and $D'^2 = -1$. If $\gamma(x)$ is contained in V, then the fiber $S_{\gamma(x)}$, and hence S'_x, is smooth. As all fibers are connected, S'_x is then irreducible, so $D' = S'_x$. Since any fiber is numerically equivalent to any other, this implies $D'^2 = 0$, contradiction. Therefore, we may assume that $\gamma(x) \notin V$, so $\gamma(x) \in U$ and $D' \subset h^{-1}(U)$. As étale morphisms are stable under base extension and $\gamma|_{\gamma^{-1}(U)}$ is étale, we find that $\gamma'|_{h^{-1}(U)}$ is étale.

For any morphism of schemes $\varphi \colon X \to Y$, let $\Omega_{X/Y}$ denote the sheaf of relative differentials of X over Y. If X is a nonsingular variety over k, then let $\mathcal{T}_X$ denote the tangent sheaf $\mathcal{H}om(\Omega_{X/k}, \mathcal{O}_X)$. For any nonsingular subvariety $Z \subset X$, let $\mathcal{N}_{Z/X}$ denote the normal sheaf of Z in X, see [Ha2], § II.8.

We will show that the self-intersection number $D'^2 = \deg \mathcal{N}_{D'/S'}$ on S' (see [Ha2], example V.1.4.1) is equal to the self-intersection number $D^2 = \deg \mathcal{N}_{D/S}$. Since D is not an exceptional curve, that implies that $D'^2 \neq -1$, which is a contradiction. As γ' induces an isomorphism from D' to D, it suffices to show that $\mathcal{N}_{D'/S'}$ is isomorphic to $\gamma'^*\mathcal{N}_{D/S}$.

There is an exact sequence

$$0 \to \mathcal{T}_{D'} \to \mathcal{T}_{S'} \otimes \mathcal{O}_{D'} \to \mathcal{N}_{D'/S'} \to 0 \tag{2.9}$$

(see [Ha2], p. 182), and by applying the isomorphism $(\gamma'|_{D'})^*$ to the similar sequence for D in S we also get the exact sequence

$$0 \to \gamma'^*\mathcal{T}_D \to \gamma'^*(\mathcal{T}_S \otimes \mathcal{O}_D) \to \gamma'^*\mathcal{N}_{D/S} \to 0. \tag{2.10}$$

The natural morphisms $\mathcal{T}_{D'} \to \gamma'^*\mathcal{T}_D$ and $\mathcal{T}_{S'} \otimes \mathcal{O}_{D'} \to \gamma'^*(\mathcal{T}_S \otimes \mathcal{O}_D)$ induce a morphism between the short exact sequences (2.9) and (2.10). To prove that the last morphism $\mathcal{N}_{D'/S'} \to \gamma'^*\mathcal{N}_{D/S}$ is an isomorphism, it suffices by the snake lemma to prove that the first two are. Clearly, $\mathcal{T}_{D'} \to \gamma'^*\mathcal{T}_D$ is an isomorphism of sheaves on D', as $\gamma'|_{D'}$ is an isomorphism. To show that

$$\mathcal{T}_{S'} \otimes \mathcal{O}_{D'} \to \gamma'^*(\mathcal{T}_S \otimes \mathcal{O}_D) \cong \gamma'^*\mathcal{T}_S \otimes \gamma'^*\mathcal{O}_D \cong \gamma'^*\mathcal{T}_S \otimes \mathcal{O}_{D'}$$

is an isomorphism, it suffices to show that $\mathcal{T}_{S'} \to \gamma'^*\mathcal{T}_S$ is an isomorphism on the open subset $h^{-1}(U) \subset S'$ containing D'. This is true, as by [SGA 1], Exposé II, Cor. 4.6, a morphism $f \colon X \to Y$ of smooth T-schemes is étale if and only if the morphism $f^*\Omega_{Y/T} \to \Omega_{X/T}$ is an isomorphism. Taking the dual gives what we need, if we choose $T = \operatorname{Spec} k$, and $f = \gamma'|_{h^{-1}(U)}$.

For the last statement we will use that by [Ko1], Thm. 12.2, we have

$$\begin{aligned} 12\chi_S = \mu + 6\sum_{b \geq 0} \nu(I_b^*) + 2\nu(II) + 10\nu(II^*) + 3\nu(III) \\ + 9\nu(III^*) + 4\nu(IV) + 8\nu(IV^*), \end{aligned} \tag{2.11}$$

where $\nu(T)$ is the number of singular fibers of g of type T and μ is the degree of the map $j(S/C)\colon C \to \mathbb{P}^1$, sending every element $x \in C$ to the j-invariant of the fiber S_x.

As the morphism γ is unramified above the points of C where g has singular fibers, it follows that the singular fibers of g' come in n-tuples, with $n = \deg \gamma$. Each n-tuple consists of n copies of one of the singular fibers of g. Hence, if $\nu'(T)$ denotes the number of singular fibers of g' of type T, then we have $\nu'(T) = n\nu(T)$. As $j(S'/C')$ is the composition of γ and $j(S/C)$, we also get $\mu' = n\mu$, where μ' is the degree of $j(S'/C')$. From (2.11) and its analogue for S' we conclude that $\chi_{S'} = n\chi_S$. $\square$

2.6 The Néron-Severi group under good reduction

In this section we will see how the Néron-Severi group of a surface behaves under good reduction. Proposition 2.6.2 is known among specialists, but by lack of reference, we will include a proof, as sketched by Bas Edixhoven. D. Harari proves a similar result about Brauer groups, see [Hr2]. Arguments similar to the ones used in this section can also be found in [Hr1] and [CR]. For all of this section, let A be a discrete valuation ring of a number field K with maximal ideal $\mathfrak{m}$, whose residue field k has $q = p^r$ elements with p prime. Let S be an integral scheme with a morphism $S \to \operatorname{Spec} A$ that is projective and smooth of relative dimension 2. Then the projective surfaces $\overline{S} = S_{\overline{\mathbb{Q}}}$ and $\widetilde{S} = S_{\overline{k}}$ are smooth over the algebraically closed fields $\overline{\mathbb{Q}}$ and $\overline{k}$ respectively. We will assume that $\overline{S}$ and $\widetilde{S}$ are integral, i.e., they are irreducible, nonsingular, projective surfaces.

Let $l \neq p$ be a prime number. For any scheme Z we set

$$H^i(Z_{\text{ét}}, \mathbb{Q}_l) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} \left(\varprojlim H^i(Z_{\text{ét}}, \mathbb{Z}/l^n\mathbb{Z}) \right).$$

Furthermore, for every integer m and every vector space H over $\mathbb{Q}_l$ with the Galois group $G(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ acting on it, we define the twistings of H to be the $G(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-spaces $H(m) = H \otimes_{\mathbb{Q}_l} W^{\otimes m}$, where

$$W = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} (\varprojlim \mu_{l^n})$$

is the one-dimensional l-adic vector space on which $G(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ operates according to its action on the group $\mu_{l^n} \subset \overline{\mathbb{F}_q}$ of l^n-th roots of unity. Here we use $W^{\otimes 0} = \mathbb{Q}_l$ and $W^{\otimes m} = \operatorname{Hom}(W^{\otimes -m}, \mathbb{Q}_l)$ for $m < 0$.

For the rest of this section, all cohomology will be étale cohomology, so we will often leave out the subscript ét.

Lemma 2.6.1 *Let L denote the maximal subextension of $\overline{\mathbb{Q}}/K$ that is unramified at $\mathfrak{m}$. Let B denote the localization at some maximal ideal of the integral closure of A in L. Then for all integers i, m the natural homomorphisms*

$$H^i(S_B, \mathbb{Q}_l)(m) \to H^i(\widetilde{S}, \mathbb{Q}_l)(m) \qquad \text{and}$$
$$H^i(S_B, \mathbb{Q}_l)(m) \to H^i(\overline{S}, \mathbb{Q}_l)(m)$$

are isomorphisms.

Proof. As tensoring with W is exact, it suffices to prove this for $m = 0$. The ring B is a strictly Henselian ring, see [Mi2], p. 38 (for the definition, see [EGA IV(4)], Déf. 18.8.2, or [Mi2], § I.4). The surface $\widetilde{S}$ is the closed fiber of $S_B \to \operatorname{Spec} B$. As B is strictly Henselian, it follows from the proper base change theorem that the maps $H^i(S_B, \mathbb{Z}/l^n\mathbb{Z}) \to H^i(\widetilde{S}, \mathbb{Z}/l^n\mathbb{Z})$ are isomorphisms for all $n \geq 0$, see [Mi2], Cor. VI.2.7, and [SGA $4\frac{1}{2}$], p. 39, Thm. IV.1.2. Hence, also the map $H^i(S_B, \mathbb{Q}_l) \to H^i(\widetilde{S}, \mathbb{Q}_l)$ obtained from taking the projective limit and tensoring with $\mathbb{Q}_l$ is an isomorphism. The surface $\overline{S}$ is the base change of S_B from $\operatorname{Spec} B$ to its geometric point $\operatorname{Spec} \overline{\mathbb{Q}}$. From the smooth base change theorem ([Mi2], Thm. VI.4.1, and [SGA $4\frac{1}{2}$], p. 63, Thm. V.3.2) it follows that $H^i(S_B, \mathbb{Z}/l^n\mathbb{Z}) \to H^i(\overline{S}, \mathbb{Z}/l^n\mathbb{Z})$ is an isomorphism. For this exact statement, see [SGA $4\frac{1}{2}$], p. 54–56: Lemme V.1.5, (1.6), and Variante (for their S take $S = \operatorname{Spec} B$; as B is a strictly Henselian local ring which is integrally closed in its fraction field L already, we get that their S' equals their S). These statements assume that the morphism $S_B \to \operatorname{Spec} B$ is locally acyclic, which follows from the fact that it is smooth, see [SGA $4\frac{1}{2}$], p. 58, Thm. (2.1). Passing to the limit and tensoring with $\mathbb{Q}_l$, we find that also the map $H^i(S_B, \mathbb{Q}_l) \to H^i(\overline{S}, \mathbb{Q}_l)$ is an isomorphism. □

Proposition 2.6.2 *There are natural injective homomorphisms*

$$\operatorname{NS}(\overline{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow \operatorname{NS}(\widetilde{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow H^2(\widetilde{S}, \mathbb{Q}_l)(1) \tag{2.12}$$

of finite dimensional vector spaces over $\mathbb{Q}_l$. The second injection respects the Galois action of $G(\overline{k}/k)$.

Proof. After replacing K and A by a finite extension if necessary, we may assume without loss of generality that the natural map $\operatorname{NS}(S_K) \to \operatorname{NS}(\overline{S})$ is surjective (take generators for $\operatorname{NS}(\overline{S})$, lift them to $\operatorname{Div} \overline{S}$ and let K be a field over which all these lifts are defined). For any scheme Z, we have $H^1(Z_{\text{ét}}, \mathbb{G}_m) \cong \operatorname{Pic} Z$, see [SGA $4\frac{1}{2}$], p. 20, Prop. 2.3, or [Mi2], Prop. III.4.9. As long as $l \neq \operatorname{char} k(z)$ for any $z \in Z$, the Kummer sequence

$$0 \to \mu_{l^n} \to \mathbb{G}_m \xrightarrow{[l^n]} \mathbb{G}_m \to 0$$

is a short exact sequence of sheaves on $Z_{\text{ét}}$, see [SGA $4\frac{1}{2}$], p. 21, (2.5), or [Mi2], p. 66. Hence, from the long exact sequence we get a δ-map

$$\operatorname{Pic} Z \cong H^1(Z_{\text{ét}}, \mathbb{G}_m) \xrightarrow{\delta} H^2(Z_{\text{ét}}, \mu_{l^n}).$$

Taking the projective limit over n, we get a homomorphism

$$\operatorname{Pic} Z \to \varprojlim H^2(Z, \mu_{l^n}) \cong \varprojlim H^2(Z, \mathbb{Z}/l^n\mathbb{Z}) \otimes \mu_{l^n} \to H^2(Z, \mathbb{Q}_l)(1).$$

Let L and B be as in Lemma 2.6.1. Note that B is a discrete valuation ring. Because S_B is smooth and projective over $\operatorname{Spec} B$, with geometrically integral fibers, it follows that the map $\operatorname{Pic} S_B \to \operatorname{Pic} S_L$ is an isomorphism, see [Hr1], Lem. 3.1.1. From the above we get the diagram below, which commutes by functoriality. The maps $H^2(S_B, \mathbb{Q}_l)(1) \to H^2(\widetilde{S}, \mathbb{Q}_l)(1)$ and $H^2(S_B, \mathbb{Q}_l)(1) \to H^2(\overline{S}, \mathbb{Q}_l)(1)$ in the bottom line of the diagram are isomorphisms by Lemma 2.6.1.

$$\begin{tikzcd}
\operatorname{Pic} \overline{S} \arrow[d] & \operatorname{Pic} S_L \arrow[l] \arrow[d] & \operatorname{Pic} S_B \arrow[l, "\cong"'] \arrow[r] \arrow[d] & \operatorname{Pic} \widetilde{S} \arrow[d] \\
H^2(\overline{S}, \mathbb{Q}_l)(1) & H^2(S_L, \mathbb{Q}_l)(1) \arrow[l] & H^2(S_B, \mathbb{Q}_l)(1) \arrow[l] \arrow[r, "\cong"] \arrow[ll, bend left, "\cong"] & H^2(\widetilde{S}, \mathbb{Q}_l)(1)
\end{tikzcd}$$

Recall that for any smooth, projective variety Z over an algebraically closed field, the group $\operatorname{Pic}^{\mathrm{n}} Z$ is the subgroup of $\operatorname{Pic} Z$ of all divisor classes on Z that are numerically equivalent to 0, see Definition 2.2.16. By Proposition 2.2.17 we have an isomorphism $\operatorname{NS}(Z)/\operatorname{NS}(Z)_{\mathrm{tors}} \cong \operatorname{Pic} Z/\operatorname{Pic}^{\mathrm{n}} Z$. By [Ta2], p. 97–98, the kernel of $\operatorname{Pic} Z \to H^2(Z, \mathbb{Q}_l)(1)$ is $\operatorname{Pic}^{\mathrm{n}} Z$. From the diagram above, it then follows that the composition

$$\gamma\colon \operatorname{Pic} S_L \cong \operatorname{Pic} S_B \to \operatorname{Pic} \widetilde{S} \to H^2(\widetilde{S}, \mathbb{Q}_l)(1)$$

factors as

$$\begin{aligned}
\gamma\colon \operatorname{Pic} S_L \to \operatorname{NS}(\widetilde{S})/\operatorname{NS}(\widetilde{S})_{\mathrm{tors}} \hookrightarrow H^2(\widetilde{S}, \mathbb{Q}_l)(1) \qquad \text{and as} \\
\gamma\colon \operatorname{Pic} S_L \to \operatorname{Pic} \overline{S} \to H^2(\overline{S}, \mathbb{Q}_l)(1) \cong H^2(S_B, \mathbb{Q}_l)(1) \cong H^2(\widetilde{S}, \mathbb{Q}_l)(1).
\end{aligned} \tag{2.13}$$

Set $M = \operatorname{Pic} S_L/\ker \gamma$. From the first factorization of γ in (2.13) we find that there are injections

$$M \hookrightarrow \operatorname{NS}(\widetilde{S})/\operatorname{NS}(\widetilde{S})_{\mathrm{tors}} \hookrightarrow H^2(\widetilde{S}, \mathbb{Q}_l)(1). \tag{2.14}$$

The second map in the second line of (2.13) has kernel $\operatorname{Pic}^{\mathrm{n}} \overline{S}$, so γ also factors as

$$\gamma\colon \operatorname{Pic} S_L \to \operatorname{NS}(\overline{S})/\operatorname{NS}(\overline{S})_{\mathrm{tors}} \hookrightarrow H^2(\widetilde{S}, \mathbb{Q}_l)(1). \tag{2.15}$$

As the map $\operatorname{NS}(S_L) \to \operatorname{NS}(\overline{S})$ is surjective, so is the first map of (2.15). We conclude that M is isomorphic to $\operatorname{NS}(\overline{S})/\operatorname{NS}(\overline{S})_{\mathrm{tors}}$. Combining this with (2.14) and tensoring with $\mathbb{Q}_l$, we find the desired homomorphisms. $\square$

Remark 2.6.3 Proposition 2.6.2 implies $\operatorname{rk}\operatorname{NS}(\overline{S}) \leq \operatorname{rk}\operatorname{NS}(\widetilde{S})$. For a shorter proof of this fact, note that without loss of generality, by enlarging A, we may assume that $\operatorname{NS}(\overline{S})$ and $\operatorname{NS}(\widetilde{S})$ are defined over the quotient field $K = Q(A)$ and the residue field k of A respectively. Let $\hat{K}$ denote the quotient field of the completion $\hat{A}$ of A, and let K' be the algebraic closure of $\hat{K}$. Then by [Fu], Exm. 20.3.6, the intersection numbers do not change under reduction, so we get $\operatorname{rk}\operatorname{NS}(S_{K'}) \leq \operatorname{rk}\operatorname{NS}(\widetilde{S})$. Thus, we find

$$\operatorname{rk}\operatorname{NS}(\overline{S}) = \operatorname{rk}\operatorname{NS}(S_K) \leq \operatorname{rk}\operatorname{NS}(S_{K'}) \leq \operatorname{rk}\operatorname{NS}(\widetilde{S}).$$

However, this does not imply that there exists a well-defined homomorphism $\operatorname{NS}(\overline{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow \operatorname{NS}(\widetilde{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l$, so Proposition 2.6.2 gives more information.

For any variety X over k, let $F_X\colon X \to X$ denote the *absolute Frobenius of* X, which acts as the identity on points, and by $f \mapsto f^p$ on the structure sheaf. Set $\varphi = F_{S_k}^r$ and let φ^* denote the automorphism on $H^2(\widetilde{S}, \mathbb{Q}_l)$ induced by $\varphi \times 1$ acting on $S_k \times_k \overline{k} \cong \widetilde{S}$.

Corollary 2.6.4 *The ranks of* $\mathrm{NS}(\widetilde{S})$ *and* $\mathrm{NS}(\overline{S})$ *are bounded from above by the number of eigenvalues λ of φ^* for which λ/q is a root of unity, counted with multiplicity.*

Proof. By Proposition 2.6.2, any upper bound for the rank of $\mathrm{NS}(\widetilde{S})$ is an upper bound for the rank of $\mathrm{NS}(\overline{S})$. For any k-variety X, the absolute Frobenius F_X acts as the identity on the site $X_{\text{ét}}$. Hence, if we set $\overline{X} = X \times_k \overline{k}$, then $F_{\overline{X}} = F_X \times F_{\overline{k}}$ acts as the identity on $H^i(\overline{X}, \mathbb{Q}_l)(m)$ for any m, see [Ta2], § 3. Therefore, $F_X = F_X \times 1$ and $F_{\overline{k}} = 1 \times F_{\overline{k}}$ act as each other's inverses.

Let $\sigma\colon x \mapsto x^q$ denote the canonical topological generator of $G(\overline{k}/k)$. Then $\sigma = F_{\overline{k}}^r$ and as we have $\widetilde{S} \cong S_k \times_k \overline{k}$, we find $\varphi \times \sigma = F_{S_k}^r \times F_{\overline{k}}^r = F_{\widetilde{S}}^r$. By the above we find that the induced automorphisms $\varphi^{*(m)}$ and $\sigma^{*(m)}$ on $H^2(\widetilde{S}, \mathbb{Q}_l)(m)$ act as each other's inverses for any m.

As every divisor on $\widetilde{S}$ is defined over a finite field extension of k, some power of $\sigma^{*(1)}$ acts as the identity on $\mathrm{NS}(\widetilde{S}) \subset H^2(\widetilde{S}, \mathbb{Q}_l)(1)$. It follows from Proposition 2.6.2 that an upper bound for $\mathrm{rk}\,\mathrm{NS}(\widetilde{S})$ is given by the number of eigenvalues (with multiplicity) of $\sigma^{*(1)}$ that are roots of unity. As σ^* acts as multiplication by q on W, this equals the number of eigenvalues ν of $\sigma^{*(0)}$ for which νq is a root of unity. The corollary follows as $\varphi^* = \varphi^{*(0)}$ acts as the inverse of $\sigma^{*(0)}$. $\square$

Remark 2.6.5 Tate's conjecture states that the upper bound mentioned is actually equal to the rank of $\mathrm{NS}(\widetilde{S})$, see [Ta2]. Tate's conjecture has been proven for ordinary K3 surfaces over fields of characteristic ≥ 5, see [NO], Thm. 0.2.

Chapter 3

A K3 surface associated to integral matrices with integral eigenvalues

3.1 Introduction

In the problem section of Nieuw Archief voor Wiskunde [NAW], F. Beukers posed the question whether symmetric, integral 3×3 matrices

$$M_{a,b,c} = \begin{pmatrix} 0 & a & b \\ a & 0 & c \\ b & c & 0 \end{pmatrix} \tag{3.1}$$

exist with integral eigenvalues and satisfying $q(a, b, c) \neq 0$, where $q(a, b, c)$ is the polynomial $q(a, b, c) = abc(a^2 - b^2)(b^2 - c^2)(c^2 - a^2)$. As it is easy to find such matrices satisfying $q(a, b, c) = 0$, we will call those trivial. R. Vidunas and the author of this thesis independently proved that the answer to this question is positive, see [BLV]. There are in fact infinitely many nontrivial examples of such matrices. This follows immediately from the fact that for every integer t, if we set

$$\begin{aligned} a &= -(4t - 7)(t + 2)(t^2 - 6t + 4), \\ b &= (5t - 6)(5t^2 - 10t - 4), \\ c &= (3t^2 - 4t + 4)(t^2 - 4t + 6), \\ x &= 2(3t^2 - 4t + 4)(4t - 7), \\ y &= (t^2 - 6t + 4)(5t^2 - 10t - 4), \\ z &= -(t + 2)(5t - 6)(t^2 - 4t + 6), \end{aligned} \tag{3.2}$$

then the matrix $M_{a,b,c}$ has eigenvalues x, y, and z. This matrix is trivial if and only if we have $t \in \{-2, -1, 0, 1, 2, 4, 10\}$. For $t = 3$ we get $a = 125$, $b = 99$, and $c = 57$ with eigenvalues 190, -55, and -135. By a computer search, we find that this is the second smallest example, when ordered by $\max(|a|, |b|, |c|)$. The smallest has $a = 26$, $b = 51$, and $c = 114$. In this chapter we will show how to find such parametrizations. We will see that there are infinitely many and that the one in (3.2) has the lowest possible degree.

If the eigenvalues of the matrix $M_{a,b,c}$ are denoted by x, y, and z, then its characteristic polynomial can be factorized as

$$\lambda^3 - (a^2 + b^2 + c^2)\lambda - 2abc = (\lambda - x)(\lambda - y)(\lambda - z).$$

Comparing coefficients, we get three homogeneous equations in x, y, z, a, b, and c. Hence, geometrically we are looking for rational points on the 2-dimensional complete intersection $X \subset \mathbb{P}^5_{\mathbb{Q}}$, given by

$$\begin{aligned} x + y + z &= 0, \\ xy + yz + zx &= -a^2 - b^2 - c^2, \\ xyz &= 2abc. \end{aligned} \tag{3.3}$$

The points on the curves on X defined by $q(a, b, c) = 0$ correspond to the trivial matrices. Parametrizations as in (3.2) correspond to curves on X that are isomorphic over $\mathbb{Q}$ to $\mathbb{P}^1$. We will see that X contains infinitely many of them, thereby proving the main theorem of this chapter, which states the following.

Theorem 3.1.1 *The rational points on X are Zariski dense.*

In Section 3.2 we will prove Theorem 3.1.1 using an elliptic fibration of a blow-up Y of X. We will see that Y is a so called elliptic K3 surface. The interaction between the geometry and the arithmetic of K3 surfaces is of much interest. F. Bogomolov and Y. Tschinkel have proved that on every elliptic K3 surface Z over a number field K the rational points are potentially dense, i.e., there is a finite field extension L/K, such that the L-points of Z are dense in Z, see [BT], Thm. 1.1. Key in their analysis of potential density of rational points is the so called Picard number of a surface, an important geometric invariant. F. Bogomolov and Y. Tschinkel have shown that if the Picard number of a K3 surface is large enough, then the rational points are potentially dense. On the other hand, it is not yet known if there exist K3 surfaces with Picard number 1 on which the rational points are not potentially dense.

After proving the main theorem, we will investigate more deeply the geometry of Y and show in Section 3.3 that its Picard number equals 20, which is maximal among K3 surfaces in characteristic 0. It is a fact that a K3 surface with maximal Picard number is either a Kummer surface or a double cover of a Kummer surface. These Kummer surfaces are K3 surfaces with a special geometric structure, described in Section 3.4. As a consequence, their arithmetic can be described more easily. It is therefore natural to ask if Y is a Kummer surface, in which case Y would have had a richer structure that we could have utilized. In Section 3.4 we will show that this is not the case.

In Section 3.5 we will describe more of the geometry of X by showing that X contains exactly 63 curves of degree smaller than 4. All points on these curves correspond to matrices that are either trivial or not defined over $\mathbb{Q}$. As the degree of a parametrization as in (3.2) corresponds to the degree of the curve that it parametrizes, this shows that the one in (3.2) has the lowest possible degree among parametrizations of nontrivial matrices.

The results of this chapter have been combined into a preprint, see [VL1].

3.2 Proof of the main theorem

Let $G \subset \mathrm{Aut}\ X$ be the group of automorphisms of X generated by permutations of x, y and z, by permutations of a, b, and c and by switching the sign of two of the coordinates a, b, and c. Then G is isomorphic to $(V_4 \rtimes S_3) \times S_3$ and has order 144. The surface X has 12 singular points, on which G acts transitively. They are all ordinary double points and their orbit under G is represented by $[x : y : z : a : b : c] = [2 : -1 : -1 : 1 : 1 : 1]$. Let $\pi\colon Y \to X$ be the blow-up of X in these 12 points.

Proposition 3.2.1 *The surface Y is a smooth K3 surface. The exceptional curves above the 12 singular points of X are all isomorphic to $\mathbb{P}^1$ and have self-intersection number -2.*

Proof. Ordinary double points are resolved after one blow-up, so Y is smooth. The exceptional curves E_i are isomorphic to $\mathbb{P}^1$, see [Ha2], exc. I.5.7. Their self-intersection number follows from [Ha2], example V.2.11.4. Since X is a complete intersection, it is geometrically connected and $H^1(X, \mathcal{O}_X) = 0$, so $q(X) = 0$, see [Ha2], exc. II.5.5. From its connectedness it follows that Y is geometrically connected as well. As Y is also smooth, it follows that Y is geometrically irreducible.

To compute the canonical sheaf on Y, note that on the nonsingular part $U = X^{\mathrm{reg}}$ of X the canonical sheaf is given by $\mathcal{O}_X(-5-1+3+2+1)|_U = \mathcal{O}_U$, see [Ha2], Prop. II.8.20 and exc. II.8.4. Hence, the canonical sheaf on Y restricts to the structure sheaf outside the exceptional curves. That implies that there are integers a_i such that $K = \sum_i a_i E_i$ is a canonical divisor. Recall that $E_i^2 = -2$ and $E_i \cdot E_j = 0$ for $i \neq j$. Applying the adjunction formula $2g_C - 2 = C \cdot (C + K)$ (see [Ha2], Prop. V.1.5) to $C = E_i$, we find that $a_i = 0$ for all i, whence $K = 0$.

It remains to show that $q(Y) = q(X)$. It follows immediately from [Ar], Prop. 1, that ordinary double points are rational singularities, i.e., we have $R^1\pi_*\mathcal{O}_Y = 0$. Also, as X is integral, the sheaf $\pi_*\mathcal{O}_Y$ is a sub-$\mathcal{O}_X$-algebra of the constant $\mathcal{O}_X$-algebra $K(X)$, where $K(X) = K(Y)$ is the function field of both X and Y. Since π is proper, $\pi_*\mathcal{O}_Y$ is finitely generated as $\mathcal{O}_X$-module. As X is normal, i.e., $\mathcal{O}_X$ is integrally closed, we get $\pi_*\mathcal{O}_Y \cong \mathcal{O}_X$. Hence, the desired equality $q(Y) = q(X)$ follows from the following lemma, applied to $f = \pi$ and $\mathcal{F} = \mathcal{O}_Y$. □

Lemma 3.2.2 *Let $f\colon W \to Z$ be a continuous map of topological spaces. Let $\mathcal{F}$ be a sheaf of groups on W and assume that $R^i f_*(\mathcal{F}) = 0$ for all $i = 1, \ldots, t$. Then for all*

$i = 0, 1, \ldots, t$, *there are isomorphisms*

$$H^i(W, \mathcal{F}) \cong H^i(Z, f_*\mathcal{F}).$$

Proof. This follows from the Leray spectral sequence. For a more elementary proof, choose an injective resolution

$$0 \to \mathcal{F} \to I_0 \to I_1 \to I_2 \to \cdots$$

of $\mathcal{F}$. Because $R^i f_*(\mathcal{F}) = 0$ for $i = 1, \ldots, t$, we conclude that the sequence

$$0 \to f_*\mathcal{F} \to f_*I_0 \to f_*I_1 \to f_*I_2 \to \cdots \to f_*I_{t+1} \tag{3.4}$$

is exact as well. As injective sheaves are flasque (see [Ha2], Lemma III.2.4) and f_* maps flasque W-sheaves to flasque Z-sheaves, the exact sequence (3.4) can be extended to a flasque resolution of $f_*\mathcal{F}$. By [Ha2], Rem. III.2.5.1, we can use that flasque resolution to compute the cohomology groups $H^i(Z, f_*\mathcal{F})$. Taking global sections we get the complex

$$0 \to \Gamma(Z, f_*I_0) \to \Gamma(Z, f_*I_1) \to \Gamma(Z, f_*I_2) \to \cdots \to \Gamma(Z, f_*I_{t+1}) \to \ldots \tag{3.5}$$

As $\Gamma(Z, f_*I_n) \cong \Gamma(W, I_n)$ for all n, we find that for $i = 0, 1, \ldots, t$, the i-th cohomology of (3.5) is isomorphic to both $H^i(Z, f_*\mathcal{F})$ and $H^i(W, \mathcal{F})$. $\square$

We will now give $\overline{Y}$ the structure of an elliptic surface over $\mathbb{P}^1$. Let $f\colon Y \to \mathbb{P}^1$ be the composition of π with the morphism $f'\colon X \to \mathbb{P}^1, [x : y : z : a : b : c] \mapsto [x : a] = [2bc : yz]$. One easily checks that f', and hence f, is well-defined everywhere.

If $a = 0$, then clearly $M_{a,b,c}$ in (3.1) has eigenvalue 0. Geometrically, this reflects the fact that the hyperplane $a = 0$ intersects X in three conics, one in each of the hyperplanes given by $xyz = 0$. Hence, each of the hyperplanes H_t given by $x = ta$ in the family of hyperplanes through the space $x = a = 0$ contains the conic given by $a = x = 0$ on X. The fibers of f consist of the inverse image under π of the other components in the intersection of X with the family of hyperplanes H_t. The fiber above $[t : 1]$ is therefore given by the intersection of the two quadrics

$$xy + yz + zx = -a^2 - b^2 - c^2 \qquad \text{and} \qquad tyz = 2bc \tag{3.6}$$

within the intersection of two hyperplanes

$$x + y + z = x - ta = 0, \tag{3.7}$$

which is isomorphic to $\mathbb{P}^3$. The conic C given by $a + b = c - y = 0$ on X maps under f' isomorphically to $\mathbb{P}^1$. The strict transform of C on Y gives a section of f that we will denote by $\mathcal{O}$.

Proposition 3.2.3 *The morphism f and its section $\mathcal{O}$ give $Y_{\mathbb{C}}$ the structure of an elliptic surface over $\mathbb{P}^1_{\mathbb{C}}$.*

Proof. Since Y is a K3 surface, it is minimal. Indeed, by the adjunction formula any smooth curve C of genus 0 on Y would have self-intersection $C^2 = -2$, while an exceptional curve that can be blown down has self-intersection -1, see [Ha2], Prop. V.3.1. Hence, f is a relatively minimal fibration by Theorem 2.3.7. The 12 exceptional curves give extra components in the fibers above $t = \pm 1, \pm 2$, so f is not smooth. From the description (3.6) above, an easy computation shows that the fibers above $t \neq 0, \pm 1, \pm 2, \infty$ are nonsingular. They are isomorphic to the complete intersection of two quadrics in $\mathbb{P}^3$, so by [Ha2], exc. II.8.4g, almost all fibers have genus 1. $\square$

Let $K \cong \mathbb{Q}(t)$ denote the function field of $\mathbb{P}^1_{\mathbb{Q}}$ and let E/K be the generic fiber of f. It can be given by the same equations (3.6) and (3.7). To put E in Weierstrass form, set $\lambda = (t^2-4)\nu + 3t$ and $\mu = t(t^2-4)(z-y)(t\nu^2 - 2\nu + t)/x$, where $\nu = (x-c)/(a+b)$. Then the change of variables

$$u = \big(\mu + (\lambda^2 + t(t^2-1)(t+8))\big)/2,$$
$$v = \big(\mu\lambda + \lambda^3 + (t^2-1)(t^2-8)\lambda - 8t(t^2-1)^2\big)/2$$

shows that E/K is isomorphic to the elliptic curve over K given by

$$v^2 = u\big(u - 8t(t^2-1)\big)\big(u - (t^2-1)(t+2)^2\big).$$

It has discriminant $\Delta = 2^{10}t^2(t^2-1)^6(t^2-4)^4$ and j-invariant

$$j = \frac{4(t^4 + 56t^2 + 16)^3}{t^2(t^2-4)^4}.$$

Lemma 3.2.4 *The singular fibers of f are at $t = 0, \pm 1, \pm 2$ and at $t = \infty$. They are described in the following table, where m_t (resp. $m_t^{(1)}$) is the number of irreducible components (resp. irreducible components of multiplicity 1).*

t	*type*	m_t	$m_t^{(1)}$
$0, \infty$	I_2	2	2
± 1	$I_0^*(4 \cdot 73^3 \cdot 3^{-4})$	5	4
± 2	I_4	4	4

Proof. This is a straightforward computation. Since we have a Weierstrass form, it also follows easily from Tate's algorithm, see [Ta3] and [Si2], IV.9. For the parameter $j = 4 \cdot 73^3 \cdot 3^{-4}$ see Remark 2.4.18. $\square$

Applying the automorphisms $(b,c) \mapsto (-c,-b)$ and $(b,c) \mapsto (-b,-c)$ and $(b,c,y,z) \mapsto (c,b,z,y)$ to the curve $\mathcal{O}$, we get three more sections, which we will denote by P, T_1 and

T_2 respectively. By Lemma 2.3.13, these sections correspond with points on the generic fiber E/K. The Weierstrass coordinates (u, v) of these points are given by

$$\begin{aligned} T_1 &= \big((t^2-1)(t+2)^2,\, 0\big), \\ T_2 &= \big(0,\, 0\big), \\ P &= \big(2t^3(t+1),\, 2t^2(t+1)^2(t-2)^2\big), \end{aligned} \tag{3.8}$$

We immediately notice that the T_i are 2-torsion points.

Proposition 3.2.5 *The section P has infinite order in the group $S(C) \cong E(K)$.*

Proof. Note that $S(C)$ and $E(K)$ are isomorphic by the identification of Lemma 2.3.13. By Corollary 2.4.35 there is a bilinear pairing on $E(K)$ that induces a nondegenerate pairing on $E(K)/E(K)_{\mathrm{tors}}$. As mentioned in Remark 2.4.36, Shioda gives an explicit formula for this pairing, see [Shi3], Thm. 8.6. We find that $\langle P, P\rangle = \frac{3}{2} \neq 0$, so P is not torsion. $\square$

The main theorem now follows immediately.

Proof of Theorem 3.1.1. By Proposition 3.2.5 the multiples of P give infinitely many rational curves on Y, so the rational points on Y are dense. As π is dominant, the rational points on X are dense as well. $\square$

The multiples of P yield infinitely many parametrizations of integral, symmetric 3×3 matrices with zeros on the diagonal and integral eigenvalues. The section $2P$, for example, is a curve of degree 8 on X which can be parametrized by

$$\begin{aligned} a &= t(t^6 - 8t^4 + 20t^2 - 12), \\ b &= -t(t^6 - 4t^4 + 4), \\ c &= (t^2-2)(t^6 - 6t^4 + 8t^2 - 4), \end{aligned}$$

and suitable polynomials for x, y, and z. The parametrization (3.2) does not come from a section of f. We will see in Section 3.5 where it does come from.

3.3 The Mordell-Weil group and the Néron-Severi group

As mentioned in the introduction, the geometry and the arithmetic of K3 surfaces are closely related. In the following sections we will further analyze the geometry of Y. Set $L = \mathbb{C}(t) \supset \mathbb{Q}(t) = K$. In this section we will find explicit generators for the Mordell-Weil group $E(L)$ and for the Néron-Severi group of $\overline{Y} = Y_{\mathbb{C}}$. This will be used in Sections 3.4 and 3.5.

Two of the irreducible components of the singular fibers of $f\colon Y \to \mathbb{P}^1$ above $t = \pm 2$ are defined over $\mathbb{Q}(\sqrt{3})$. They are all in the same orbit under G. In that same orbit we also find a section, given by $z = 2b$ and $2(c-a) = \sqrt{3}(y-x)$. We will denote it by Q. Its Weierstrass coordinates are given by

$$Q = \big(2t(t+1)(t+2),\, 2\sqrt{3}t(t^2-4)(t+1)^2\big).$$

It follows immediately that the Galois conjugate of Q under the automorphism that sends $\sqrt{3}$ to $-\sqrt{3}$ is equal to $-Q$.

Recall that a complex K3 surface is called singular if its Picard number equals 20, see Remark 2.2.24.

Proposition 3.3.1 *The surface $\overline{Y}$ is a singular K3 surface. The Mordell-Weil group $E(L)$ is isomorphic to $\mathbb{Z}^2 \times (\mathbb{Z}/2\mathbb{Z})^2$ and generated by P, Q, T_1 and T_2. The Mordell-Weil group $E(K)$ is isomorphic to $\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$ and generated by P, T_1 and T_2.*

Proof. From Shioda's explicit formula for the pairing on $E(K)$ (see Remark 2.4.36), we find that $\langle P,P\rangle = \frac{3}{2}$ and $\langle Q,Q\rangle = \frac{1}{2}$ and $\langle P,Q\rangle = 0$. Hence, P and Q are linearly independent and the Mordell-Weil rank $r = \operatorname{rk} E(L)$ is at least 2.

By Lemma 3.2.4 and Theorem 2.4.32, the rank ρ of $\mathrm{NS}(\overline{Y}) = \mathrm{Pic}(\overline{Y})$ is at least $2+18 = 20$. As $\overline{Y}$ is a K3 surface (see Proposition 3.2.1) and 20 is the maximal Picard number for K3 surfaces in characteristic 0, we conclude that $\overline{Y}$ is a singular K3 surface. Using Theorem 2.4.32 again, we find that the Mordell-Weil rank of $E(L)$ equals 2. Since E has additive reduction at $t = \pm 1$, the order of the torsion group $E(L)_{\mathrm{tors}}$ is at most 4, see [Si2], Remark IV.9.2.2. Hence we have $E(L)_{\mathrm{tors}} = \langle T_1, T_2\rangle$.

From Shioda's explicit formula for the height pairing it follows that with singular fibers only of type I_2, I_4 and I_0^*, the pairing takes values in $\frac{1}{4}\mathbb{Z}$. Hence, the lattice $\Lambda = \big(E(L)/E(L)_{\mathrm{tors}}\big)(4)$ is integral, see Definition 2.1.6. In Λ we have $\langle P,P\rangle = 6$ and $\langle Q,Q\rangle = 2$ and $\langle P,Q\rangle = 0$. Hence, by Lemma 2.1.9 the sublattice Λ' of Λ generated by P and Q has discriminant $\operatorname{disc}\Lambda' = 12 = n^2 \operatorname{disc}\Lambda$, with $n = [\Lambda : \Lambda']$. Therefore, n divides 2. Suppose $n = 2$. Then there is an $R \in \Lambda \setminus \Lambda'$ with $2R = aP + bQ$. By adding multiples of P and Q to R, we may assume $a, b \in \{0,1\}$. In Λ we get $4 | \langle 2R, 2R\rangle = 6a^2 + 2b^2$. Hence, we find $a = b = 1$, so $2R = P + Q + T$ for some torsion element $T \in E(L)[2]$. Since all the 2-torsion of $E(L)$ is rational over L, it is easy to check whether an element of $E(L)$ is in $2E(L)$. If e is the Weierstrass u-coordinate of one of the 2-torsion points, then there is a homomorphism

$$E(L)/2E(L) \to L^*/L^{*2},$$

given by $S \mapsto u(S) - e$, where $u(S)$ denotes the Weierstrass u-coordinate of the point S, see [Si1], § X.1. We can use $e = 0$ and find that for none of the four torsion points $T \in E(L)[2]$ the value $u(P+Q+T)$ is a square in L. Hence, we get $n = 1$ and $E(L)$ is generated by P, Q, T_1, and T_2.

Suppose $aP + bQ + \varepsilon_1 T_1 + \varepsilon_2 T_2$ is contained in $E(\mathbb{Q}(t))$ for some integers a, b, ε_i. Then also $bQ \in E(\mathbb{Q}(t))$. As the Galois automorphism $\sqrt{3} \mapsto -\sqrt{3}$ sends Q to $-Q$, we find that $bQ = -bQ$. But Q has infinite order, so $b = 0$. Thus, we have $E(\mathbb{Q}(t)) = \langle P, T_1, T_2\rangle$. □

To work with explicit generators of the Néron-Severi group of $\overline{Y}$, we will name some of the irreducible divisors that we encountered so far as in the table below. The exceptional curves are given by the point on $\overline{X} = X_{\mathbb{C}}$ that they lie above. Other components of singular fibers are given by their equations on $\overline{X}$. Sections are given by their equations and the name they already have.

D_1	$x = -2a, b + c = \frac{\sqrt{3}}{2}(y - z)$	D_{11}	$[-1 : -1 : 2 : -1 : -1 : 1]$
D_2	$[2 : -1 : -1 : -1 : 1 : -1]$	D_{12}	$(T_1)\colon a - b = c + y = 0$
D_3	$(\mathcal{O})\colon a + b = c - y = 0$	D_{13}	$[2 : -1 : -1 : 1 : 1 : 1]$
D_4	$[-1 : -1 : 2 : 1 : -1 : -1]$	D_{14}	$x = 2a, 2(b - c) = \sqrt{3}(y - z)$
D_5	$a = -x, b = c$	D_{15}	$(Q)\colon z = 2b, c - a = \frac{\sqrt{3}}{2}(y - x)$
D_6	$[-1 : 2 : -1 : 1 : -1 : -1]$	D_{16}	$x = 2a, 2(b - c) = \sqrt{3}(z - y)$
D_7	$(T_2)\colon a + c = b - z = 0$	D_{17}	$x = b = 0$
D_8	$[-1 : 2 : -1 : 1 : 1 : 1]$	D_{18}	$a = y = 0$
D_9	$[-1 : 2 : -1 : -1 : 1 : -1]$	D_{19}	$(P)\colon a - c = b + y = 0$
D_{10}	$a = x, b = -c$	D_{20}	F (whole fiber)

Proposition 3.3.2 *The sequence $\{D_1, \ldots, D_{20}\}$ forms an ordered basis for the Néron-Severi lattice $\mathrm{NS}(\overline{Y})$. With respect to this basis the Gram matrix of inner products is given by*

$$
\begin{pmatrix}
-2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & -2 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & -2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -2 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -2 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}.
$$

Proof. By Theorem 2.4.32 the Néron-Severi group $\mathrm{NS}(\overline{Y})$ is generated by $(\mathcal{O})$, all irreducible components of the singular fibers, and any set of generators of the Mordell-Weil group $E(L)$. Thus, from Lemma 3.2.4 and Proposition 3.3.1 we can find a set of generators for $\mathrm{NS}(\overline{Y})$. Using a computer algebra package or even by hand, one checks that $\{D_1, \ldots, D_{20}\}$ generates the same lattice. A big part of the Gram matrix is easy to compute, as we know how all fibral divisors intersect each other. Also, every section intersects each fiber in exactly one irreducible component, with multiplicity 1. The sections are rational curves, so by the adjunction formula they have self-intersection -2. That leaves $\binom{5}{2}$ more unknown intersection numbers among the sections. By applying appropriate automorphisms from $G \subset \mathrm{Aut}\ X$, we find that they are equal to intersection numbers that are already known by the above. $\square$

Remark 3.3.3 By Proposition 3.3.2 the hyperplane section H is numerically equivalent with a linear combination of the D_i. This linear combination is uniquely determined by the intersection numbers $H \cdot D_i$ for $i = 1, \ldots, 20$ and turns out to be some uninformative linear combination with many nonzero coefficients. The reason for choosing the D_i and their order in this manner is that $D_1, \ldots, D_8$ and $D_9, \ldots, D_{16}$ generate two orthogonal sublattices, both isomorphic to $E_8(-1)$. In fact, we have the following proposition, which will be used in Section 3.4.

Proposition 3.3.4 *The Néron-Severi lattice* $\mathrm{NS}(\overline{Y})$ *has discriminant* -48*. It is isomorphic to the orthogonal direct sum*

$$E_8(-1) \oplus E_8(-1) \oplus \mathbb{Z}(-2) \oplus \mathbb{Z}(-24) \oplus U,$$

where U *is the unimodular lattice with Gram matrix*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Proof. The discriminant of $\mathrm{NS}(\overline{Y})$ is the determinant of the Gram matrix, which equals -48. With respect to the basis $D_1, \ldots, D_{20}$, let $C_1, \ldots, C_4$ be defined by

$$\begin{aligned}
C_1 &= (0, 0, 0, -1, -2, -2, -2, -1, 1, 2, 3, 4, 4, 2, 0, 2, 1, -2, 0, 0)\\
C_2 &= (6, 12, 26, 29, 32, 19, 6, 16, 9, 18, 27, 36, 34, 23, 12, 17, 7, -3, -8, 4)\\
C_3 &= (1, 2, 4, 4, 4, 2, 0, 2, 2, 4, 6, 8, 8, 5, 2, 4, 2, -1, -1, 0)\\
C_4 &= (1, 2, 4, 5, 6, 4, 2, 3, 1, 2, 3, 4, 4, 3, 2, 2, 0, 0, -1, 1)
\end{aligned}$$

and let $L_1, \ldots, L_5$ be the lattices generated by $(D_1, \ldots, D_8)$, $(D_9, \ldots, D_{16})$, (C_1), (C_2), and (C_3, C_4) respectively. Then one easily checks that $L_1, \ldots, L_5$ are isomorphic to $E_8(-1)$, $E_8(-1)$, $\mathbb{Z}(-2)$, $\mathbb{Z}(-24)$, and U respectively. They are orthogonal to each other, and the orthogonal direct sum $L = L_1 \oplus \cdots \oplus L_5$ has discriminant -48 and rank 20. By Lemma 2.1.9 we find that the index $[\mathrm{NS}(\overline{Y}) : L]$ equals 1, so $\mathrm{NS}(\overline{Y}) = L$. $\square$

3.4 The surface $\overline{Y}$ is not Kummer

If A is an abelian surface, then the involution $\iota = [-1]$ has 16 fixed points. The quotient $A/\langle\iota\rangle$ therefore has 16 ordinary double points. A minimal resolution of such a quotient is called a Kummer surface. All Kummer surfaces are K3 surfaces. Because of their rich geometric structure, their arithmetic can be analyzed and described more easily. Every complex singular surface is either a Kummer surface or a double cover of a Kummer surface, see [SI], Thm. 4 and its proof. It is therefore natural to ask whether our complex singular K3 surface $\overline{Y}$ has the rich structure of a Kummer surface. In Corollary 3.4.3 we will see that this is not the case.

Shioda and Inose have classified complex singular K3 surfaces by showing that the set of their isomorphism classes is in bijection with the set of equivalence classes of positive definite even integral binary quadratic forms modulo the action of $\mathrm{SL}_2(\mathbb{Z})$, see [SI]. A singular K3 surface S corresponds with the binary quadratic form given by the intersection product on the oriented lattice $T_S = \mathrm{NS}(S)^\perp$ of transcendental cycles on S. Here the orthogonal complement is taken in the unimodular lattice $H^2(S,\mathbb{Z})$ of signature $(3,19)$ (see [BPV], Prop. VIII.3.2). To find out which quadratic form the surface $\overline{Y}$ corresponds to, we will use discriminant forms as defined by Nikulin [Ni], § 1.3, see Definition 2.1.18.

Lemma 3.4.1 *The embedding $\mathrm{NS}(\overline{Y}) \to H^2(\overline{Y},\mathbb{Z})$ makes $\mathrm{NS}(\overline{Y})$ into a primitive sublattice of the even unimodular lattice $H^2(\overline{Y},\mathbb{Z})$. We have $\operatorname{disc} T_{\overline{Y}} = 48$.*

Proof. The first statement follows from Lemma 2.2.26. From Lemma 2.1.17 and 2.1.19 we find

$$|\operatorname{disc} T_{\overline{Y}}| = |A_{T_{\overline{Y}}}| = |A_{\mathrm{NS}(\overline{Y})}| = |\operatorname{disc} \mathrm{NS}(\overline{Y})| = 48.$$

As $T_{\overline{Y}}$ is positive definite, we get $\operatorname{disc} T_{\overline{Y}} = 48$. □

Up to the action of $\mathrm{SL}_2(\mathbb{Z})$, there are only four 2-dimensional positive definite even lattices with discriminant 48. The transcendental lattice $T_{\overline{Y}}$ is equivalent to one of them. They are given by the Gram matrices

$$\begin{pmatrix} 2 & 0 \\ 0 & 24 \end{pmatrix}, \quad \begin{pmatrix} 4 & 0 \\ 0 & 12 \end{pmatrix}, \quad \begin{pmatrix} 8 & 4 \\ 4 & 8 \end{pmatrix}, \quad \begin{pmatrix} 6 & 0 \\ 0 & 8 \end{pmatrix}. \tag{3.9}$$

Proposition 3.4.2 *Under the correspondence of Shioda and Inose, the singular K3 surface $\overline{Y}$ corresponds to the matrix*

$$\begin{pmatrix} 2 & 0 \\ 0 & 24 \end{pmatrix}.$$

Proof. As $E_8(-1)$ and U as in Proposition 3.3.4 are unimodular, it follows from Proposition 3.3.4 and Lemma 2.1.17 that the discriminant-quadratic form of $\mathrm{NS}(\overline{Y})$ is isomorphic to that of $\mathbb{Z}(-2) \oplus \mathbb{Z}(-24)$. By Lemma 2.1.19 and 3.4.1 we find that the discriminant-quadratic form associated to $T_{\overline{Y}}$ is isomorphic to that of $\mathbb{Z}(2) \oplus \mathbb{Z}(24)$, whence it takes on the value $\frac{1}{24} + 2\mathbb{Z}$. Of the four lattices described in (3.9), the lattice $\mathbb{Z}(2) \oplus \mathbb{Z}(24)$ is the only one for which that is true. $\square$

Corollary 3.4.3 *The surface $\overline{Y}$ is not a Kummer surface.*

Proof. By [In], Thm. 0, a singular K3 surface S is a Kummer surface if and only if its corresponding positive definite even integral binary quadratic form is twice another such form, i.e., if $x^2 \equiv 0 \bmod 4$ for all $x \in T_S$. This is not true in our case. $\square$

3.5 All curves on X of low degree

Note that so far we have seen 63 rational curves of degree 2 on $\overline{X}$, namely those in the orbits under G of

$$\begin{array}{lll} D_{10}: & x = a, & b = -c, \\ D_{16}: & x = 2a, & 2(b-c) = \sqrt{3}(z-y), \\ D_{17}: & x = 0, & b = 0. \end{array} \tag{3.10}$$

These orbits have sizes 18, 36, and 9 respectively. All of these curves correspond to infinitely many matrices that are either trivial or not defined over $\mathbb{Q}$. To find more rational curves of low degree, we look at fibrations of $\overline{Y}$ other than f. The conic $(\mathcal{O})$ given by $a + b = c - y = 0$ on X determines a plane in the four-space in $\mathbb{P}^5$ given by $x + y + z = 0$. The family of hyperplanes in this four-space that contain that plane, cut out another family of elliptic curves on Y. One singular fiber in this family is contained in the hyperplane section $a + b = 2(c - y)$ on X. It is the degree 4 curve corresponding to the parametrization in (3.2). We will now see that this is the lowest degree of a parametrization of nontrivial matrices defined over $\mathbb{Q}$.

Recall that $G \subset \operatorname{Aut} X$ is the group of automorphisms of X generated by permutations of x, y and z, by permutations of a, b, and c and by switching the sign of two of the coordinates a, b, and c.

Proposition 3.5.1 *The union of the three orbits under the action of G of the curves described in* (3.10) *consists of all* 63 *curves on $\overline{X}$ of degree smaller than* 4.

Arguments similar to the ones used to prove Proposition 3.5.1 can be found in [Br], p. 302. To prove this proposition we will use the following lemma.

Lemma 3.5.2 *Let S be a minimal, nonsingular, algebraic K3 surface over $\mathbb{C}$. Suppose D is a divisor on S with $D^2 = -2$.*

(a) *If $D \cdot H$ is positive for some ample divisor H on S, then D is linearly equivalent with an effective divisor.*

(b) *If D is effective and its corresponding closed subscheme is reduced and simply connected, then the complete linear system $|D|$ has dimension* 0.

Proof. Since the canonical sheaf on S is trivial and the Euler characteristic χ of $\mathcal{O}_S$ equals 2, the Riemann-Roch Theorem for surfaces (see [Ha2], Thm V.1.6) tells us that

$$l(D) - s(D) + l(-D) = \frac{1}{2}D^2 + \chi = 1,$$

where $l(D) = \dim H^0(S, \mathcal{L}(D)) = \dim |D| + 1$ and $s(D) = \dim H^1(S, \mathcal{L}(D))$ is the superabundance. For (a) it is enough to prove $l(D) \geq 1$. Because $s(D)$ is nonnegative, it suffices to show $l(-D) = 0$. As we have $(-D) \cdot H < 0$, this follows from the fact that effective divisors have nonnegative intersection with ample divisors. For (b), D is effective, so we also find $l(-D) = 0$. In order to prove $l(D) = 1$, it suffices to show that $s(D) = 0$ or by symmetry, that $s(-D) = 0$. Now $\mathcal{L}(-D)$ is equal to the ideal sheaf $\mathcal{I}_Z$ of the closed subscheme Z corresponding to D and $H^1(S, \mathcal{L}(-D)) = H^1(S, \mathcal{I}_Z)$ fits in the exact sequence

$$H^0(Z, \mathcal{O}_Z) \to H^0(S, \mathcal{O}_S) \to H^1(S, \mathcal{I}_Z) \to H^1(Z, \mathcal{O}_Z).$$

As S and Z are projective and connected, the first map is an isomorphism of one-dimensional vector spaces. Hence the map $H^1(S, \mathcal{I}_Z) \to H^1(Z, \mathcal{O}_Z)$ is injective. By the Hodge decomposition we know that $H^1(Z, \mathcal{O}_Z)$ is a direct summand of $H^1(Z, \mathbb{C})$. Hence it is trivial, as Z is simply connected. Therefore, also $H^1(S, \mathcal{I}_Z)$ is trivial and $s(-D) = 0$. □

Proof of Proposition 3.5.1. Let C be a curve on $\overline{X}$ of degree d and arithmetic genus g_a and let C also denote its strict transform on $\overline{Y}$. Let its coordinates with respect to the basis $\{D_1, \ldots, D_{20}\}$ of $\mathrm{NS}(\overline{Y})$ be given by $m_1, \ldots, m_{20}$. Let H denote a hyperplane section. If E is any of the 12 exceptional curves on $\overline{Y}$, then we have $H \cdot E = 0$. For any curve D on $\overline{X}$ we have $H \cdot D = \deg D$. This determines $H \cdot D_i$ for all $i = 1, \ldots, 20$ (see Remark 3.3.3), and we find

$$\begin{aligned} d = C \cdot H = 2\big(&m_1 + m_3 + m_5 + m_7 + m_{10} + m_{12} + m_{14} + \\ &+ m_{15} + m_{16} + m_{17} + m_{18} + m_{19} + 2m_{20}\big). \end{aligned} \tag{3.11}$$

This implies that d is even, say $d = 2k$. Since we have $H^2 = 6$, we can write the divisor class $[C] \in \mathrm{NS}(\overline{Y})$ as $[C] = \frac{d}{6}H + D = \frac{k}{3}H + D$ for some element $D \in \frac{1}{6}\langle H \rangle^{\perp}$, where the orthogonal complement is taken inside $\mathrm{NS}(\overline{Y})$. From the adjunction formula (see [Ha2], Prop. V.1.5) we find $C^2 = 2g_a - 2$, so we get $D^2 = C^2 - (\frac{kH}{3})^2 = 2g_a - 2 - \frac{2k^2}{3}$. By the Hodge Index Theorem ([Ha2], Thm. V.1.9) the lattice $\frac{1}{e}\langle H \rangle^{\perp}$ is negative definite, so for fixed k and g_a there are only finitely many elements $D \in \frac{1}{e}\langle H \rangle^{\perp}$ with $D^2 = 2g_a - 2 - \frac{2k^2}{3}$. We will now make this more concrete. Set

$$
\begin{aligned}
v_1 =&2m_2 + m_5 + m_7 + m_{10} + m_{12} + m_{14} + m_{15} + m_{16} + m_{17} + m_{18} + 2m_{20} - k,\\
v_2 =&4m_3 - m_4 + 2m_5 + 2m_7 + 2m_{10} + 2m_{12} + 2m_{14} + 2m_{15} + 2m_{16} + m_{17}+\\
&+ 2m_{18} + 2m_{19} + 3m_{20} - 2k,\\
v_3 =&7m_4 - 2m_5 + 2m_7 + 2m_{10} + 2m_{12} + 2m_{14} + 2m_{15} + 2m_{16} + m_{17} + 2m_{18}+\\
&+ 2m_{19} + 3m_{20} - 2k,\\
v_4 =&33m_5 - 14m_6 + 9m_7 - 14m_8 + 9m_{10} + 9m_{12} + 9m_{14} + 9m_{15} + 9m_{16} + 15m_{17}+\\
&+ 9m_{18} + 16m_{19} + 24m_{20} - 9k,\\
v_5 =&52m_6 - 24m_7 - 14m_8 + 9m_{10} + 9m_{12} + 9m_{14} + 9m_{15} + 9m_{16} + 15m_{17} + 9m_{18}+\\
&+ 16m_{19} + 24m_{20} - 9k,\\
v_6 =&24m_7 + m_8 + 4m_{10} + 4m_{12} + 4m_{14} + 4m_{15} + 4m_{16} + 11m_{17} - 9m_{18} - 3m_{19}+\\
&+ 2m_{20} - 4k,\\
v_7 =&35m_8 + 8m_{10} + 8m_{12} + 8m_{14} + 8m_{15} + 8m_{16} + 13m_{17} + 9m_{18} + 15m_{19}+\\
&+ 22m_{20} - 8k,\\
v_8 =&2m_9 - m_{10},\\
v_9 =&211m_{10} - 140m_{11} + m_{12} + m_{14} + m_{15} + m_{16} + 41m_{17} + 23m_{18} + 50m_{19}+\\
&+ 64m_{20} - k,\\
v_{10} =&282m_{11} - 210m_{12} + m_{14} + m_{15} + m_{16} + 41m_{17} + 23m_{18} + 50m_{19} + 64m_{20} - k,\\
v_{11} =&119m_{12} - 94m_{13} + m_{14} + m_{15} + m_{16} - 53m_{17} + 23m_{18} + 50m_{19} - 30m_{20} - k,\\
v_{12} =&144m_{13} - 118m_{14} + m_{15} - 118m_{16} - 53m_{17} + 23m_{18} - 69m_{19} - 30m_{20} - k,\\
v_{13} =&86m_{14} - 71m_{15} - 58m_{16} - 5m_{17} + 23m_{18} - 9m_{19} + 18m_{20} - k,\\
v_{14} =&1231m_{15} - 672m_{16} + 249m_{17} - 595m_{18} + 259m_{19} - 346m_{20} - 19k,\\
v_{15} =&364m_{16} + 19m_{17} + 271m_{18} - 89m_{19} + 290m_{20} - 41k,\\
v_{16} =&529m_{17} + 361m_{18} + 185m_{19} + 162m_{20} - 107k,\\
v_{17} =&62m_{18} + m_{19} - 22m_{20} + 8k,\\
v_{18} =&30m_{19} - 9m_{20} - 8k,\\
v_{19} =&3m_{20} - 4k.
\end{aligned}
$$

After using (3.11) to express m_1 in terms of $m_2, \ldots, m_{20}$, and k, we can rewrite the equation $C^2 = 2g_a - 2$ as

$$
\begin{aligned}
112(3 - 3g_a + k^2) = 84v_1^2 + 42v_2^2 + 6v_3^2 + \frac{4v_4^2}{11} + \frac{14v_5^2}{143} + \frac{7v_6^2}{13}+\\
+ \frac{v_7^2}{5} + 84v_8^2 + \frac{6v_9^2}{1055} + \frac{28v_{10}^2}{9917} + \frac{12v_{11}^2}{799} + \frac{v_{12}^2}{102} + \frac{7v_{13}^2}{258}+\\
+ \frac{7v_{14}^2}{52933} + \frac{6v_{15}^2}{16003} + \frac{6v_{16}^2}{6877} + \frac{336v_{17}^2}{16399} + \frac{28v_{18}^2}{155} + \frac{28v_{19}^2}{5}.
\end{aligned}
\tag{3.12}
$$

Suppose k and g_a are fixed. Since the m_i are all integral, so are the v_j. As the right-hand side of (3.12) is a positive definite quadratic form in the v_j, we find that there are only finitely many integral solutions $(v_1, \ldots, v_{19})$ of (3.12). The m_i being linear combinations of the v_j, there are also only finitely many integral solutions in terms of the m_i. In our case the even degree d is smaller than 4, so $d = 2$ and $k = 1$. As all curves have even degree, the conic C is irreducible and hence, as all irreducible conics are, smooth. Therefore we have $g_a = 0$. A computer search shows that for $k = 1$ and $g_a = 0$ there are exactly 441 solutions of (3.12) corresponding to integral m_i.

By Lemma 3.5.2(a) these correspond to 441 effective divisor classes $[D]$ on $\overline{Y}$ with $D^2 = -2$ and $H \cdot D = 2$. We will exhibit 441 of such divisors satisfying the hypotheses of Lemma 3.5.2(b). That lemma then implies that each is the only effective divisor in its equivalence class and we conclude that they are the only 441 effective divisors D on $\overline{Y}$ satisfying $D^2 = -2$ and $D \cdot H = 2$.

The first 9 of these 441 divisors correspond to the curves in the orbit of D_{17}. Another 16 correspond to $D_{10} + \varepsilon_1 E_1 + \varepsilon_2 E_2 + \varepsilon_3 E_3 + \varepsilon_4 E_4$ where $\varepsilon_i \in \{0, 1\}$ and the E_i are the four exceptional curves of π that meet D_{10}. Each of these 16 divisors generates an orbit under G of size 18, giving 288 divisors on $\overline{Y}$ altogether. The last 144 divisors correspond to the divisors in the size 36 orbits of $D_{16} + \delta_1 M_1 + \delta_2 M_2$, with $\delta_i \in \{0, 1\}$ and where M_1 and M_2 are the exceptional curves of π in the fiber above $t = 2$. Of these 441 effective divisors, only 63 are the strict transform of a curve on $\overline{X}$, all in an orbit of one of the curves described in (3.10). $\square$

Chapter 4

An elliptic K3 surface associated to Heron triangles

4.1 Introduction

A *rational triangle* is a triangle with rational sides and area. A *Heron triangle* is a triangle with integral sides and area. Let $\mathbb{Q}(s)$ denote the field of rational functions in s with coefficients in $\mathbb{Q}$. The main theorem of this chapter states the following.

Theorem 4.1.1 *There exists a sequence $\{(a_n, b_n, c_n)\}_{n\geq 1}$ of triples of elements in $\mathbb{Q}(s)$ such that*

1. *for all $n \geq 1$ and all $\sigma \in \mathbb{R}$ with $\sigma > 1$, there exists a triangle $\Delta_n(\sigma)$ with sides $a_n(\sigma)$, $b_n(\sigma)$, and $c_n(\sigma)$, inradius $\sigma - 1$, perimeter $2\sigma(\sigma+1)$, and area $\sigma(\sigma^2-1)$, and*
2. *for all $m, n \geq 1$ and $\sigma_0, \sigma_1 \in \mathbb{Q}$ with $\sigma_0, \sigma_1 > 1$, the rational triangles $\Delta_m(\sigma_0)$ and $\Delta_n(\sigma_1)$ are similar if and only if $m = n$ and $\sigma_0 = \sigma_1$.*

Remark 4.1.2 The triples of the sequence mentioned in Theorem 4.1.1 can be computed explicitly. We will see that we can take the first four to be

$$(a_n, b_n, c_n) = \left(\frac{s(s+1)(y_n+z_n)}{x_n+y_n+z_n}, \frac{s(s+1)(x_n+z_n)}{x_n+y_n+z_n}, \frac{s(s+1)(x_n+y_n)}{x_n+y_n+z_n}\right), \tag{4.1}$$

with

$$
\begin{aligned}
(x_1,y_1,z_1) &= \big(1+s, -1+s, (-1+s)s\big),\\
x_2 =&(-1+s)(1+6s-2s^2-2s^3+s^4)^3,\\
y_2 =&(-1+s)(-1+4s+4s^2-4s^3+s^4)^3,\\
z_2 =&s(1+s)(3+4s^2-4s^3+s^4)^3,\\
x_3 =&(-1+s)(1+2s+2s^2-2s^3+s^4)^3\\
&(-1-22s+66s^2+14s^3-72s^4+30s^5+6s^6-6s^7+s^8)^3,\\
y_3 =&(1+s)(-1+20s+68s^2-84s^3+139s^4+32s^5-224s^6+\\
&64s^7+149s^8-148s^9+60s^{10}-12s^{11}+s^{12})^3,\\
z_3 =&(-1+s)s(5+10s+126s^2+62s^3-225s^4+52s^5+28s^6+\\
&12s^7+27s^8-62s^9+38s^{10}-10s^{11}+s^{12})^3,\\
x_4 =&(1+s)(-1-62s+198s^2+1698s^3+7764s^4-8298s^5-10830s^6+43622s^7-15685s^8\\
&-45356s^9-1348s^{10}+75284s^{11}-13088s^{12}-93076s^{13}+85220s^{14}+12s^{15}-49467s^{16}\\
&+40842s^{17}-16034s^{18}+2282s^{19}+844s^{20}-546s^{21}+138s^{22}-18s^{23}+s^{24})^3,\\
y_4 =&(-1+s)(-1+54s+550s^2-10s^3+5092s^4+16674s^5+98s^6-51662s^7+22875s^8+\\
&41916s^9-63076s^{10}+45628s^{11}+13088s^{12}-63644s^{13}+38884s^{14}+17668s^{15}-\\
&31195s^{16}+8302s^{17}+8990s^{18}-9554s^{19}+4476s^{20}-1254s^{21}+218s^{22}-22s^{23}+s^{24})^3,\\
z_4 =&(-1+s)s(-7-28s-1168s^2-2588s^3+5170s^4+6940s^5+20176s^6-10628s^7-\\
&70305s^8+46664s^9+85440s^{10}-107832s^{11}+380s^{12}+66840s^{13}-46848s^{14}+13656s^{15}-\\
&1465s^{16}-2796s^{17}+5712s^{18}-5228s^{19}+2738s^{20}-884s^{21}+176s^{22}-20s^{23}+s^{24})^3.
\end{aligned}
$$

Multiplying these four triples by a common denominator and substituting only integral σ, we obtain an infinite parametrized family of quadruples of pairwise nonsimilar Heron triangles, all with the same area and the same perimeter. For any positive integer N we can do the same to N triples of the sequence. We find that Theorem 4.1.1 implies the following corollary.

Corollary 4.1.3 *For every integer $N > 0$ there exists an infinite family, parametrized by $s \in \mathbb{Z}_{>0}$, of N-tuples of pairwise nonsimilar Heron triangles, all N with the same area $A(s)$ and the same perimeter $p(s)$, such that for any two different s and s' the corresponding ratios $A(s)/p(s)^2$ and $A(s')/p(s')^2$ are different.*

This corollary generalizes a theorem of Mohammed Aassila [Aa], and Alpar-Vajk Kramer and Florian Luca [KL]. Their papers give identical parametrizations to prove the existence of an infinite parametrized family of *pairs* of Heron triangles with the same area and perimeter. The corollary also answers the question, posed by Alpar-Vajk Kramer and Florian Luca and later by Richard Guy, whether triples of Heron triangles with the same area and perimeter exist, or even N-tuples with $N > 3$. Shortly after Richard Guy had posed this question, Randall Rathbun found with a computer search a set of 8 Heron triangles with the same area and perimeter. Later he found the smallest 9-tuple. Using our methods, we can find an N-tuple for any given positive

a	b	c
1154397878350700583600	2324466316136026062000	2632653985016982326400
1096939160423742636000	2485350726331508315280	2529228292748458020720
1353301222256224441200	2044007602377661720800	2714209354869822810000
1326882629217053462400	2076293397636039582000	2708342152650615927600
1175291957596867110000	2287901677455234640800	2648324544451607221200
1392068029775844821400	1997996327914674087000	2721453821813190063600
1664717974861560418800	1703885276761144351875	2742914927881004201325
1159621398162242215200	2314969007387768550000	2636927773953698206800
1582886815525601586000	1787918651729320350240	2740712712248787035760
1363338670812365847600	2031949206689694692400	2716230302001648432000
1629738181200989059200	1739432097243363322800	2742347901059356590000
1958819929328111850000	1426020908550865426800	2726677341624731695200
2256059203526140412400	1195069414854334519500	2660389561123234040100
2227944754401017652000	1213597769548172408400	2669975655554518911600
2005582596002614412784	1385590865209533198216	2720344718291561361000
2462169105650632177800	1100472310428896790000	2548876763424180004200
2198208931289532607600	1234160196742812482000	2679149051471363882400
2440795514101169425200	1105486738297174396800	2565235927105365150000
2469616851505228370400	1099107024377149242000	2542794303621331359600
2623055767363274578335	1143817472264343917040	2344644939876090476625
$p = a + b + c = 6111518179503708972000$		
$A = 1340792724147847711994993266314426038400000$		

Table 4.1: 20 triangles with the same area and the same perimeter

integer N. For example, Table 4.1 shows 20 values of a, b, and c such that the triangle with sides a, b, and c has perimeter p and area A as given.

We will exhibit a bijection between the set of triples (a, b, c) of sides of (rational) triangles up to scaling and a subset of the set of (rational) points on a certain algebraic surface X that we will describe in Section 4.2. We will prove Theorem 4.1.1 in Section 4.3 by finding infinitely many suitable curves on X. We will use that some blow-up $\widetilde{X}$ of X can be given the structure of an elliptic surface over $\mathbb{P}^1$, which follows from one of the constructions of elliptic surfaces described in Section 2.5.

The relation between the geometry and the arithmetic of K3 surfaces in general is not clear at all, see [BT]. The last section of this chapter is therefore dedicated to a deeper analysis of the geometry of the K3 surface Y. This section not needed for the proof of the main theorem and serves its own interest. Section 2.6 is used in section 4.4 to determine the full Néron-Severi group of Y and the Mordell-Weil group of the generic fiber of $Y \to C$.

The results of this chapter and those of Sections 2.5 and 2.6 have been combined into a preprint, see [VL2]. The main theorem has also been incorporated in Guy's book on unsolved problems in number theory in the sections about Heron triangles, see [Gu], D21 and D22.

4.2 A surface associated to Heron triangles

For a triangle with sides a, b, and c, let r, p, and A denote its inradius, perimeter, and area respectively. The line segments from the vertices of the triangle to the midpoint of the incircle divide the triangle in three smaller triangles of areas $ar/2$, $br/2$, and $cr/2$. Adding these we find $A = rp/2$. Set $x = p/2 - a$, $y = p/2 - b$, and $z = p/2 - c$. Then we get $p = 2(x + y + z)$, so $A = r(x + y + z)$. Heron's formula $A^2 = (x + y + z)xyz$ then yields $r^2(x + y + z) = xyz$. Therefore, the point $[r : x : y : z] \in \mathbb{P}^3$ lies on the surface $X \subset \mathbb{P}^3_{\mathbb{Q}}$ given by $r^2(x + y + z) = xyz$. Conversely, if $[1 : x : y : z]$ lies on X, with $x, y, z > 0$, then the triangle with sides $a = y + z$, $b = x + z$, and $c = x + y$ has inradius 1. Thus we get a bijection between the set of triples (a, b, c) of sides of triangles up to scaling and the set of real points $[r : x : y : z]$ on X with positive ratios x/r, y/r, and z/r. Let $G \subset \operatorname{Aut} X$ denote the group of automorphisms of X induced by the permutations of the coordinates x, y, and z. Let $f\colon X \dashrightarrow \mathbb{P}^1$ be the rational map given by $f\colon [r : x : y : z] \mapsto [r : x + y + z]$. Note that if we let G act trivially on $\mathbb{P}^1$, then f commutes with the action of G.

Lemma 4.2.1 *For $i = 1, 2$, let Δ_i denote a triangle, let a_i, b_i, and c_i denote the sides of Δ_i, and let P_i be the point on X corresponding to the equivalence class (under scaling) of the triple (a_i, b_i, c_i). Then Δ_1 and Δ_2 are similar if and only if P_1 and P_2 are in the same orbit under G. Up to scaling, Δ_1 and Δ_2 have the same inradius and perimeter if and only if P_1 and P_2 map to the same point under f.*

Proof. This is obvious. □

To set our strategy for proving Theorem 4.1.1, note that it asserts that for fixed σ, the infinitely many pairwise nonsimilar triangles $\Delta_n(\sigma)$, with $n \geq 1$, all have the same perimeter $2\sigma(\sigma+1)$ and inradius $\sigma-1$. By Lemma 4.2.1 this is equivalent to the statement that the infinitely many points corresponding to the triples $(a_n(\sigma), b_n(\sigma), c_n(\sigma))$ all map under f to $[\sigma - 1 : \sigma(\sigma + 1)]$, and that they are all in different orbits under G. To prove Theorem 4.1.1, we will find a suitable infinite collection of curves on X, mapping surjectively to $\mathbb{P}^1$ under f. Those maps will not be surjective on rational points, but for rational σ each of these curves will intersect $f^{-1}([\sigma - 1 : \sigma(\sigma + 1)])$ in a rational point.

Remark 4.2.2 Since the equation $r^2(x + y + z) = xyz$ is linear in x, we find that X is rational. A parametrization is given by the birational equivalence $\mathbb{P}^2 \dashrightarrow X$, given by

$$\begin{aligned} [r : x : y : z] &= [vw(u - v) : v(uv + w^2) : w^2(u - v) : uv(u - v)], \quad \text{or} \\ [u : v : w] &= [yz : r^2 : yr]. \end{aligned}$$

4.3 Proof of the main theorem

The rational map f is defined everywhere, except at the three intersection points $M_1 = [0:0:1:-1]$, $M_2 = [0:1:0:-1]$, and $M_3 = [0:1:-1:0]$ of X with the line L given by $r = x+y+z = 0$. A straightforward computation shows that X has exactly three singular points $N_1 = [0:1:0:0]$, $N_2 = [0:0:1:0]$, and $N_3 = [0:0:0:1]$. They are all ordinary double points, forming a full orbit under G, and all mapping to $[0:1]$ under f. Let $\pi\colon \widetilde{X} \to X$ be the blow-up of X at the six points M_i and N_i. Let $\widetilde{M}_i$ and $\widetilde{N}_i$ denote the exceptional curves above M_i and N_i respectively.

Proposition 4.3.1 *The surface $\widetilde{X}$ is smooth. The rational map $f \circ \pi$ extends to a morphism $\widetilde{f}\colon \widetilde{X} \to \mathbb{P}^1$. It maps the $\widetilde{M}_i$ isomorphically to $\mathbb{P}^1$ and together with the section $\mathcal{O} = \widetilde{f}|_{\widetilde{M}_3}^{-1}$ it makes $\widetilde{X}_k$ into an elliptic surface over $\mathbb{P}^1$ for any algebraically closed field k of characteristic* 0.

Proof. Ordinary double points are resolved by blowing up once, see [Ha2], exc. I.5.7. Hence $\widetilde{X}$ is the minimal desingularization of X blown up at the M_i. The rational map f sends all points of X (except for the M_i) in the plane through L given by $t_1 r = t_0(x+y+z)$ to the point $[t_0 : t_1]$. Hence this proposition follows from Proposition 2.5.3. □

Remark 4.3.2 In this explicit case, it would have been easier to check by hand that $\widetilde{f}$ makes $\widetilde{X}_k$ into an elliptic surface over $\mathbb{P}^1$. From Theorem 2.3.7 it follows that, in order to prove that $\widetilde{f}$ is a minimal fibration, it suffices to check that no reducible fiber contains a rational curve with self-intersection -1. As the only singular points of X lie above $[0:1] \in \mathbb{P}^1$, it follows that for all $\tau \neq 0, \infty$, the fiber $\widetilde{X}_\tau$ above $[\tau : 1]$ is given by the intersection of X with the plane given by $r = \tau(x+y+z)$. Hence for $\tau \neq 0, \infty$, the fiber is isomorphic to the plane curve given by $\tau^2(x+y+z)^3 = xyz$, which is nonsingular as long as $\tau(27\tau^2 - 1) \neq 0$. For τ with $27\tau^2 = 1$ we get a nodal curve, whence a fiber of type I_1, following the Kodaira-Néron classification of special fibers, see [Si2], IV.8 and [Ko2]. At $\tau = 0$ and $\tau = \infty$ one checks that the fibers are of type I_6 and IV respectively. None of these fibers contains an exceptional curve.

Remark 4.3.3 From the previous remark, it follows that the fiber of $\widetilde{f}$ above every *rational* point $[\tau : 1] \in \mathbb{P}^1$ with $\tau > 0$, is a curve of genus 1, which can therefore not be rationally parametrized. Therefore, there is no rational parametrization of infinitely many rational triangles, all having the same area and the same perimeter.

Remark 4.3.4 Later we will see a Weierstrass form for the generic fiber of $\widetilde{f}$. Based on that, Tate's algorithm (see [Si2], IV.9 and [Ta3]) describes the special fibers of a minimal proper regular model. They coincide with the fibers described in Remark 4.3.2, which gives another proof of the fact that $\widetilde{f}$ is relatively minimal.

Let E denote the generic fiber of $\widetilde{f}$, an elliptic curve over $k(\mathbb{P}^1) \cong \mathbb{Q}(t)$. By Lemma 2.3.13 we can identify the sets $\widetilde{X}(\mathbb{P}^1)$ and $E(k(\mathbb{P}^1))$. The curve E is isomorphic to the plane curve in $\mathbb{P}^2_{\mathbb{Q}(t)}$ given by

$$t^2(x+y+z)^3 = xyz. \tag{4.2}$$

The origin $\mathcal{O} = \widetilde{M_3}$ then has coordinates $[x : y : z] = [1 : -1 : 0]$. Let P denote the section $\widetilde{M_1} = [0 : 1 : -1]$. A standard computation shows that the $\widetilde{M_i}$ correspond with inflection points. As they all lie on the line given by $x + y + z = 0$, we find that P has order 3 and $2P = \widetilde{M_2} = [1 : 0 : -1]$. This also follows from the following lemma, which gives a different interpretation of the action of G.

Lemma 4.3.5 *The automorphism $\widetilde{X} \to \widetilde{X}$ induced by the 3-cycle $(x\,y\,z)$ on the coordinates of X corresponds with translation by P on each nonsingular fiber and on the generic fiber of $\widetilde{f}$. Similarly, the automorphism induced by $(x\,y)$ corresponds with multiplication by -1.*

Proof. Let $\mathrm{Aut}\,(E)$ be the group of all automorphisms of the generic fiber E and let $\mathrm{Aut}\,(E, \mathcal{O})$ be the subgroup of those automorphisms that fix the point $\mathcal{O}$. Then $\mathrm{Aut}\,(E)$ is isomorphic to the semi-direct product $E(\mathbb{Q}(t)) \rtimes \mathrm{Aut}\,(E, \mathcal{O})$ of the group of translations, isomorphic to $E(\mathbb{Q}(t))$, and the group $\mathrm{Aut}\,(E, \mathcal{O})$. Consider the composition

$$S_3 = G \to \mathrm{Aut}\,(E) \cong E(\mathbb{Q}(t)) \rtimes \mathrm{Aut}\,(E, \mathcal{O}) \to \mathrm{Aut}\,(E, \mathcal{O}).$$

As the automorphism group of an elliptic curve over a field of characteristic 0 is abelian, we find that the commutator subgroup A_3 of S_3 is contained in the kernel of this composition. We conclude that the automorphism φ induced by $(x\,y\,z)$ is a translation by $\varphi(\mathcal{O}) = P$. Hence $\varphi = T_P$ on E. As E is dense in $\widetilde{X}$, we find $\varphi = T_P$ on $\widetilde{X}$, see [Ha2], exc. II.4.2. Let $\mathrm{End}\,(E, \mathcal{O})$ denote the ring of all endomorphisms of E that fix $\mathcal{O}$. The automorphism ψ induced by $(x\,y)$ fixes $\mathcal{O}$, so we have $\psi \in \mathrm{Aut}\,(E, \mathcal{O}) \subset \mathrm{End}\,(E, \mathcal{O})$. As the endomorphism ring of an elliptic curve over a field of characteristic 0 is a commutative integral domain, and we have $\psi^2 = 1$ and $\psi \neq 1$, we find $\psi = [-1]$. $\square$

As mentioned before, we want infinitely many τ for which the fiber X_τ above $[\tau : 1]$ has infinitely many rational points $[r_i : x_i : y_i : z_i]$ with x_i/r_i, y_i/r_i, $z_i/r_i > 0$, and all in different orbits under G. If the Mordell-Weil rank of $E(\mathbb{Q}(t)) \cong \widetilde{X}(\mathbb{P}^1)$ had been positive, we might have been able to find infinitely many such points for almost all rational τ satisfying some inequalities. Unfortunately, the next theorem tells us that this is not the case.

Theorem 4.3.6 *The Mordell-Weil group $E(\mathbb{C}(t))$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. It is generated by the 3-torsion point P and the point Q given by $[r : x : y : z] = [t : it : -it : 1]$. The Mordell-Weil group $E(\mathbb{R}(t))$ is equal to $\langle P \rangle \cong \mathbb{Z}/3\mathbb{Z}$.*

Proof. As $\widetilde{X}$ is rational, the Néron-Severi group $\mathrm{NS}(\widetilde{X}_{\mathbb{C}})$ is a unimodular lattice of rank 10, see [Shi3], Lemma 10.1. Let $T \subset \mathrm{NS}(\widetilde{X}_{\mathbb{C}})$ be as in Theorem 2.4.32. From Remark 4.3.2 and Theorem 2.4.32, we find that T has rank $2+(6-1)+(3-1)+(1-1)+(1-1) = 9$ and we can find explicit generators. Consider the lattice $T + \langle (P), (Q) \rangle$. Computing the explicit intersections of our generators, we find that the lattice $T + \langle (P), (Q) \rangle$ has rank 10, and thus it has finite index in $\mathrm{NS}(\widetilde{X}_{\mathbb{C}})$. Also, it is already unimodular, so it is equal to $\mathrm{NS}(\widetilde{X}_{\mathbb{C}})$. Hence, $E(\mathbb{C}(t))$ is generated by P and Q and has rank 1.

Complex conjugation on Q permutes the x- and y-coordinates, so by Lemma 4.3.5 we find $\overline{Q} = -Q$ in $E(\mathbb{C}(t))$. If $mQ + nP$ is real for some integers m, n, then so is mQ and hence $mQ = m\overline{Q} = -mQ$, so $2mQ = 0$. Since Q has infinite order, we conclude that $m = 0$, so $E(\mathbb{R}(t)) = \langle P \rangle$. □

To find more curves over $\mathbb{Q}$, we will apply a base change to our base curve $\mathbb{P}^1$ by a rational curve on $\widetilde{X}$. As we have a parametrization of X, it is easy to find such a curve. Taking $u = s$ and $v = w = 1$ in the parametrization of Remark 4.2.2, we find a curve C on X parametrized by

$$\beta \colon \mathbb{P}^1 \to C, \quad [s : 1] \mapsto [r : x : y : z] = [s-1 : s+1 : s-1 : s(s-1)].$$

We will denote its strict transform on $\widetilde{X}$ by C as well. The map $\widetilde{f}$ induces a 2-1 map from C to $\mathbb{P}^1$. The composition $\widetilde{f} \circ \beta$ is given by $[s : 1] \mapsto [s-1 : s(s+1)]$. Hence, if we identify the function field $K = k(C)$ of C with $\mathbb{Q}(s)$, then the field extension $K/k(\mathbb{P}^1)$ is given by $\mathbb{Q}(t) \hookrightarrow \mathbb{Q}(s),\ t \mapsto (s-1)s^{-1}(s+1)^{-1}$. Throughout the rest of this chapter, as in Theorem 4.1.1 and Remarks 4.3.2 and 4.3.3, one should think of σ and τ as specific values for the indeterminates s and t respectively.

Let Y denote the fibered product $\widetilde{X} \times_{\mathbb{P}^1} C$, let δ denote the projection $Y \to \widetilde{X}$, and let g denote the projection $Y \to C$. The generic fiber of g is isomorphic to $E_K = E \times_{k(\mathbb{P}^1)} K$. The identity on C and the composition $\mathcal{O} \circ \widetilde{f}|_C \colon C \to \widetilde{X}$ together induce a section $C \to Y$ of g, which we will also denote by $\mathcal{O}$. The closed immersion $C \to \widetilde{X}$ and the identity on C together induce a section of g which we will denote by R.

$$\begin{tikzcd}
& Y \arrow[r, "\delta"] \arrow[dd, "g"] & \widetilde{X} \arrow[dr, "\pi"] \arrow[dd, "\widetilde{f}"'] & \\
& & & X \arrow[dl, dashed, "f"] \\
\mathbb{P}^1 \arrow[r, "\cong", "\beta"'] & C \arrow[r, "\widetilde{f}|_C"'] \arrow[uu, bend left, "R"] \arrow[uur, hook] & \mathbb{P}^1 &
\end{tikzcd}$$

Proposition 4.3.7 *The fibration g and its section $\mathcal{O}$ make Y_k into an elliptic surface over C_k for any algebraically closed field k of characteristic 0.*

Proof. One easily checks that $\widetilde{f}|_C \colon C \to \mathbb{P}^1$ is unramified at the points of $\mathbb{P}^1$ where $\widetilde{f}$ has singular fibers. Hence, this proposition follows immediately from Proposition 2.5.15

and Proposition 4.3.1. $\square$

From (4.2) we find that E_K is isomorphic to the plane cubic over K given by

$$(s-1)^2(x+y+z)^3 = s^2(s+1)^2 xyz.$$

The linear transformation

$$p = -4(s-1)^2(x+y)z^{-1}, \qquad q = 4(s-1)^2 s(s+1)(x-y)z^{-1}, \tag{4.3}$$

or, equivalently,

$$\begin{aligned} x &= -s(s+1)p + q, \\ y &= -s(s+1)p - q, \\ z &= 8(s-1)^2 s(s+1), \end{aligned} \tag{4.4}$$

gives the Weierstrass equation

$$q^2 = (p - 4(s-1)^2)^3 + s^2(s+1)^2 p^2 = F(s,p) \tag{4.5}$$

with

$$\begin{aligned} j = j(E_K) = j(E) &= \frac{(24t^2-1)^3}{t^6(27t^2-1)}, \\ \Delta = 2^{12}(s-1)^6 s^4 (s+1)^4 &(s^4 + 2s^3 - 26s^2 + 54s - 27). \end{aligned} \tag{4.6}$$

The Weierstrass coordinates of P and R are given by

$$\begin{aligned} (p_P, q_P) &= (4(s-1)^2, 4s(s+1)(s-1)^2) \qquad \text{and} \\ (p_R, q_R) &= (8 - 8s, 8s^2 - 8). \end{aligned}$$

Proposition 4.3.8 *The section R has infinite order in the group $Y(C) \cong E_K(K)$.*

Proof. The p-coordinate of $2R+P$ equals $4(s^4 - 6s^3 + 10s^2 - 2s + 1)(s-1)^{-2}$, so $2R+P$ is contained in the kernel of reduction at $s-1$. In characteristic 0 the kernel of reduction has no nontrivial torsion (see [Si1], Prop. VII.3.1), so we find that $2R+P$ has infinite order, whence so does R. $\square$

For every integer $n \geq 1$, let $\gamma_n \colon \mathbb{P}^1 \to X$ denote the composition

$$\mathbb{P}^1 \xrightarrow{\beta} C \xrightarrow{(2n-1)R} Y \xrightarrow{\delta} \widetilde{X} \xrightarrow{\pi} X. \tag{4.7}$$

Theorem 4.1.1 will follow from the following proposition.

Proposition 4.3.9 *Let $\sigma > 1$ be a real number. For every integer $n \geq 1$, let r_n, x_n, y_n, and z_n be such that $\gamma([\sigma : 1]) = [r_n : x_n : y_n : z_n]$ and set*

$$a_n = \frac{(\sigma-1)(y_n+z_n)}{r_n}, \quad b_n = \frac{(\sigma-1)(x_n+z_n)}{r_n}, \quad c_n = \frac{(\sigma-1)(x_n+y_n)}{r_n}.$$

Then for every $n \geq 1$ there is a triangle Δ_n with sides a_n, b_n, c_n, perimeter $2\sigma(\sigma+1)$, inradius $\sigma - 1$, and area $\sigma(\sigma^2-1)$. If σ is rational, then the triangles Δ_n are pairwise nonsimilar.

Proof. Let a real number $\sigma > 1$ be given and set $c = \beta([\sigma : 1]) \in C$. Then $\widetilde{f}|_C(c) = [\tau : 1]$ for $\tau = (\sigma - 1)\sigma^{-1}(\sigma + 1)^{-1} > 0$, so the fiber Y_c is isomorphic to the fiber $\widetilde{X}_\tau$ of $\widetilde{f}$ above $[\tau : 1]$. All roots of Δ in (4.6) are less than 1, so this fiber is nonsingular. By Remark 4.3.2, it is isomorphic to the intersection E_τ of X with the hyperplane given by $r = \tau(x + y + z)$. This intersection E_τ can be given the structure of an elliptic curve with M_3 as origin. The specialization map $Y(C) \to Y_c(\mathbb{Q})\colon S \mapsto S \cap Y_c = S(c)$ induces a homomorphism $\psi\colon Y(C) \to E_\tau \subset X$ sending a section S of g to $\pi(\delta(S(c)))$. Set $\Theta_n = \gamma_n([\sigma : 1]) \in X = [r_n : x_n : y_n : z_n]$. Then we have $\Theta_n = \psi((2n-1)R) \in E_\tau$, so on E_τ we get $\Theta_n = (2n - 1)\Theta_1$. The elliptic curve E_τ has a Weierstrass model $q^2 = F(\sigma, p)$, see (4.5). For $n \geq 1$, let (p_n, q_n) denote the Weierstrass coordinates of Θ_n, so $(p_1, q_1) = (8 - 8\sigma, 8\sigma^2 - 8)$.

Note that $F(\sigma, 0) = -64(\sigma-1)^6 < 0$, but for $p_1 = 8-8\sigma < 0$ we have $F(\sigma, p_1) = q_1^2 > 0$. We conclude that for any real point on E_τ with Weierstrass coordinates (p, q), the condition $p < 0$ is equivalent to the point lying on the real connected component of E_τ that does not contain $\mathcal{O}$. Since Θ_1 lies on this component, so do all its odd multiples Θ_n.

If $\Theta_n = M_i$ for $i = 1, 2$, or 3, then $3\Theta_n = \mathcal{O}$, which contradicts the fact that Θ_n lies on the real component of E_τ that does not contain $\mathcal{O}$. Hence f is well-defined at Θ_n and from $[r_n : x_n + y_n + z_n] = f(\Theta_n) = [\tau : 1]$, with $\tau > 0$, we find $r_n \neq 0$ and $x_n + y_n + z_n \neq 0$, whence $x_n y_n z_n \neq 0$. To make computations easier, we may assume $z_n = 8(\sigma - 1)^2\sigma(\sigma + 1) > 0$. As Θ_n lies on the real connected component that does not contain $\mathcal{O}$, we have $p_n < 0$ and therefore also $p_n < 4(\sigma - 1)^2$. That implies

$$(\sigma(\sigma + 1)p_n)^2 = q_n^2 - (p_n - 4(\sigma - 1)^2)^3 > q_n^2$$

and combined with $p_n < 0$ this gives $-\sigma(\sigma + 1)p_n > |q_n|$. By (4.4) we get

$$\begin{aligned} x_n &= -\sigma(\sigma + 1)p_n + q_n > 0, \\ y_n &= -\sigma(\sigma + 1)p_n - q_n > 0. \end{aligned}$$

From $r_n = \tau(x_n + y_n + z_n)$ we also find $r_n > 0$. We conclude $x_n/r_n, y_n/r_n, z_n/r_n > 0$, which proves that there is a triangle with sides a_n, b_n, and c_n. This triangle has inradius $\sigma - 1$, perimeter $2(\sigma - 1)(x_n + y_n + z_n)/r_n = 2(\sigma - 1)/\tau = 2\sigma(\sigma + 1)$ and hence area $\sigma(\sigma^2 - 1)$.

Now suppose σ is rational. We will show that Θ_1 has infinite order. Assume that Θ_1 has finite order. As Θ_1 lies on the real component that does not contain $\mathcal{O}$, it has even order, so by Mazur's Theorem (see [Si1], Thm. III.7.5 for statement, [Maz], Thm. 8 for a proof) we find that $m\Theta_1 = \mathcal{O}$ for $m = 8, 10$, or 12. For each of these three values for m we can compute explicit rational functions $\xi_m, \eta_m \in \mathbb{Q}(s)$ such that the coordinates of $m\Theta_1$ are given by $(\xi_m(\sigma), \eta_m(\sigma))$. For $m = 8, 10$, or 12, these rational functions turn out to not have any rational poles, so Θ_1 has infinite order. To show that the triangles are pairwise nonsimilar, it suffices by Lemma 4.2.1 to show that the Θ_n lie in different orbits under G. Suppose that Θ_n and $\Theta_{n'}$ are in the same orbit under G for some $n, n' \geq 1$. Then by Lemma 4.3.5 we get $\Theta_n = \pm\Theta_{n'} + kP$ for $k = 0, 1$ or 2. Hence $3\left((2n-1) \mp (2n'-1)\right)\Theta_1 = 3(\Theta_n \mp \Theta_{n'}) = 3kP = \mathcal{O}$, so $2n - 1 = \pm(2n' - 1)$, as Θ_1 has infinite order. From $n, n' \geq 1$ we find $n = n'$ and hence $k = 0$. Thus, $\Theta_n = \Theta_{n'}$. $\square$

Proof of Theorem 4.1.1. Consider the open affine subset $U \subset X$ defined by $r \neq 0$, which is isomorphic to $\operatorname{Spec} A$ for $A = \mathbb{Q}[x, y, z]/\big(x + y + z - xyz\big)$. For each $n \geq 1$, let $V_n \subset \mathbb{P}^1$ be a dense open affine subset such that the composition γ_n of morphisms in (4.7) maps V_n to U. This is possible because the image of $\mathbb{P}^1$ is not entirely contained in the closed subset of X given by $r = 0$. Then there is a ring $B_n \subset \mathbb{Q}(s)$ such that V_n is isomorphic to $\operatorname{Spec} B_n$ and the composition in (4.7) is given by a ring homomorphism $\varphi_n \colon A \to B_n \subset \mathbb{Q}(s)$. Let $x_n(s)$, $y_n(s)$, $z_n(s) \in \mathbb{Q}(s)$ be the images under φ_n of $x, y, z \in A$ respectively. Then for any real number $\sigma > 1$ the values r_n, x_n, y_n, and z_n from Proposition 4.3.9 can be given by 1, $x_n(\sigma)$, $y_n(\sigma)$, and $z_n(\sigma)$ respectively. It follows from Proposition 4.3.9 that 1 and 2 of Theorem 4.1.1 are true for $a_n(s) = (y_n(s)+z_n(s))(s-1)$, $b_n(s) = (x_n(s) + z_n(s))(s - 1)$, and $c_n(s) = (x_n(s) + y_n(s))(s - 1)$. Note that if $\sigma_0 \neq \sigma_1$, then $\Delta_n(\sigma_0)$ is automatically not similar to $\Delta_m(\sigma_1)$ for any $m, n \geq 1$. $\square$

Corollary 4.3.10 *The set of rational points on Y is Zariski dense in Y.*

Proof. The infinitely many multiples of the section R give infinitely many curves on Y, each with infinitely many rational points. Hence the Zariski closure of the set of rational points is Y. $\square$

Remark 4.3.11 The four triples given in Remark 4.1.2 correspond to the sections $R, 3R, 5R$, and $7R$.

Remark 4.3.12 As mentioned before, Randall Rathbun found with a computer search a set of 8 Heron triangles with the same area and perimeter. His triangles correspond to $\tau = r/(x + y + z) = 28/195$. The 8 points on the corresponding elliptic curve above $[\tau : 1] = [28 : 195]$ generate a group of rank 4. This yields relatively many points of relatively low height. As in the proof of Proposition 4.3.9 we can take any n points on the real connected component that does not contain $\mathcal{O}$ and scale them to have the same perimeter and area. This is how we found the values in Table 4.1.

4.4 Computing the Néron-Severi group and the Mordell-Weil group

As in Section 2.6, in this section also all cohomology is étale cohomology, so we often will leave out the subscript ét. We consider the elliptic surface $Y \to C$ of the previous section over the algebraic closure and let $\overline{Y}$ and $\overline{C}$ denote $Y_{\overline{\mathbb{Q}}}$ and $C_{\overline{\mathbb{Q}}}$ respectively. Set $L = k(\overline{C}) \cong \overline{\mathbb{Q}}(s) \supset \mathbb{Q}(s) = k(C) = K$ and recall that we have encountered several points of $E(L)$, such as $P = \widetilde{M_1}$, the point Q from Theorem 4.3.6, and R induced by the closed immersion $C \to \widetilde{X}$. By Theorem 4.3.6 and Proposition 4.3.8 the points Q and R both have infinite order in $E(L)$. Suppose there are integers m, n such that $mQ + nR = 0$. Since complex conjugation sends Q and R to $-Q$ and R respectively, we find that also $-mQ + nR = 0$, whence $2mQ = 2nR = 0$. Therefore $m = n = 0$, so Q and R are linearly independent, and P, Q, and R generate a group isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}/3\mathbb{Z}$. We will show that this is the full Mordell-Weil group $E(L)$.

Proposition 4.4.1 *The surface $\overline{Y}$ is a K3 surface. Its Néron-Severi lattice has rank 18. The rank of the Mordell-Weil group $\overline{Y}(\overline{C}) \cong E(L)$ equals 2.*

Proof. To prove that $\overline{Y}$ is a K3 surface, it suffices by definition to show that we have $\dim H^1(\overline{Y}, \mathcal{O}_{\overline{Y}}) = 0$ and that any canonical divisor $K_{\overline{Y}}$ is linearly equivalent to 0.

By Theorem 2.4.24 we get $\operatorname{Pic}^0 \overline{Y} \cong \operatorname{Pic}^0 \overline{C} = 0$, as C is isomorphic to $\mathbb{P}^1$. We conclude that $\mathrm{NS}(\overline{Y}) \cong \operatorname{Pic}(\overline{Y})$, so algebraic and numerical equivalence on $\overline{Y}$ coincide with linear equivalence. As $\widetilde{X}$ is rational, we have $\chi(\mathcal{O}_{\widetilde{X}}) = \chi(\mathcal{O}_{\mathbb{P}^2}) = 1$, see [Ha2], Cor. V.5.6. By Proposition 2.5.15 we get $\chi(\mathcal{O}_{\overline{Y}}) = (\deg \widetilde{f}|_C) \cdot \chi(\mathcal{O}_{\widetilde{X}_{\overline{\mathbb{Q}}}}) = 2$. From Theorem 2.3.10 we then find that $K_{\overline{Y}} = 0$ in $\operatorname{Pic} \overline{Y}$. Hence, the canonical sheaf $\omega_{\overline{Y}}$ is isomorphic to $\mathcal{O}_{\overline{Y}}$. We find from Serre duality that $H^2(\overline{Y}, \mathcal{O}_{\overline{Y}}) \cong H^0(\overline{Y}, \omega_{\overline{Y}}) \cong H^0(\overline{Y}, \mathcal{O}_{\overline{Y}})$. Since $\overline{Y}$ is connected and projective, we get $\dim H^2(\overline{Y}, \mathcal{O}_{\overline{Y}}) = \dim H^0(\overline{Y}, \mathcal{O}_{\overline{Y}}) = 1$. Therefore, we get

$$\dim H^1(\overline{Y}, \mathcal{O}_{\overline{Y}}) = \dim H^0(\overline{Y}, \mathcal{O}_{\overline{Y}}) + \dim H^2(\overline{Y}, \mathcal{O}_{\overline{Y}}) - \chi(\mathcal{O}_{\overline{Y}}) = 1 + 1 - 2 = 0.$$

As seen in the proof of Proposition 2.5.15, the singular fibers of g come in pairs of copies of a singular fiber of $\widetilde{f}$. Hence, from Remark 4.3.2 and Theorem 2.4.32 we find $\rho = 2 + 2\left((6-1) + (3-1) + (1-1) + (1-1)\right) + \operatorname{rk} E(L) = 16 + \operatorname{rk} E(L)$ with $\rho = \operatorname{rk} NS(\overline{Y})$. Since Q and R are linearly independent, we have $\operatorname{rk} E(L) \geq 2$, so we get $\rho \geq 18$.

We will show $\rho \leq 18$ by reduction modulo a prime of good reduction. Take $p = 11$ and let $A = \mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ at p with residue field $k = A/p \cong \mathbb{F}_p$. Let $\mathfrak{X}$ be the closed subscheme of $\mathbb{P}^3_A$ given by $r^2(x+y+z) = xyz$ and $\mathfrak{f}\colon \mathfrak{X} \dashrightarrow \mathbb{P}^1_A$ the rational map that sends $[r : x : y : z]$ to $[r : x + y + z]$.

As $\mathfrak{X}$ is projective and $\mathfrak{X}_{\mathbb{Q}} \cong X$, there are A-points $\mathfrak{M}_i$ and $\mathfrak{N}_i$ on $\mathfrak{X}$ such that $(\mathfrak{N}_i)_{\mathbb{Q}} = N_i$ and $(\mathfrak{M}_i)_{\mathbb{Q}} = M_i$. Let $\pi' \colon \widetilde{\mathfrak{X}} \to \mathfrak{X}$ be the blow-up at the 6 points $\mathfrak{N}_i$ and $\mathfrak{M}_i$, and let $\widetilde{\mathfrak{f}}\colon \widetilde{\mathfrak{X}} \to \mathbb{P}^1_A$ be the morphism induced by the composition $\mathfrak{f} \circ \pi'$. Let $\mathfrak{C} \subset \widetilde{\mathfrak{X}}$ be the strict transform of the curve in $\mathfrak{X}$ parametrized by

$$[r : x : y : z] = [s - 1 : s + 1 : s - 1 : s(s-1)].$$

Let $\mathfrak{Y}$ denote the fibered product $\mathfrak{Y} = \mathfrak{C} \times_{\mathbb{P}^1_A} \widetilde{\mathfrak{X}}$, and let $\mathfrak{g}$ denote the projection $\mathfrak{Y} \to \mathfrak{C}$. Then $\mathfrak{Y}$ is a model of Y over A, i.e., $\mathfrak{Y}_{\mathbb{Q}} \cong Y$. Note that $\overline{Y} \cong \mathfrak{Y}_{\overline{\mathbb{Q}}}$. Set $\widetilde{Y} = \mathfrak{Y}_{\overline{k}}$ and $\widetilde{C} = \mathfrak{C}_{\overline{k}}$. The following diagram shows how the base changes of $\mathfrak{Y}$ that we will deal with are related. A similar diagram holds for $\mathfrak{C}$.

$$\begin{tikzcd}
\overline{Y} \arrow[d, "\cong"'] & Y \arrow[d, "\cong"'] & & & \widetilde{Y} \arrow[d, "\cong"'] \\
\mathfrak{Y}_{\overline{Q}} \arrow[r] \arrow[d] & \mathfrak{Y}_{\mathbb{Q}} \arrow[r] \arrow[d] & \mathfrak{Y} \arrow[d] & \mathfrak{Y}_k \arrow[l] \arrow[d] & \mathfrak{Y}_{\overline{k}} \arrow[l] \arrow[d] \\
\operatorname{Spec}\overline{\mathbb{Q}} \arrow[r] & \operatorname{Spec}\mathbb{Q} \arrow[r] & \operatorname{Spec}A & \operatorname{Spec}k \arrow[l] & \operatorname{Spec}\overline{k} \arrow[l]
\end{tikzcd}$$

We will show that $\mathfrak{Y}$ is smooth over $\operatorname{Spec} A$. Note that for each of the $\mathfrak{N}_i$ and $\mathfrak{M}_i$ there is an affine neighborhood $U = \operatorname{Spec} S \subset \mathfrak{X}$ for some A-algebra S, on which that point corresponds to an ideal $I \subset S$ satisfying $pS \cap I^n = pI^n$. Set $T = S \otimes_A k \cong S/pS$ and $J = IT$. Then $U_k = \operatorname{Spec} T$ and we have

$$I^n \otimes_A k \cong I^n/pI^n \cong I^n/(pS \cap I^n) \cong I^n \cdot S/pS \cong I^n T = J^n.$$

This implies

$$\operatorname{Proj}\left(T \oplus J \oplus J^2 \oplus \ldots\right) \cong \operatorname{Proj}\left(S \oplus I \oplus I^2 \oplus \ldots\right) \times_{\operatorname{Spec} A} \operatorname{Spec} k,$$

which tells us that the blow-up of the reduction $\mathfrak{X}_k$ at the points $(\mathfrak{M}_i)_k$ and $(\mathfrak{N}_i)_k$ is isomorphic to $\widetilde{\mathfrak{X}} \times_A k$, i.e., the reduction $\widetilde{\mathfrak{X}}_k$ of $\widetilde{\mathfrak{X}}$.

One easily checks that $\mathfrak{X}_k$ is geometrically regular outside the three ordinary double points $(\mathfrak{M}_i)_k$. Hence, this blow-up of $\mathfrak{X}_k$ at the points $(\mathfrak{M}_i)_k$ and $(\mathfrak{N}_i)_k$ is smooth over k, see [Ha2], exc. I.5.7. Thus $\widetilde{\mathfrak{X}}_k$ is smooth over k. As the morphism $\mathfrak{C}_k \to \mathbb{P}^1_k$ is unramified at the points of $\mathbb{P}^1_k$ where $\widetilde{\mathfrak{f}}_k$ has singular fibers (as is easily checked), $\mathfrak{Y}_k$ is smooth over k as well (cf. Proposition 2.5.15). Since the other fiber $\mathfrak{Y}_{\mathbb{Q}} \cong Y$ of $\mathfrak{Y} \to \operatorname{Spec} A$ is also smooth over its ground field $\mathbb{Q}$, we conclude that $\mathfrak{Y}$ is smooth over $\operatorname{Spec} A$ (cf. Remark 2.3.12).

Let $\varphi\colon \mathfrak{Y}_k \to \mathfrak{Y}_k$ denote the absolute Frobenius of $\mathfrak{Y}_k$ as in Section 2.6. Let φ_i^* denote the induced automorphism on $H^i(\widetilde{Y}, \mathbb{Q}_l)$. By Corollary 2.6.4 the Picard number ρ is bounded from above by the number of eigenvalues λ of φ_2^* for which λ/p is a root of unity. We will count these eigenvalues using the Lefschetz trace formula and the Weil conjectures. The characteristic polynomial of $(\varphi_i^*)^n$ acting on $H^i(\widetilde{Y}, \mathbb{Q}_l)$ is

$$P_i(t) = \det\left(t \cdot \operatorname{Id} - (\varphi_i^*)^n\right) = \prod_{i=1}^{b_i}(t - \alpha_{ij}).$$

By the Weil conjectures, $P_i(t)$ is a rational polynomial and the roots have absolute value $|\alpha_{ij}| = p^{ni/2}$, see [De], Thm. 1.6.

By Lemma 2.6.1 we have $\dim H^i(\overline{Y}, \mathbb{Q}_l) = \dim H^i(\widetilde{Y}, \mathbb{Q}_l)$ for $0 \le i \le 4$. Since $\overline{Y}$ is a K3 surface, the Betti numbers equal $\dim H^i(\widetilde{Y}, \mathbb{Q}_l) = b_i = 1, 0, 22, 0, 1$ for $i = 0, 1, 2, 3, 4$ respectively. Therefore, from the Weil conjectures we find $P_i(t) = 1 - t, 1, 1, 1 -$

n	1	2	3
$\mathrm{Tr}(\varphi_0^*)^n$	1	1	1
$\mathrm{Tr}(\varphi_1^*)^n$	0	0	0
$\mathrm{Tr}(\varphi_3^*)^n$	0	0	0
$\mathrm{Tr}(\varphi_4^*)^n$	p^2	p^4	p^6
$\#\mathfrak{Y}_k(\mathbb{F}_{p^n})$	298	16908	1792858
$\mathrm{Tr}(\varphi_2^*)^n$	176	2266	21296
$\mathrm{Tr}(\varphi_2^*)^n\vert V$	$16p$	$18p^2$	$16p^3$
$\mathrm{Tr}(\varphi_{2,W}^*)^n$	0	88	0

Table 4.2: computing $\mathrm{Tr}(\varphi_{2,W}^*)^n$

p^2t for $i = 0, 1, 3, 4$ respectively, whence $\mathrm{Tr}\,\varphi_i^* = 1, 0, 0, p^2$ for $i = 0, 1, 3, 4$. Similarly, we get $\mathrm{Tr}(\varphi_i^*)^n = 1, 0, 0, p^{2n}$ for $i = 0, 1, 3, 4$ and $n \geq 1$. That means that for any $n \geq 1$, if we know the number of $\mathbb{F}_{p^n}$-points of $\mathfrak{Y}_k$, then from the Lefschetz Trace Formula (see [Mi2], Thm. VI.12.3)

$$\#\mathfrak{Y}_k(\mathbb{F}_{p^n}) = \sum_{i=0}^{4} (-1)^i \,\mathrm{Tr}\left((\varphi_i^*)^n\right)$$

we can compute $\mathrm{Tr}(\varphi_2^*)^n$.

Let V denote the image in $H^2(\widetilde{Y}, \mathbb{Q}_l)$ under the composed map in (2.12) of the 18-dimensional subspace of $\mathrm{NS}(\overline{Y}) \otimes \mathbb{Q}_l$ that we already know, i.e., generated by the irreducible components of the singular fibers of g and the sections $\mathcal{O}$, Q, and R.

All these generators of V are defined over the $k = \mathbb{F}_p$, except for the image of Q, which is defined over $\mathbb{F}_{p^2}$. In the Mordell-Weil group modulo torsion $\widetilde{Y}(\widetilde{C})/\widetilde{Y}(\widetilde{C})_{\mathrm{tors}}$ we have $\varphi(Q) = -Q$. Hence V is φ_2^*-invariant and we find that $\mathrm{Tr}(\varphi_2^*)^n|V = 17p^n + (-1)^n p^n$.

Set $W = H^2(\widetilde{Y}, \mathbb{Q}_l)/V$ and let $\varphi_{2,W}^*$ denote the automorphism on W induced by φ_2^*. Then W has dimension 4 and from just linear algebra we get

$$\mathrm{char}(\varphi_2^*) = \mathrm{char}(\varphi_2^*|V) \cdot \mathrm{char}(\varphi_{2,W}^*) \tag{4.8}$$

and

$$\mathrm{Tr}(\varphi_2^*)^n = \mathrm{Tr}(\varphi_2^*)^n|V + \mathrm{Tr}(\varphi_{2,W}^*)^n.$$

This last equality allows us to compute $\mathrm{Tr}(\varphi_{2,W}^*)^n$ for $n \geq 1$, which is done for $n = 1, 2, 3$ in Table 4.2.

We computed the number of points on $\mathfrak{Y}_k(\mathbb{F}_{p^n})$ as follows. As $\mathfrak{Y}_k$ has the structure of elliptic surface over $\mathfrak{C}_k$, we can let the computer package Magma compute the number of points above every point of $\mathfrak{C}_k(\mathbb{F}_{p^n})$ with a nonsingular elliptic fiber. Adding to that the contribution of the singular fibers gives the total number of points.

For any linear operator T on an m-dimensional vector space with characteristic polynomial

$$\mathrm{char}\,T = X^m + c_1 X^{m-1} + c_2 X^{m-2} + \ldots + c_{m-1} X + c_m,$$

we have $c_1 = -t_1$, $c_2 = \frac{1}{2}(t_1^2 - t_2)$, and $c_3 = -\frac{1}{6}(t_1^3 + 2t_3 - 3t_1t_2)$ with $t_n = \operatorname{Tr} T^n$. From this and Table 4.2 we find that the characteristic polynomial of $\varphi_{2,W}^*$ equals $h = X^4 - 44X^2 + c_4$ for some c_4. By the Weil conjectures, and (4.8), the roots of h have absolute value p and their product c_4 is rational, so $c_4 = \pm p^4$. As not all roots of $X^4 - 44X^2 - 11^4$ have absolute value 11, we get $h = X^4 - 44X^2 + 11^4$. If α is a root of h then $\beta = (\alpha/p)^2$ satisfies $11\beta^2 - 4\beta + 11 = 0$. As the only quadratic roots of unity are $\pm\sqrt{-1}$ and ζ_6^i, we find that β is not a root of unity, and thus neither is α/p. From (4.8) it follows that α/p is a root of unity for at most $22 - 4 = 18$ roots α of $\operatorname{char}(\varphi_2^*)$. From Corollary 2.6.4 we find $\rho \leq 18$. □

Corollary 4.4.2 *The Mordell-Weil group $E(L)$ is generated by P, Q, and R and is isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}/3\mathbb{Z}$.*

Proof. As $\overline{Y} \to \overline{C}$ is a relatively minimal fibration and $\overline{Y}$ is regular and projective, the Néron model of $\overline{Y}/\overline{C}$ is obtained from $\overline{Y}$ by deleting the singular points of the singular fibers, see [Si2], Thm. IV.6.1, and [BLR], § 1.5, Prop. 1. Note that at $\sigma = 0$ and $\sigma = -1$ we have additive reduction (type IV), whence the identity component of the reduction has no torsion. Since we are in characteristic 0, the kernel of reduction $E_1(L)$ has no torsion either, see [Si1], Prop. VII.3.1. It follows that the group $E_0(L)$ of nonsingular reduction has no torsion, see [Si2], Rem. IV.9.2.2. By the classification of singular fibers we find that $E(L)/E_0(L)$ has order at most 3, see [Si2], Cor. IV.9.2 and Tate's Algorithm IV.9.4. We conclude that $E(L)_{\mathrm{tors}}$ has order 3 and is generated by P.

With Shioda's explicit formula for the Mordell-Weil pairing ([Shi3], Thm. 8.6), we find $\langle Q, R\rangle = 0$ and $\langle Q, Q\rangle = \langle R, R\rangle = 1$. Hence, as seen before, Q and R are linearly independent. As the rank $\operatorname{rk} E(L)$ equals 2 by Proposition 4.4.1, the group generated by Q and R has finite index in the Mordell-Weil lattice $E(L)/E(L)_{\mathrm{tors}}$. If the Mordell-Weil lattice were not generated by Q and R, then it would contain a nonzero element $S = aQ + bR$ with $a, b \in \mathbb{Q}$ and $-\frac{1}{2} < a, b \leq \frac{1}{2}$, so that $\langle S, S\rangle = a^2 + b^2 \leq \frac{1}{2}$. The types of singular fibers are I_1, I_6, and IV by Remark 4.3.2). From Table 2.2 we find that the number of simple irreducible components in these singular fibers are 1, 6, and 3 respectively. It follows from Proposition 2.4.38 that the values of the Mordell-Weil pairing are contained in $\frac{1}{m}\mathbb{Z}$ with $m = \operatorname{lcm}\{1, 6, 3\} = 6$. As for any rational a, b the 3-adic valuation of $a^2 + b^2$ is even, we conclude that in fact we have $\langle S, S\rangle \in \frac{1}{2}\mathbb{Z}$, so that $a^2 + b^2 \geq \frac{1}{2}$. Thus, we find $a^2 + b^2 = \frac{1}{2}$, whence $a = b = \frac{1}{2}$. Therefore, $2S = Q + R + \varepsilon P$ for some $\varepsilon \in \{0, 1, 2\}$. After adding εP to S if necessary, we may assume $\varepsilon = 0$ without loss of generality.

It suffices to check $Q + R \notin 2E(K)$. Let (p_S, q_S), (p_{2S}, q_{2S}), and (p_{Q+R}, q_{Q+R}) denote the Weierstrass coordinates of S, $2S$, and $Q + R$ respectively. Using addition formulas, we can compute $p_{Q+R} \in \mathbb{Q}(i)(s)$ explicitly and express p_{2S} in terms of p_S. Let u be defined by $p_S - 4(s-1)^2 = 2(s-1)u$. Then in terms of u, the equation $p_{2S} = p_{Q+R}$ simplifies to

$$\begin{aligned} &u^4 + 4(s-1)(s+1)(s+i)u^3 + 2(s^2 + (1+i)s - 2 + i)s^2(s+1)^2u^2 + \\ &\quad 8(s^2 + (1+i)s - 2 + i)(s-1)s^2(s+1)^2u + 8(s+i)s^2(s-1)^2(s+1)^3 = 0 \end{aligned} \tag{4.9}$$

By Gauss's Theorem any root $u \in L = \overline{\mathbb{Q}}(s)$ of this equation is contained in $\overline{\mathbb{Q}}[s]$ and divides the constant term $8(s+i)s^2(s-1)^2(s+1)^3$. Hence, any root u is of the form

$$u = cs^k(s+1)^l(s-1)^m(s+i)^n,$$

for some constant c and exponents k, l, m, and n. Considering the four Newton polygons, we find $k = 0$, $l = 1$, and $m, n \in \{0, 1\}$. One easily checks that for none of the four possibilities for m, n there is a c such that (4.9) is satisfied. □

Corollary 4.4.3 *The discriminant of the Néron-Severi lattice* $\mathrm{NS}(\overline{Y})$ *equals* -36*.*

Proof. From Lemma 2.4.37, we find the following equation, relating the discriminant of the Néron-Severi lattice to that of the Mordell-Weil lattice.

$$|\operatorname{disc} \mathrm{NS}(\overline{Y})| = \frac{\operatorname{disc} E(L)/E(L)_{\mathrm{tors}} \cdot \prod m_v^{(1)}}{|E(L)_{\mathrm{tors}}|^2}$$

Here $m_v^{(1)}$ is the number of irreducible components of multiplicity 1 of the fiber of g above $v \in C$. In the proof of Corollary 4.4.2 we have seen that $\operatorname{disc} E(L)/E(L)_{\mathrm{tors}} = 1$, so we get

$$|\operatorname{disc} \mathrm{NS}(\overline{Y})| = \frac{1 \cdot 6 \cdot 6 \cdot 3 \cdot 3}{3^2} = 36.$$

By the Hodge index Theorem $\operatorname{disc} \mathrm{NS}(\overline{Y})$ is negative, so we get $\operatorname{disc} \mathrm{NS}(\overline{Y}) = -36$. □

Chapter 5

K3 surfaces with Picard number one and infinitely many rational points

5.1 Introduction

In the previous two chapters we solved two Diophantine open problems by showing that the rational points on a certain K3 surface are Zariski dense. In general, little is known about the arithmetic of K3 surfaces. It is for instance an open question if there exists a K3 surface X over a number field K such that the set $X(K)$ of rational points is neither empty, nor dense. The K3 surfaces we analyzed in the previous chapters have an elliptic fibration and relatively high geometric Picard numbers 18 and 20. The density of rational points on these surfaces is consistent with a theorem of Bogomolov and Tschinkel that was already mentioned in the introduction of chapter 3. Recall that if X is a variety over a number field K, then we say that the rational points on X are potentially dense if there exists a finite field extension L of K such that the set $X(L)$ of L-rational points is Zariski dense in X. Bogomolov and Tschinkel proved that if the geometric Picard number of a K3 surface X over a number field is at least 2, then in most cases the rational points on X are potentially dense, see [BT]. However, it is not yet known whether there exists a K3 surface over a number field and with geometric Picard number 1 on which the rational points are potentially dense. Neither do we know if there exists a K3 surface over a number field and with geometric Picard number 1 on which the rational points are *not* potentially dense.

In December 2002, at the AIM workshop on rational and integral points on higher-dimensional varieties in Palo Alto, Swinnerton-Dyer and Poonen asked a related question. They asked whether there exists a K3 surface over a number field and with Picard number 1 that contains infinitely many rational points. In this chapter we will show that such K3 surfaces do indeed exist. The main theorem of this chapter states something stronger. A polarization of a K3 surface X is a choice of an ample divisor H

on X. The degree of such a polarization is H^2. A K3 surface polarized by a very ample divisor of degree 4 is a smooth quartic surface in $\mathbb{P}^3$.

Theorem 5.1.1 *In the moduli space of K3 surfaces polarized by a very ample divisor of degree* 4*, the set of surfaces defined over* $\mathbb{Q}$ *with geometric Picard number* 1 *and infinitely many rational points is dense in both the Zariski topology and the real analytic topology.*

We will prove this theorem by exhibiting an explicit family of quartic surfaces in $\mathbb{P}^3_{\mathbb{Q}}$ with geometric Picard number 1 and infinitely many rational points. Proving that these surfaces contain infinitely many rational points is the easy part. It is much harder to prove that the geometric Picard number of these surfaces equals 1. It has been known since Noether that a general hypersurface in $\mathbb{P}^3_{\mathbb{C}}$ of degree at least 4 has geometric Picard number 1. A modern proof of this fact was given by Deligne, see [SGA 7 II], Thm. XIX.1.2. Despite this fact, it has been an old challenge, attributed to Mumford, to find even just one explicit quartic surface, defined over a number field, whose geometric Picard number equals 1. Deligne's result does not imply that such surfaces exist, as "general" means "up to a countable union of closed subsets of the moduli space." A priori, this could exclude all surfaces defined over $\overline{\mathbb{Q}}$! Terasoma and Ellenberg have proven independently that such surfaces do exist. The following theorems state their results.

Theorem 5.1.2 (Terasoma, 1985) *For any given positive integers* $(n; a_1, \ldots, a_d)$ *not equal to* $(2; 3)$, $(n; 2)$, *or* $(n; 2, 2)$, *and with* n *even, there is a smooth complete intersection* X *over* $\mathbb{Q}$ *of dimension* n *defined by equations of degrees* $a_1, \ldots, a_d$ *such that the middle geometric Picard number of* X *is* 1*.*

Proof. See [Te]. □

Theorem 5.1.3 (Ellenberg, 2004) *For every even integer* d *there exists a number field* K *and a polarized K3 surface* X/K *of degree* d*, with geometric Picard number* 1*.*

Proof. See [Ell]. □

The proofs of Terasoma and Ellenberg are ineffective in the sense that they do not give explicit examples. In principle it might be possible to extend their methods to test whether a given explicit K3 surface has geometric Picard number 1. In practice however, it is an understatement to say that the amount of work involved is not encouraging.

Shioda has found explicit examples of surfaces with geometric Picard number 1. In fact, he has shown that for every prime $m \geq 5$ the surface in $\mathbb{P}^3$ given by

$$w^m + xy^{m-1} + yz^{m-1} + zx^{m-1} = 0$$

has geometric Picard number 1, see [Shi2]. However, for $m = 4$ this equation determines a K3 surface with geometric Picard number 20, i.e., a singular K3 surface.

In the next section we will prove the main theorem of this chapter. Having explicit examples of K3 surfaces with geometric Picard number 1, we can use a computer search to look into the distribution of rational points on such surfaces. This is what section 5.3 is devoted to.

The results of this chapter have been combined into a preprint, see [VL3].

5.2 Proof of the main theorem

First we will give a family of smooth quartic surfaces in $\mathbb{P}^3$ with Picard number 1. Let $R = \mathbb{Z}[x, y, z, w]$ be the homogeneous coordinate ring of $\mathbb{P}^3_{\mathbb{Z}}$. Throughout the rest of this chapter, for any homogeneous polynomial $h \in R$ of degree 4, let $\mathfrak{X}_h$ denote the scheme in $\mathbb{P}^3_{\mathbb{Z}}$ given by

$$wf + 2zg = 3pq + 6h, \tag{5.1}$$

with $f, g, p, q \in R$ equal to

$$\begin{aligned} f &= x^3 - x^2y - x^2z + x^2w - xy^2 - xyz + 2xyw + xz^2 + 2xzw + y^3 + \\ &\quad + y^2z - y^2w + yz^2 + yzw - yw^2 + z^2w + zw^2 + 2w^3, \\ g &= xy^2 + xyz - xz^2 - yz^2 + z^3, \\ p &= z^2 + xy + yz, \\ q &= z^2 + xy. \end{aligned}$$

Its base extensions to $\mathbb{Q}$ and $\overline{\mathbb{Q}}$ are denoted X_h and $\overline{X}_h$ respectively. We will use the following lemma.

Lemma 5.2.1 *Let V be a vector space of dimension n and T a linear operator on V. Let t_i denote the trace of T^i. Then the characteristic polynomial of T is equal to*

$$f_T(x) = \det(x \cdot \mathrm{Id} - T) = x^n + c_1x^{n-1} + c_2x^{n-2} + \ldots + c_n,$$

with the c_i given recursively by

$$c_1 = -t_1 \qquad \textit{and} \qquad -kc_k = t_k + \sum_{i=1}^{k-1} c_it_{k-i}.$$

Proof. Let the eigenvalues be denoted by $x_1, \ldots, x_n$. For fixed k, set

$$a_i = (-1)^i \sum x_m^{k-i} \prod_{j \in J} x_j,$$

where the sum ranges over the set

$$\{(m, J) \mid J \subset \{1, \ldots, n\},\ \#J = i,\ m \in \{1, \ldots, n\} \setminus J\}.$$

As $(-1)^ic_i$ is the i-th symmetric function in the x_j, one checks that $c_it_{k-i} = a_i - a_{i-1}$. Together with the identities $a_0 = t_k$ and $a_{k-1} = -kc_k$ this implies the lemma. $\square$

Theorem 5.2.2 *For any $h \in R$ the quartic surface X_h is smooth over $\mathbb{Q}$ and has geometric Picard number* 1*. The Picard group* $\operatorname{Pic} X_h$ *is generated by a hyperplane section.*

Proof. For $p = 2, 3$, let $X_p/\mathbb{F}_p$ denote the fiber of $\mathfrak{X}_h \to \operatorname{Spec} \mathbb{Z}$ over p. As they are independent of h, one easily checks that X_p is smooth over $\mathbb{F}_p$ for $p = 2, 3$. As the morphism $\mathfrak{X}_h \to \operatorname{Spec} \mathbb{Z}$ is flat and projective, it follows that the generic fiber X_h of $\mathfrak{X}_h \to \operatorname{Spec} \mathbb{Z}$ is smooth over $\mathbb{Q}$ as well, cf. [Ha2], exc. III.10.2.

We will first show that X_2 and X_3 have geometric Picard number 2. For $p = 2, 3$, let Φ_p denote the absolute Frobenius of X_p. Set $\overline{X}_p = X_p \times \overline{\mathbb{F}}_p$ and let $\Phi_p^*(i)$ denote the automorphism on $H^i_{\text{ét}}(\overline{X}_p, \mathbb{Q}_l)$ induced by $\Phi_p \times 1$ acting on $\overline{X}_p = X_p \times_{\mathbb{F}_p} \overline{\mathbb{F}}_p$. Then by Corollary 2.6.4 the geometric Picard number of X_p is bounded from above by the number of eigenvalues λ of $\Phi_p^*(2)$ for which λ/p is a root of unity. We will find the characteristic polynomial of $\Phi_p^*(2)$ from the traces of its powers. These traces we will compute with the Lefschetz formula

$$\#X_p(\mathbb{F}_{p^n}) = \sum_{i=0}^{4} (-1)^i \operatorname{Tr}(\Phi_p^*(i)^n). \tag{5.2}$$

As X_p is a smooth hypersurface in $\mathbb{P}^3$ of degree 4, it is a K3 surface and its Betti numbers are $b_0 = 1$, $b_1 = 0$, $b_2 = 22$, $b_3 = 0$, and $b_4 = 1$. It follows that $\operatorname{Tr}(\Phi_p^*(i)^n) = 0$ for $i = 1, 3$, and for $i = 0$ and $i = 4$ the automorphism $\Phi_p^*(i)^n$ has only one eigenvalue, which by the Weil conjectures equals 1 and p^{2n} respectively. From the Lefschetz formula (5.2) we conclude $\operatorname{Tr}(\Phi_p^*(2)^n) = \#X_p(\mathbb{F}_{p^n}) - p^{2n} - 1$. After counting points on X_p over $\mathbb{F}_{p^n}$ for $n = 1, \ldots, 11$, this allows us to compute the traces of the first 11 powers of $\Phi_p^*(2)$. With Lemma 5.2.1 we can then compute the first coefficients of the characteristic polynomial f_p of $\Phi_p^*(2)$. Writing $f_p = x^{22} + c_1 x^{21} + \ldots + c_{22}$ we find

p	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}
2	-3	-2	12	0	-32	64	-128	128	256	0	-2048
3	-5	-6	72	27	-891	0	9477	-4374	-78732	19683	708588

The Weil conjectures give a functional equation $p^{22} f_p(x) = \pm x^{22} f_p(p^2/x)$. As in our case (both for $p = 2$ and $p = 3$) the middle coefficient c_{11} of f_p is nonzero, the sign of the functional equation is positive. This allows us to compute the remaining coefficients of f_p. If λ is a root of f_p then λ/p is a root of $\widetilde{f}_p(x) = p^{-22} f_p(px)$. Hence, the number of roots of $\widetilde{f}_p(x)$ that are also a root of unity gives an upper bound for the geometric Picard number of X_p. After factorization into irreducible factors, we find

$$\begin{aligned}
\widetilde{f}_2 = & \frac{1}{2}(x-1)^2 \big(2x^{20} + x^{19} - x^{18} + x^{16} + x^{14} + x^{11} + \\
& \qquad\qquad + 2x^{10} + x^9 + x^6 + x^4 - x^2 + x + 2\big) \\
\widetilde{f}_3 = & \frac{1}{3}(x-1)^2 \big(3x^{20} + x^{19} - 3x^{18} + x^{17} + 6x^{16} - 6x^{14} + x^{13} + 6x^{12} - x^{11} + \\
& \qquad\qquad -7x^{10} - x^9 + 6x^8 + x^7 - 6x^6 + 6x^4 + x^3 - 3x^2 + x + 3\big)
\end{aligned}$$

Neither for $p = 2$ nor for $p = 3$ the roots of the irreducible factor of $\widetilde{f}_p$ of degree 20 are integral. Therefore these roots are not roots of unity and we conclude that $\widetilde{f}_p$ has two roots that are roots of unity, counted with multiplicities. By Corollary 2.6.4 this implies that the geometric Picard number of X_p is at most 2.

Note that besides the hyperplane section H, the surface X_2 also contains the conic C given by $w = z^2 + xy = 0$. We have $H^2 = \deg X_2 = 4$ and $H \cdot C = \deg C = 2$. As the genus $g(C)$ of C equals 0 and the canonical divisor K on X_2 is trivial, the adjunction formula $2g(C) - 2 = C \cdot (C + K)$ yields $C^2 = -2$. Thus H and C generate a sublattice of $\mathrm{NS}(\overline{X}_2)$ of rank 2 with Gram matrix

$$\begin{pmatrix} 4 & 2 \\ 2 & -2 \end{pmatrix}.$$

We conclude that the inner product space $\mathrm{NS}(\overline{X}_2)_{\mathbb{Q}}$ has rank 2 and discriminant $-12 \in \mathbb{Q}^*/\mathbb{Q}^{*2}$, see Definition 2.1.10. Similarly, X_3 contains the line L given by $w = z = 0$. The hyperplane section on X_3 and L generate a sublattice of $\mathrm{NS}(\overline{X}_3)$ of rank 2 with Gram matrix

$$\begin{pmatrix} 4 & 1 \\ 1 & -2 \end{pmatrix}.$$

We conclude that the inner product space $\mathrm{NS}(\overline{X}_3)_{\mathbb{Q}}$ also has rank 2, and discriminant $-9 \in \mathbb{Q}^*/\mathbb{Q}^{*2}$.

Let ρ denote the geometric Picard number $\rho = \operatorname{rk} \mathrm{NS}(\overline{X}_h)$. It follows from Proposition 2.6.2 that there is an injection $\mathrm{NS}(\overline{X}_h)_{\mathbb{Q}} \hookrightarrow \mathrm{NS}(\overline{X}_p)_{\mathbb{Q}}$ of inner product spaces for $p = 2, 3$. Hence we get $\rho \leq 2$ and if we had equality, then both these injections would be isomorphisms and $\mathrm{NS}(\overline{X}_2)_{\mathbb{Q}}$ and $\mathrm{NS}(\overline{X}_3)_{\mathbb{Q}}$ would be isomorphic as inner product spaces. This is not the case because they have different discriminants. We conclude $\rho \leq 1$. As a hyperplane section H on X_h has selfintersection $H^2 = 4 \neq 0$, we find $\rho = 1$. Since $\mathrm{NS}(\overline{X}_h)$ is a 1-dimensional even lattice (see Lemma 2.2.26), the discriminant of $\mathrm{NS}(\overline{X}_h)$ is even. The sublattice of finite index in $\mathrm{NS}(\overline{X}_h)$ generated by H gives

$$4 = \operatorname{disc}\langle H \rangle = [\mathrm{NS}(\overline{X}_h) : \langle H \rangle]^2 \cdot \operatorname{disc} \mathrm{NS}(\overline{X}_h).$$

Together with $\operatorname{disc} \mathrm{NS}(\overline{X}_h)$ being even this implies $[\mathrm{NS}(\overline{X}_h) : \langle H \rangle] = 1$, so H generates $\mathrm{NS}(\overline{X}_h)$. $\square$

Remark 5.2.3 In the proof we counted points over $\mathbb{F}_{p^n}$ for $p = 2, 3$ and $n = 1, \ldots, 11$ in order to find the traces of powers of Frobenius up to the 11-th power. We could have got away with less counting. In both cases $p = 2$ and $p = 3$ we already know a 2-dimensional subspace W of $\mathrm{NS}(\overline{X}_p)_{\mathbb{Q}_l} \subset H^2(\overline{X}_p, \mathbb{Q}_l)(1)$, generated by the hyperplane section H and another divisor class. Therefore it suffices to find out the characteristic polynomial of

Frobenius acting on the quotient $V = H^2(\overline{X}_p, \mathbb{Q}_l)(1)/W$. This implies it suffices to know the traces of powers of Frobenius acting on V up to the 10-th power.

An extra trick was used for $p = 3$. The family of planes through the line L given by $w = z = 0$ cuts out a fibration of curves of genus 1. We can give all nonsingular fibers the structure of an elliptic curve by quickly looking for a point on it. There are efficient algorithms available in for instance MAGMA to count the number of points on these elliptic curves.

Using these few speed-ups we let a computer run for one night to compute the characteristic polynomial of several random surfaces given by an equation of the form (5.1). If the middle coefficient was zero, no more effort was spent on trying to find the sign of the functional equation (see proof of Theorem 5.2.2) and the surface was discarded. After one night two examples over $\mathbb{F}_3$ were found with geometric Picard number 2 and one example over $\mathbb{F}_2$. This allows us to construct two families of surfaces with geometric Picard number 1 with the Chinese Remainder Theorem. One of these families consists of the surfaces X_h. A program written in MAGMA that checks the characteristic polynomial of Frobenius on X_2 and X_3 is electronically available from the author upon request.

Remark 5.2.4 For $p = 2, 3$, let $A_p \subset \mathrm{NS}(\overline{X}_p)$ denote the lattice as described in the proof of Theorem 5.2.2, i.e., A_2 is generated by a hyperplane section and a conic, and A_3 is generated by a hyperplane section and a line. Then in fact A_p equals $\mathrm{NS}(\overline{X}_p)$ for $p = 2, 3$. Indeed, we have $\operatorname{disc} A_p = [\mathrm{NS}(\overline{X}_p) : A_p]^2 \cdot \operatorname{disc} \mathrm{NS}(\overline{X}_p)$. For $p = 2$ this implies $\operatorname{disc} \mathrm{NS}(\overline{X}_2) = -12$ or $\operatorname{disc} \mathrm{NS}(\overline{X}_2) = -3$. The latter is impossible because modulo 4 the discriminant of an even lattice of rank 2 is congruent to 0 or -1. We conclude $\operatorname{disc} \mathrm{NS}(\overline{X}_2) = -12$, and therefore $[\mathrm{NS}(\overline{X}_2) : A_2] = 1$, so $A_2 = \mathrm{NS}(\overline{X}_2)$.

For $p = 3$ we find $\operatorname{disc} \mathrm{NS}(\overline{X}_3) = -9$ or $\operatorname{disc} \mathrm{NS}(\overline{X}_3) = -1$. Suppose the latter equation held. By the classification of even unimodular lattices we find that $\operatorname{disc} \mathrm{NS}(\overline{X}_3)$ is isomorphic to the lattice with Gram matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

By a theorem of Van Geemen this is impossible, see [VG], 5.4. From this contradiction we conclude $\operatorname{disc} \mathrm{NS}(\overline{X}_3) = -9$ and thus $[\mathrm{NS}(\overline{X}_3) : A_3] = 1$, so $A_3 = \mathrm{NS}(\overline{X}_3)$. For a more concrete proof, note that the index $[\mathrm{NS}(\overline{X}_3) : A_3]$ divides 3. Suppose we had $A_3 \subsetneq \mathrm{NS}(\overline{X}_3)$. Then there is an element $D \in \mathrm{NS}(\overline{X}_3) \setminus A_3$ with $3D \in A_3$, say $3D = aH + bL$. After replacing D by $\varepsilon D + kH + lL$ for some integers k, l and $\varepsilon \in \{\pm 1\}$, we may assume $a \in \{0, 1\}$ and $b \in \{0, \pm 1\}$. From $9 | (3D)^2 = 4a^2 + 2ab - 2b^2$ we find $(a, b) = (1, -1)$. Since L is contained in a hyperplane, we find that $3D = H - L$ is effective. Set $\chi = \chi(\overline{X}_3, \mathcal{O}_{\overline{X}_3}) = 2$. Because the canonical sheaf $K_{\overline{X}_3}$ on $\overline{X}_3$ is trivial and we have $D^2 = 0$, the theorem of Riemann-Roch on surfaces yields $h^0(\overline{X}_3, \mathcal{L}(D)) - h^1(\overline{X}_3, \mathcal{L}(D)) + h^0(\overline{X}_3, \mathcal{L}(-D)) = \chi = 2 > 0$. This implies that D or $-D$ is effective. Since $3D = H - L$ is effective, the divisor $-D$ is not effective, so D is effective. Then from $\deg D = D \cdot H = 1$ we find that D is a line, and thus nonsingular with genus $g(D) = 0$.

This contradicts the adjunction formula $2g(D) - 2 = D \cdot (D + K_{\overline{X}_3}) = 0$, where the last equality follows from the fact that $K_{\overline{X}_3}$ is trivial and $D^2 = 0$.

Since there are $\binom{4+3}{3} = 35$ monomials of degree 4 in $\mathbb{Q}[x, y, z, w]$, the quartic surfaces in $\mathbb{P}^3_{\mathbb{Q}}$ are parametrized by the space $\mathbb{P}^{34}_{\mathbb{Q}}$, which we will denote by M. Let $M' \cong \mathbb{P}^{27} \subset M$ denote the subvariety of those surfaces X for which the coefficients of the monomials x^4, x^3y, x^3z, y^4, y^3x, y^3z, and x^2z^2 in the defining polynomial of X are all zero. Note that the vanishing of the coefficients of the first 6 of these monomials is equivalent to the tangency of the plane H_w given by $w = 0$ to the surface X at the points $P = [1 : 0 : 0 : 0]$ and $Q = [0 : 1 : 0 : 0]$. Thus, the vanishing of these coefficients yields a singularity at P and Q in the plane curve $C_X = H_w \cap X$. If the singularity at P in C_X is not worse than a double point, then the vanishing of the coefficient of x^2z^2 is equivalent to the fact that the line given by $y = w = 0$ is one of the limit-tangent lines to C_X at P.

Proposition 5.2.5 *There is a nonempty Zariski open subset $U \subset M'$ with $X_0 \in U$ such that every surface $X \in U$ defined over $\mathbb{Q}$ has infinitely many rational points.*

Proof. The singular $X \in M'$ form a closed subset of M'. So do the surfaces X for which the intersection $H_w \cap X$ has worse singularities than just two double points at P and Q. Leaving out these closed subsets we obtain an open subset V of M'. Let $X \in V$ be given. The plane quartic curve $C_X = X \cap H_w$ has two double points, so the geometric genus g of the normalization $\widetilde{C}_X$ of C_X equals $p_a - 2$, where p_a is the arithmetic genus of C_X, see [Ha2], exercise IV.1.8. As we have $p_a = \frac{1}{2}(4-1)(4-2) = 3$, we get $g = 1$. Now assume X is defined over $\mathbb{Q}$. One of the limit-tangents to C_X at P is given by $w = y = 0$. Its slope, being rational, corresponds to a rational point P' on $\widetilde{C}_X$ above P. Fixing this point as the unit element $\mathcal{O} = P'$, the curve $\widetilde{C}_X$ obtains the structure of an elliptic curve. Let $D \in \mathrm{Pic}^0(\widetilde{C}_X)$ be the pull back under normalization of the divisor $P - Q \in \mathrm{Pic}^0(C_X)$. By the theory of elliptic curves there is a unique point R on $\widetilde{C}_X$ (depending on X) such that D is linearly equivalent to $R - \mathcal{O}$, see [Si1], Prop. III.3.4. As D is defined over $\mathbb{Q}$, so is R. By Mazur's theorem (see [Si1], Thm. III.7.5 for statement, [Maz], Thm. 8 for a proof), the point R has finite order if and only if $mR = \mathcal{O}$ for some $m \in \{1, 2, \ldots, 10, 12\}$. Note that we have $\mathrm{lcm}(1, 2, \ldots, 10, 12) = 2520$. Take for U the complement in V of the closed subset of those X for which we have $2520R = \mathcal{O}$ for the corresponding point R on $\widetilde{C}_X$. Then each $X \in U$ contains an elliptic curve with infinitely many rational points. By choosing a Weierstrass equation, one verifies easily that if we take $X = X_h$ with $h = 0$, then the corresponding point R on $\widetilde{C}_X$ satisfies $mR \neq \mathcal{O}$ for $m \in \{1, 2, \ldots, 10, 12\}$. Therefore, we find $X_0 \in U$, so U is nonempty. $\square$

Remark 5.2.6 If $\widetilde{C}_X$ is the normalization of C_X as in the proof of Proposition 5.2.5, then generically there is another rational point P'' on $\widetilde{C}_X$ above P, besides P'. Generically this point also has infinite order and the Mordell-Weil rank of $\widetilde{C}_X$ is at least 2 with independent points P'' and R as in the proof of Proposition 5.2.5. For $X = X_h$ with

$h = 0$ the curve $\widetilde{C}_X$ is given by

$$3x^2y^2 + xy^2z + 4xyz^2 + 2xz^3 + 5yz^3 + z^4 = 0.$$

As the point $P = [1 : 0 : 0]$ is a cusp, there is only one point above P on $\widetilde{C}_X$ in this case. Both points on $\widetilde{C}_X$ above $Q = [0 : 1 : 0]$ are rational and we have an extra rational point $[1 : 1 : -1]$. These generate the full Mordell-Weil group of rank 3.

Lemma 5.2.7 *Let X be a variety over $\mathbb{Q}$ such that the set $X(\mathbb{R})$ of real points is Zariski dense in X. If a set $S \subset X(\mathbb{R})$ is dense in the real analytic topology, then S is dense in the Zariski topology.*

Proof. As this is a local question, we may assume X is affine, say $X = \operatorname{Spec} A$. Suppose there is a Zariski open U of X such that $U \cap S = \emptyset$. There is an element $f \in A$, such that the open subset $V(f) = \{x \in X \mid f(x) \neq 0\}$ is contained in U. By assumption, there is a point $x \in X(\mathbb{R}) \cap V(f)$. Let x be such a point. Then we have $f(x) \neq 0$, so in a small open neighborhood W of x in the real analytic topology we also have $f(y) \neq 0$ for all $y \in W$. This implies $W \subset V(f) \subset U$, so we also find $W \cap S = \emptyset$. This contradicts the assumption that S is dense in the real analytic topology. $\square$

From the local and global Torelli theorem for K3 surfaces, see [PS], one can find a very precise description of the moduli space of polarized K3 surfaces in general, see [Be]. A polarization of a K3 surface Z by a very ample divisor of degree 4 gives an embedding of Z as a smooth quartic surface in $\mathbb{P}^3$. An isomorphism between two smooth quartic surfaces in $\mathbb{P}^3$ that sends a hyperplane section to a hyperplane section comes from an automorphism of $\mathbb{P}^3$. We conclude that the moduli space of K3 surfaces polarized by a very ample divisor of degree 4 is isomorphic to the open subset in $M = \mathbb{P}^{34}$ of smooth quartic surfaces modulo the action of PGL(4) by linear transformations of $\mathbb{P}^3$. We are now ready to prove the main theorem of this chapter.

Proof of Theorem 5.1.1. By the description of the moduli space of K3 surfaces polarized by a very ample divisor of degree 4 given above, it suffices to prove that the set $S \subset M(\mathbb{Q})$ of those surfaces with geometric Picard number 1 and infinitely many rational points is dense in M. Let U be as in Proposition 5.2.5. We will first show that $S \cap U$ is dense in U. To show that $S \cap U$ is dense in U in the real analytic topology, consider any $X \in U(\mathbb{R})$, say with defining polynomial $F \in \mathbb{R}[x, y, z, w]$. We can approximate F with a polynomial $h' \in \mathbb{Q}[x, y, z, w]$, such that the surface defined by h' is also contained in U. After scaling we may assume h' has integral coefficients. By taking $h = Nh'$ for an arbitrarily large integer N, the surface X_h will be arbitrarily close to the surface defined by h' and hence close to the surface X defined by F. Checking the coefficients of the defining equation of X_h in (5.1) we see $X_h \in M'$. By choosing X_h close enough to X, we can ensure that X_h is contained in U, so X_h contains infinitely many rational points. By Theorem 5.2.2 the surface X_h has geometric Picard number 1. The fact that $S \cap U$ is dense in U in the Zariski topology follows from Lemma 5.2.7, as the set of real surfaces is Zariski dense in M'. As U is a dense open subset of M' (both in the Zariski and in the real analytic topology) it follows that $S \cap M'$ is dense in M'.

Let W denote the $\mathbb{Q}$-vector space of 4×4-matrices and let T denote the dense open subset of $\mathbb{P}(W)$ corresponding to elements of $\mathrm{PGL}(4)$. Let $\varphi\colon T \times M' \to M$ be given by sending (A, X) to $A(X)$. Note that $T \times (S \cap M')$ is dense in $T \times M'$ and φ sends $T(\mathbb{Q}) \times S$ to S. Hence, in order to prove that S is dense in M, it suffices to show that φ is dominant, which can be checked after extending to the algebraic closure. A general quartic surface in $\mathbb{P}^3$ has a one-dimensional family of bitangent planes, i.e., planes that are tangent at two different points. This is closely related to the theorem of Bogomolov and Mumford, see the appendix to [MM]. In fact, for a general quartic surface $Y \subset \mathbb{P}^3$, there is such a bitangent plane H, such that the two tangent points are ordinary double points in the intersection $H \cap Y$. Let Y be such a quartic surface and H such a plane, say tangent at P and Q. Then there is a linear transformation that sends H, P, and Q to the plane given by $w = 0$, and the points $[1 : 0 : 0 : 0]$ and $[0 : 1 : 0 : 0]$. Also, one of the limit-tangent lines to the curve $Y \cap H$ at the singular point P can be sent to the line given by $y = w = 0$. This means that there is a linear transformation B that sends Y to an element X in M'. Then $\varphi(B^{-1}, X) = Y$, so φ is indeed dominant. □

Remark 5.2.8 The explicit polynomials f, g, p, and q for X_h in (5.1) were found by letting a computer pick random polynomials modulo $p = 2$ and $p = 3$ such that the surface X_h with $h = 0$ is contained in M' as in Proposition 5.2.5. The computer then computed the characteristic polynomial of Frobenius and tested if there were only 2 eigenvalues that were roots of unity, see Remark 5.2.3.

By requiring more coefficients to vanish than is required for M', we can also find quartic surfaces Y for which the plane H_w given by $w = 0$ is tangent also at the third point $[0 : 0 : 1 : 0]$. In that case the intersection $H_w \cap Y$ has geometric genus 0 and if it has a point defined over $\mathbb{Q}$, then the intersection is birational to $\mathbb{P}^1$. The quartic surface Z given by

$$w(x^3 + y^3 + z^3 + x^2z + xw^2) = 3x^2y^2 - 4x^2yz + x^2z^2 + xy^2z + xyz^2 - y^2z^2 \tag{5.3}$$

is an example of such a surface. As in the proof of Theorem 5.2.2, modulo 3 the surface Z contains the line $z = w = 0$. Also, the reduction of Z at $p = 2$ contains a conic again, as the right-hand side of (5.3) factors over $\mathbb{F}_4$ as $(xy + xz + \zeta yz)(xy + xz + \zeta^2 yz)$, with $\zeta^2 + \zeta + 1 = 0$. An argument very similar to the one in the proof of Theorem 5.2.2 shows that Z also has geometric Picard number 1 with the Picard group generated by a hyperplane section. The only difference is that Frobenius does not act trivially on the conic $w = xy + xz + \zeta yz = 0$.

The hyperplane section $H_w \cap Z$ is a curve of geometric genus 0, parametrized by

$$[x : y : z : w] = [-(t^2 + t - 1)(t^2 - t - 3) : 2(t + 2)(t^2 + t - 1) : 2(t + 2)(t^2 - t - 3) : 0].$$

The Cremona transformation $[x : y : z : w] \mapsto [yz : xz : xy]$ gives a birational map from this curve to a nonsingular plane curve of degree 2.

Remark 5.2.9 In finding the explicit surfaces X_h not much computing power was needed, as we constructed the surface to have good reduction at small primes p so that counting points over $\mathbb{F}_{p^n}$ was relatively easy. Based on ideas of for instance Alan Lauder, Daqing Wan, Kiran Kedlaya, and Bas Edixhoven, it should be possible to develop more efficient algorithms for finding characteristic polynomials of (K3) surfaces. Together with these algorithms, the method used in the proof of Theorem 5.2.2 becomes a strong tool in finding Picard numbers of K3 surfaces over number fields.

Kloosterman has used this method to construct an elliptic K3 surface with Mordell-Weil rank 15 over $\overline{\mathbb{Q}}$, see [Kl]. In the proof of Theorem 5.2.2 we were able to compute the discriminant up to squares of the Néron-Severi lattice of $\overline{X}_p$ because we knew a priori a sublattice of finite index. Kloosterman realized that it is not always necessary to know such a sublattice. The image in $\mathbb{Q}^*/\mathbb{Q}^{*2}$ of the discriminant of the Néron-Severi lattice can also be deduced from the Artin-Tate conjecture, which has been proved for ordinary K3 surfaces in characteristic $p \geq 5$, see [NO], Thm. 0.2, and [Mi1], Thm. 6.1. It allows one to compute the ratio $\operatorname{disc} \mathrm{NS}(\overline{X}_p) \cdot \# \operatorname{Br}(\overline{X}_p)/(\mathrm{NS}(\overline{X}_p)^2_{\mathrm{tors}})$ from the characteristic polynomial of Frobenius acting on $H^2(\overline{X}_p, \mathbb{Q}_l)$. For an elliptic surface the Brauer group has square order, so this ratio determines the same element in $\mathbb{Q}^*/\mathbb{Q}^{*2}$ as $\operatorname{disc} \mathrm{NS}(\overline{X}_p)$.

5.3 More rational points

We now have an infinite family of explicit K3 surfaces with geometric Picard number 1 at our disposal. Heuristics say that on such a surface the number of rational points with height at most B grows asymptotically like $\log B$. Here the height of a point $[x : y : z : w]$ with $x, y, z, w \in \mathbb{Z}$ and $\gcd(x, y, z, w) = 1$ is defined to be the maximum of the absolute value of the coordinates x, y, z, and w. These heuristics assume the surface has no special characteristics, such as in our examples the existence of a curve with infinitely many rational points. We will therefore only consider the complement of these curves.

We have done a computer search for rational points on two explicit surfaces, namely the surface $X = X_h$ with $h = 0$ and the surface Y given by equation (5.3). On both surfaces we discard the points on the hyperplane H_w given by $w = 0$, as we already know these contain infinitely many rational points. We will also discard the points on Y that are contained in the hyperplane H_x given by $x = 0$, as the intersection $H_x \cap Y$ can be parametrized by

$$[x : y : z : w] = [0 : 1 + t^3 : t(1 + t^3) : -t^2].$$

This curve has a triple point at $[0 : 0 : 0 : 1]$. Table 5.1 shows all points found on X (outside H_w) with height at most 1500 and on Y (outside $H_w \cup H_x$) with height at most 400. They are ordered by height.

Remark 5.3.1 The picture on the cover of this thesis shows the K3 surface Y. More precisely, it shows the affine part given by $z = 1$ and $|x|, |y|, |w| \leq 5$. The curves shown are

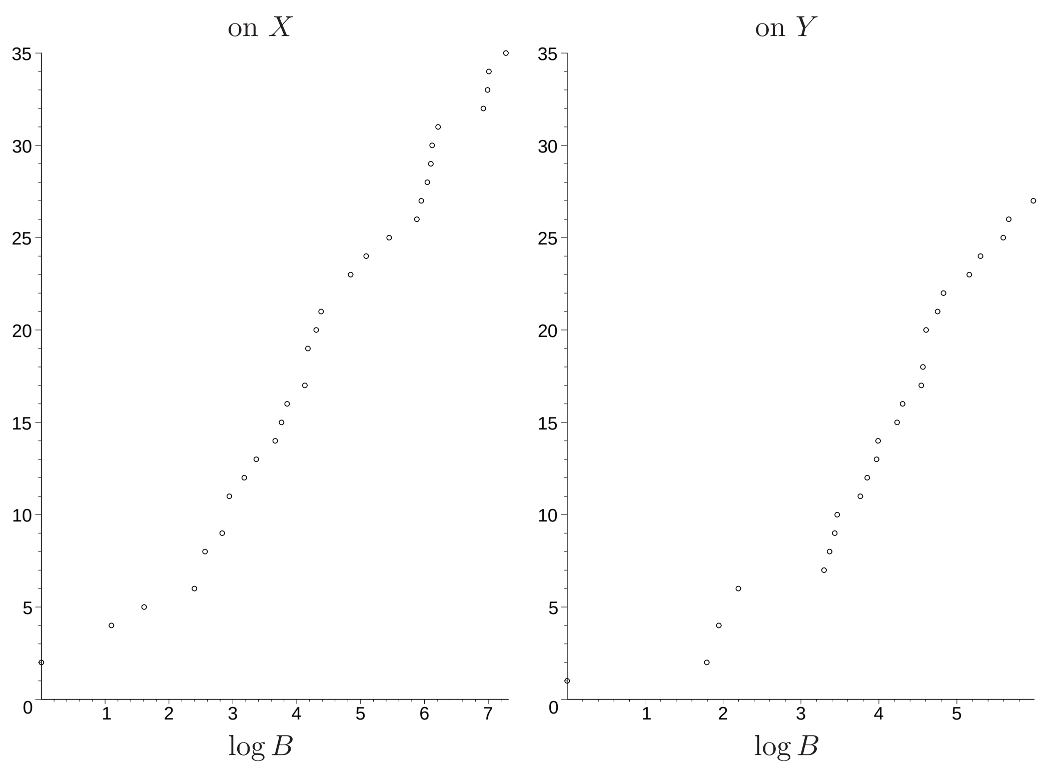
$X \setminus H_w$	$Y \setminus (H_w \cup H_x)$
$[x : y : z : w] =$	$[x : y : z : w] =$
$[0 : 1 : 1 : 1]$	$[1 : 1 : 0 : 1]$
$[1 : 1 : 0 : 1]$	$[1 : -4 : -6 : 3]$
$[2 : 3 : -1 : 3]$	$[5 : 7 : 4 : 3]$
$[-2 : 1 : -3 : 1]$	$[6 : -2 : 7 : 4]$
$[-2 : 1 : 7 : 5]$	$[-1 : 5 : -9 : 3]$
$[-4 : 11 : -5 : 6]$	$[-3 : 3 : 5 : 9]$
$[-2 : 1 : -13 : 10]$	$[27 : -3 : 0 : 1]$
$[10 : 13 : -7 : 13]$	$[13 : -9 : -29 : 7]$
$[9 : 17 : -5 : 16]$	$[31 : 20 : 30 : 3]$
$[-19 : 5 : -1 : 16]$	$[32 : -10 : 30 : 21]$
$[12 : -16 : -2 : 19]$	$[38 : -43 : -24 : 12]$
$[24 : 14 : -4 : 15]$	$[-47 : 9 : 21 : 9]$
$[12 : 29 : -13 : 24]$	$[3 : -34 : 26 : 53]$
$[1 : -43 : -4 : 37]$	$[54 : 15 : -30 : 52]$
$[-25 : 47 : 37 : 32]$	$[29 : 3 : 69 : 9]$
$[-35 : 62 : 32 : 37]$	$[29 : -64 : 74 : 28]$
$[-39 : -34 : 30 : 36]$	$[-48 : -9 : 94 : 36]$
$[37 : 65 : -40 : 25]$	$[-64 : 96 : 36 : 27]$
$[65 : 38 : -40 : 25]$	$[-64 : 16 : 100 : 3]$
$[-74 : 37 : -34 : 72]$	$[34 : 75 : -80 : 100]$
$[18 : 80 : -10 : 25]$	$[2 : 5 : -30 : 116]$
$[127 : 61 : -46 : 57]$	$[125 : -75 : -45 : 27]$
$[-44 : -127 : 68 : 64]$	$[-7 : 44 : -174 : 12]$
$[120 : 157 : -63 : 162]$	$[6 : 128 : -201 : 108]$
$[232 : 75 : 22 : 72]$	$[-55 : -28 : 162 : 269]$
$[-239 : 358 : 200 : 292]$	$[101 : -211 : -259 : 289]$
$[-384 : 117 : 359 : 80]$	$[-347 : 150 : 300 : 396]$
$[-266 : -422 : 316 : 263]$	
$[-446 : -104 : 118 : 293]$	
$[-67 : 455 : -117 : 338]$	
$[13 : -217 : -430 : 499]$	
$[338 : -959 : -182 : 1016]$	
$[1084 : 583 : -521 : 503]$	
$[-1106 : -209 : 812 : 196]$	
$[-514 : 1445 : 194 : 736]$	

Table 5.1: Rational points on X and Y of height at most 1500 and 400 respectively

the intersection of Y with the hyperplanes H_w and H_x, both of which contain infinitely many rational points. All rational points outside these curves with height at most 400 are plotted as well. These are the 27 points from the right column in Table 5.1, but only 13 of them are visible.

Remark 5.3.2 Some of the points in Table 5.1 may lie on a curve of geometric genus ≤ 1. As the Picard groups $\operatorname{Pic} X$ and $\operatorname{Pic} Y$ are generated by a hyperplane section, such a curve is the intersection of a hypersurface of some degree with X or Y respectively. For both X and Y we computed the genus of this curve of intersection for all hyperplanes (degree 1) through 3 of the points of Table 5.1. All these curves of intersection turn out to have geometric genus 3 as expected. The program used to check this is electronically available from the author upon request.

The following graphs show how the number of points with height at most B grows in terms of B. As mentioned before, this is expected to grow like $\log B$. We will not draw any conclusions from these graphs about the asymptotic behavior, nor will we speculate about the rational points being infinite in number, let alone about their density. With an analytic method developed by Noam Elkies, see [Elk], a more efficient algorithm for finding rational points can be implemented than the one we have used. This will allow us to obtain more precise data about the distribution of rational points on K3 surfaces.



Number of points with height at most B as a function of $\log B$

5.4 Conclusion and open problems

We end with the conclusion that still very little is known about the arithmetic of K3 surfaces, but this chapter has brought us closer to understanding the distribution of rational points on K3 surfaces with geometric Picard number 1. We reiterate three questions that remain unsolved.

Question 2 *Does there exist a K3 surface over a number field such that the set of rational points is neither empty nor dense?*

Question 3 *Does there exist a K3 surface over a number field with geometric Picard number* 1*, such that the set of rational points is potentially dense?*

Question 4 *Does there exist a K3 surface over a number field with geometric Picard number* 1*, such that the set of rational points is not potentially dense?*

Bibliography

[Aa] Aassila, M., Some results on Heron triangles, *Elem. Math.*, **56** (2001), pp. 143–146.

[Ar] Artin, M., On Isolated Rational Singularities of Surfaces, *Amer. J. Math.*, **88** (1966), pp. 129–136.

[Be] Beauville, A., Application aux espaces de modules, *Géométrie des surfaces K3: Modules et Périodes, Astérique*, **126** (1985), pp. 141–152.

[BLR] Bosch, S., Lütkebohmert, W., and Raynaud, M., *Néron Models*, Springer-Verlag, Berlin, 1990.

[BLV] Beukers, F., van Luijk, R., and Vidunas, R., A linear algebra exercise, *Nieuw Archief voor Wiskunde*, **3** (2002), pp. 139–140.

[BM] Bombieri, E. and Mumford, D., Enriques' classification of surfaces in char. p, II, *Complex Analysis and Algebraic Geometry — Collection of papers dedicated to K. Kodaira*, ed. W.L. Baily and T. Shioda, Iwanami and Cambridge Univ. Press (1977), pp. 23–42.

[Bo] Bourbaki, N., *Lie Groups and Lie Algebras, Chapters 4–6*, Elements of Mathematics, Springer, 2002; orig. Hermann, Paris, 1968.

[BPV] Barth, W., Peters, C., and Van de Ven, A., *Compact Complex Surfaces*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 4, Springer-Verlag, 1984.

[Br] Bremner, A., On squares of squares II, *Acta Arith.*, **99**, no. 3 (2001), pp. 289–308.

[BT] Bogomolov, F. and Tschinkel, Yu., Density of rational points on elliptic K3 surfaces, *Asian J. Math.*, **4**, 2 (2000), pp. 351–368.

[BW] Bruce, J. and Wall, C., On the classification of cubic surfaces, *J. London Math. Soc. (2)*, **19** (1979), pp. 245–256.

[Ch] Chinburg, T., Minimal Models of Curves over Dedekind Rings, *Arithmetic Geometry*, ed. Cornell, G. & Silverman, J. (1986), pp. 309–326.

[CR] Colliot-Thélène, J.-L. and Raskind, W., Groupe de Chow de codimension deux des variétés définies sur un corps de nombres: un théorème de finitude pour la torsion, *Invent. Math.*, **105** (1991), pp. 221–245.

[CS] Conway, J.H. and Sloane, N.J.A., *Sphere packings, lattices and groups, third edition*, Grundlehren der mathematischen Wissenschaften **290**, Springer, 1999.

[De] Deligne, P., La Conjecture de Weil. I, *Publ. Math. IHES*, **43** (1974), pp. 273–307.

[Du] Du Val, P., On isolated singularities which do not affect the conditions of adjunction, Part I, *Proc. Cambridge Phil. Soc.*, **30** (1934), pp. 453–465.

[EGA II] Grothendieck, A., *Éléments de géométrie algébrique. IV. Étude globale élémentaire de quelques classes de morphismes*, IHES Publ. Math., no. **8**, 1961.

[EGA IV(1)] Grothendieck, A., *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas, Première partie*, IHES Publ. Math., no. **20**, 1964.

[EGA IV(2)] Grothendieck, A., *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas, Seconde partie*, IHES Publ. Math., no. **24**, 1965.

[EGA IV(4)] Grothendieck, A., *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie*, IHES Publ. Math., no. **32**, 1967.

[Elk] Elkies, N., Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction, *Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., Springer*, **1838** (2000), pp. 33–63.

[Ell] Ellenberg, J., K3 surfaces over number fields with geometric Picard number one, *Arithmetic of higher-dimensional algebraic varieties*, Progress in Math., Vol. **226**, ed. B. Poonen and Y. Tschinkel (2004), pp. 135–140.

[FJ] Fried, M.D. and Jarden, M., *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. **11**, Springer-Verlag, 1986.

[Fu] Fulton, W., *Intersection Theory, second edition*, Springer, 1998.

[GAGA] Serre, J.-P., Géométrie algébrique et géométrie analytique, *Ann. Inst. Fourier*, **6** (1956), pp. 1–42.

[GH] Griffiths, P. and Harris, J., *Principles of Algebraic Geometry*, Reprint of the 1978 original, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1994.

[Gu] Guy, R., *Unsolved Problems in Number Theory*, Problem Books in Math., Springer-Verlag, New-York, 1994.

[Ha1] Hartshorne, R., Equivalence relations of algebraic cycles and subvarieties of small codimension, *Algebraic Geometry, Arcata 1974*, Amer. Math. Soc. Proc. Symp. Pure Math. **29** (1975), pp. 129–164.

[Ha2] Hartshorne, R., *Algebraic Geometry*, GTM **52**, Springer-Verlag, New-York, 1977.

[Hr1] Harari, D., Méthode des fibrations et obstruction de Manin, *Duke Math. J.*, **75**, no. 1 (1994), pp. 221–260.

[Hr2] Harari, D., Flèches de spécialisations en cohomologie étale et applications arithmétiques, *Bull. Soc. Math. France*, **125**, no. 2 (1997), pp. 143–166.

[In] Inose, H., On certain Kummer surfaces which can be realized as non-singular quartic surfaces in $\mathbb{P}^3$, *Journal of the Faculty of Science. The University of Tokyo*, Section 1A, mathematics, **23** (1976), pp. 545–560.

[KL] Kramer, A.-V. and Luca, F., Some remarks on Heron triangles, *Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.)*, **27** (2000), pp. 25–38 (2001).

[Kl] Kloosterman, R., An explicit example of an elliptic K3 surface with Mordell-Weil rank 15, Preprint, available at `arXiv:math.AG/0502439`, 2005

[Ko1] Kodaira, K., On compact analytic surfaces II–III, *Ann. of Math.*, **77** (1963), pp. 563–626; **78** (1963), pp. 1–40.

[Ko2] Kodaira, K., On the structure of compact complex analytic surfaces I, II, *Amer. J. Math.*, **86** (1964), pp. 751–798; **88** (1966), pp. 682–721.

[La] Lang, S., *Algebra, 3rd ed.*, Addison-Wesley, 1993.

[Lic] Lichtenbaum, S., Curves over discrete valuation rings, *Amer. J. Math.*, **90** (1968), pp. 380–405.

[Lip] Lipman, J., Rational singularities, with applications to algebraic surfaces and unique factorization, *IHES Publ. Math.*, **36** (1969), pp. 195–279.

[Man] Manin, Y., *Cubic forms: Algebra, Geometry, Arithmetic*, North-Holland, Amsterdam, 1974.

[Maz] Mazur, B., Modular curves and the Eisenstein ideal, *IHES Publ. Math.*, **47** (1977), pp. 33–186.

[Mi1] Milne, J.S., On a Conjecture of Artin and Tate, *Ann. of Math.*, **102** (1975), pp. 517–533.

[Mi2] Milne, J.S., *Étale Cohomology*, Princeton Mathematical Series **33**, Princeton University Press, New Jersey, 1980.

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

[MM] Mori, S. and Mukai, S., The uniruledness of the moduli space of curves of genus 11, *Algebraic Geometry*, Lect. Notes in Math. **1016**, ed. A. Dold and B. Eckmann, Springer-Verlag (1983), pp. 334–353.

[Mu] Mutsasaka, T., The Criteria for Algebraic Equivalence and the Torsion Group, *Am. J. Math.*, Vol. **79**, No. 1 (1957), pp. 53–66.

[Na] Nagata, M., On rational surfaces I, II, *Mem. Coll. Sci. Kyoto (A)*, **32** (1960), pp. 351–370; **33** (1960), pp. 271–293.

[NAW] Problem 10, Problem Section, *Nieuw Archief voor Wiskunde*, **1** (2000), pp. 413–417.

[Ne] Néron, A., Modèles minimaux des variétés abéliennes, *Ann. of Math.*, **82** (1964), pp. 361–482.

[Ni] Nikulin, V., Integral symmetric bilinear forms and some of their applications, *Math. USSR Izvestija*, **14**, 1 (1980), pp. 103–167.

[NO] Nygaard, N. and Ogus, A., Tate's conjecture for K3 surfaces of finite height, *Ann. of Math.*, **122** (1985), pp. 461–507.

[Og] Oguiso, K., An elementary proof of the topological Euler characteristic formula for an elliptic surface, *Comment. Math. Univ. Sancti Pauli*, **39**, 1 (1990), pp. 81–86.

[O'Su] O'Sullivan, M., *Classification and Divisor Class Groups of Normal Cubic Surfaces in* $\mathbb{P}^3$, U.C. Berkeley, Ph.D. dissertation (not published), 1996.

[Pi] Pinkham, H., Singularités Rationnelles de Surfaces, *Séminaire sur les Singularités des Surfaces*, Lect. Notes in Math. **777**, ed. M. Demazure, H. Pinkham, and B. Teissier, Springer-Verlag (1980), pp. 147–172.

[PS] Pjateckii, I. and Shafarevich, I., Torelli's theorem for algebraic surfaces of type K3, *Izv. Akad. Nauk SSSR Ser. Mat.*, **35** (1971), pp. 530–572.

[SGA 1] Grothendieck, A., *Revêtements étales et groupe fondamental*, Lect. Notes in Math. **224**, Springer-Verlag, Heidelberg, 1971.

[SGA $4\frac{1}{2}$] Grothendieck, A. et al., *Cohomologie étale*, Lect. Notes in Math. **569**, Springer-Verlag, Heidelberg, 1977.

[SGA 6] Grothendieck, A. et al., *Théorie des Intersections et Théorème de Riemann-Roch*, Lect. Notes in Math. **225**, Springer-Verlag, Heidelberg, 1971.

[SGA 7 II] Deligne, P., Katz, N., *Groupes de monodromie en géométrie algébrique, II (SGA 7 II)*, Lect. Notes in Math. **340**, Springer, Berlin, 1973.

[Sha] Shafarevich, I., *Lectures on Minimal Models and Birational Transformations of Two-dimensional Schemes*, Tata Institute, Bombay, 1966.

[Shi1] Shioda, T., On elliptic modular surfaces, *J. Math. Soc. Japan*, Vol. **24**, No. 1 (1972), pp. 20–59.

[Shi2] Shioda, T., On the Picard number of a complex projective variety, *Ann. Sci. École Norm. Sup.* (4), **14** (1981), no. 3, pp. 303–321.

[Shi3] Shioda, T., On the Mordell-Weil Lattices, *Comm. Math. Univ. Sancti Pauli*, **39**, 2 (1990), pp. 211–240.

[SI] Shioda, T. and Inose, H., On singular K3 surfaces, *Complex Analysis and Algebraic Geometry*, 1977, pp. 119–136.

[Si1] Silverman, J.H., *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag, New-York, 1986.

[Si2] Silverman, J.H., *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM **151**, Springer-Verlag, New-York, 1994.

[Ta1] Tate, J., Genus change in inseparable extensions of function fields, *Proc. AMS*, **3** (1952), pp. 400–406.

[Ta2] Tate, J., Algebraic cycles and poles of zeta functions, *Arithmetical Algebraic Geometry*, ed. O.F.G. Schilling (1965), pp. 93–110.

[Ta3] Tate, J., Algorithm for determining the type of a singular fiber in an elliptic pencil, *Modular functions of one variable IV*, Lect. Notes in Math. **476**, ed. B.J. Birch and W. Kuyk, Springer-Verlag, Berlin (1975), pp. 33–52.

[Te] Terasoma, T., Complete intersections with middle Picard number 1 defined over $\mathbb{Q}$, *Math. Z.*, **189** (1985), no. 2, pp. 289–296.

[VG] Van Geemen, B., Some remarks on Brauer groups of K3 surfaces, To appear in: *Advances in Math.*, Available at: `arXiv:math.AG/0408006`

[VL1] Van Luijk, R., A K3 surface associated to certain integral matrices with integral eigenvalues, preprint, available at `arXiv:math.AG/0411600`, 2004

[VL2] Van Luijk, R., An elliptic K3 surface associated to Heron triangles, preprint, available at `arXiv:math.AG/0411606`, 2004

[VL3] Van Luijk, R., K3 surfaces with Picard number one and infinitely many rational points, preprint, 2005

[We] Weil, A., *Foundation of Algebraic Geometry, 2nd ed.*, AMS, 1962.