Computations on diagonal quartic surfaces

Martin James Bright
Clare College

A dissertation submitted for the degree of Doctor of Philosophy at the University of Cambridge

September 2002

Preface

This dissertation is not substantially the same as any I have submitted for a degree or diploma or other qualification at any other university. Except where indicated in the text, it is the result of my own work and contains nothing which is the outcome of work done in collaboration.

I thank my research supervisor, Sir Peter Swinnerton-Dyer, for his expert guidance in the course of my studies. In particular, he has made me realise the great value of explicit calculations in understanding number theory. I would also like to thank the many people who have helped me with mathematical discussions, as well as those who have given moral support. I acknowledge the financial support of the Engineering and Physical Sciences Research Council. I am also very grateful to IBM Research for awarding me their first Special European Research Fellowship, including an IBM ThinkPad computer which has been invaluable both for computation and for producing this dissertation. Finally, I would like to thank the authors of PARI/GP for making the fruits of their work freely available.

Clare College
September 2002

Summary

We are concerned with the solubility in integers of the equation

$$a_0 X_0^4 + a_1 X_1^4 + a_2 X_2^4 + a_3 X_3^4 = 0$$

where a_0, a_1, a_2 and a_3 are fixed integral coefficients. As the equation is homogeneous, this is equivalent to studying rational solutions. This equation defines a surface in three-dimensional projective space $\mathbb{P}^3$, which we denote by V. Geometrically, V is a K3 surface.

One condition which is clearly necessary for V to have rational points is that there be points on V in each completion $\mathbb{Q}_v$ of $\mathbb{Q}$. Varieties for which this condition is sufficient are said to satisfy the *Hasse principle*. In general, the Hasse principle does not hold, but many counterexamples are explained by the so-called *Brauer–Manin obstruction*. This was first put forward by Manin and is defined in terms of the *Brauer group* of the variety.

The aim of this dissertation is to classify all diagonal quartic surfaces, defined by the above equation, into finitely many cases. The cases are distinguished by the action of the absolute Galois group of $\mathbb{Q}$ on the Picard group of V, and we show that there are 546 such cases. They are described in terms of algebraic constraints on the coefficients a_i. In each case, we compute that part of the Brauer group of V which splits over the algebraic closure of $\mathbb{Q}$; this is done using the Galois cohomology of the Picard group of V. We also investigate the elliptic fibrations which may exist on V: to such a fibration is associated a *vertical Brauer group*, and we show how these groups may also be computed. Finally, an indication is given of how these results may be used to look further into the Brauer–Manin obstruction on V.

Contents

List of notation

	Arithmetic
k_v	Completion of the field k with respect to the valuation v
$\mathbb{F}_p$	Finite field with p elements
ϵ	Primitive eighth root of unity, $\epsilon = (1+i)/\sqrt{2}$
α_{ij}	Fourth root of a_i/a_j
$H^i(L/K, M)$	Galois cohomology of $\mathrm{Gal}(L/K)$ with values in M
$H^i(k, M)$	Galois cohomology of $\mathrm{Gal}(\bar{k}/k)$ with values in M
$\hat{H}^i(\quad)$	Tate cohomology groups
$\cup$	Cup product
$\mathrm{Br}\, L/K$, $\mathrm{Br}\, k$	Brauer group of L/K, of $\bar{k}/k$
inv_v	Local invariant map $\mathrm{Br}\, k_v \xrightarrow{\mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}$
$(\quad,\quad)_v$	Local Hilbert symbol at v
	Linear algebra
$\mathbf{M}^T$	Transpose of matrix $\mathbf{M}$
$\mathbf{M}_{(i)}$	ith column of matrix $\mathbf{M}$
$\mathbf{I_n}$	$n \times n$ identity matrix
$(\mathbf{M_1} \vert \mathbf{M_2})$	Matrix made by joining matrices $\mathbf{M_1}$ and $\mathbf{M_2}$
	Geometry
$\mathbb{P}^n_k$	n-dimensional projective space over the field k
$\mathrm{Pic}\, X$	Picard group of X
$\mathrm{NS}\, X$	Néron–Severi group of X
$\mathrm{Pic}^0\, X$	Subgroup of $\mathrm{Pic}\, X$ algebraically equivalent to 0
$\mathrm{Pic}^n\, X$	Subgroup of $\mathrm{Pic}\, X$ numerically equivalent to 0

$\mathrm{Pic}_{\mathrm{vert}}$	Vertical Picard group of a fibration
$\mathcal{L}(D)$	Line bundle associated to divisor D
$h^i(X,\mathcal{F})$	Dimension of cohomology group $H^i(X,\mathcal{F})$ over $k(X)$
$\chi(X,\mathcal{F})$	Euler characteristic of $\mathcal{F}$, alternating sum of the $h^i(X,\mathcal{F})$
$\ell(D)$	$h^0(\mathcal{L}(D))$
$s(D)$	$h^1(\mathcal{L}(D))$, the superabundance of D
$\mathcal{O}_X$, $\mathcal{K}_X$, Ω_X, $\mathcal{D}_X$	Sheaves of regular functions, rational functions, regular differentials and divisors on X
$h^{i,j}(X)$	Dimension of $H^i(X,\Omega^j_X)$
p_a, p_g	Arithmetic, geometric genus
Π	Divisor class of a plane section
$D_1.D_2$	Intersection number of divisors D_1 and D_2
X_t	Fibre of map $X\to Y$ at the point $t\in Y$

Arithmetic and geometry

$k(X)$	Function field of scheme X (nothing to do with the field k)
X_K	Product scheme $X\times_{\operatorname{Spec} k}\operatorname{Spec} K$
$\bar{X}$	$X_{\bar{k}}$
$\mathbb{G}_{\mathrm{m}}$	Étale sheaf corresponding to the multiplicative group scheme; étale sheaf of rational functions on a variety
$\operatorname{Br} X$	Brauer group of scheme X
$\operatorname{Br}_0 X$	Image of $\operatorname{Br} k$ in $\operatorname{Br} X$
$\operatorname{Br}_1 X$	Kernel of $\operatorname{Br} X\to\operatorname{Br}\bar{X}$
$H^2_{\mathrm{Az}}(X)$	Kernel of $H^2(k,k(\bar{X})^\times/\bar{k}^\times)\to H^2(k,\operatorname{Div}\bar{X})$

Chapter 1

Introduction

We are concerned with the solubility in integers of the equation

$$a_0X_0^4 + a_1X_1^4 + a_2X_2^4 + a_3X_3^4 = 0 \tag{1.1}$$

where a_0, a_1, a_2 and a_3 are fixed non-zero integral coefficients. As the equation is homogeneous, this is equivalent to studying rational solutions, and we allow the coefficients to be any rational numbers. The equation (1.1) defines a surface in three-dimensional projective space $\mathbb{P}^3$, which we denote throughout by V. Where we need to make a distinction between the variety defined over the rational numbers $\mathbb{Q}$ and that defined over the algebraic closure $\bar{\mathbb{Q}}$, we will always denote the former by V and the latter by $\bar{V}$.

1.1 Background

One condition which is clearly necessary for rational solutions of (1.1) is that there be solutions in the real numbers $\mathbb{R}$ and in each p-adic field $\mathbb{Q}_p$, where p runs through all rational primes. In other words, we require that V have points everywhere locally. For certain classes of varieties, this condition is also a sufficient one: if points exist everywhere locally, then points also exist globally. This was first proved for quadratic forms, and in that case is the well-known theorem of Hasse–Minkowski [36, Chapter IV, Theorem 8]. A family of varieties for which local solubility is a sufficient condition for global solubility is said to satisfy the *Hasse principle*.

However, it has been known for a long time that not every variety satisfies the Hasse principle: in the case of curves, several famous examples of curves of genus 1 not satisfying the Hasse principle were known some time ago; see, for example, Selmer [34]. Such curves are now described by elements of the Tate–Shafarevich group of their Jacobians. Examples have also been exhibited of cubic surfaces not satisfying the Hasse principle: see Swinnerton-Dyer [42]; Mordell [30]; and Cassels and Guy [6]. To explain these counterexamples to the Hasse principle, Manin put forward in [25] and [24] a definition of an obstruction to the Hasse principle, based on the Brauer group of the variety, which accounted for all the examples listed above. This obstruction is known as the *Brauer–Manin obstruction* to the Hasse principle.

The *Brauer group* of a variety, defined in Chapter 4, is the group of Azumaya algebras on that variety modulo equivalence. An *Azumaya algebra* may be considered as a continuously varying family of central simple algebras over the base field k (in our case $k = \mathbb{Q}$), parametrised by the points of the variety; alternatively, it is a central simple algebra over the function field of the variety which specialises at each point x to a central simple algebra over $k(x)$. The equivalence relation defined on Azumaya algebras is a straightforward extension of that used to define the Brauer group of a field in terms of central simple algebras.

Manin's obstruction relies on the fundamental theorem of Albert–Brauer–Hasse–Noether, which forms a basic part of class field theory:

Theorem 1.1 (Albert–Brauer–Hasse–Noether). *Let k be an algebraic number field. Then there exist injective group homomorphisms*

$$\mathrm{inv}_v : \mathrm{Br}\, k_v \to \mathbb{Q}/\mathbb{Z}$$

for each place v of k, called local invariant *maps, such that the sequence*

$$0 \to \mathrm{Br}\, k \to \bigoplus_v \mathrm{Br}\, k_v \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}$$

is exact.

Proof. See [46, Section 10.2, Theorem B]. □

Note that implicit in this statement is that, for any algebra in $\operatorname{Br} k$, all but finitely many of the local invariants are zero.

Manin's observation was that, for any rational point x on the variety and any Azumaya algebra $\mathcal{A}$ in the Brauer group, we must have

$$\sum_v \operatorname{inv}_v \mathcal{A}(x) = 0.$$

Therefore, if it possible to show that, for any adèlic point (x_v) on the variety, the sum $\sum_v \operatorname{inv}_v \mathcal{A}(x_v)$ is non-zero for some Azumaya algebra $\mathcal{A}$, then no rational point can exist. This is Manin's obstruction. A more formal definition follows.

Definition 1.2. Let X be a complete algebraic variety defined over a number field k. The set of *adèlic points* of X is simply

$$X(\mathbb{A}_k) = \prod_v X(k_v).$$

Let B be a subgroup of the Brauer group $\operatorname{Br} X$. We define

$$X(\mathbb{A}_k)^B = \Big\{ (x_v) \in X(\mathbb{A}_k) \quad \Big| \quad \sum_v \operatorname{inv}_v \mathcal{A}(x_v) = 0 \text{ for all } \mathcal{A} \in B \Big\}.$$

The sum exists because $\operatorname{inv}_v \mathcal{A}(x_v)$ is zero for all but finitely many primes v. If $X(\mathbb{A}_k)^B$ is empty, we say that there is a *Brauer–Manin obstruction to the Hasse principle* attached to B.

The natural question to ask, given this definition, is the following: for a given family of varieties, is the Brauer–Manin obstruction the only obstruction to the Hasse principle? In other words, is it a sufficient condition for the existence of a rational point that the variety have points everywhere locally, and that there be no Brauer–Manin obstruction? This has been answered affirmatively for curves of genus 1, where it fits into the theory of the Tate–Shafarevich group (assuming this group to be finite; see [23, Chapter X, Theorem 2.1]); extensive work has also been done on rational varieties, which is described in the survey by Manin and Tsfasman [26]. However, the Brauer–Manin obstruction is known not to be the only obstruction to the Hasse principle for all varieties. Examples are known (see Skorobogatov's paper [41]) of varieties for which the Brauer–Manin obstruction is not the only obstruction.

A good brief overview of this material is presented in Chapter X of Lang's survey [23].

The *geometry* of the diagonal quartic surface $\bar{V}$, that is, its structure as a variety over the complex numbers, does not depend on the coefficients a_i and is well understood. Any non-singular surface in $\mathbb{P}^3$ defined by an equation of degree 4 falls into the class of *K3 surfaces*. The definition and properties of K3 surfaces, and how they fit into the more general classification of algebraic surfaces, are described in many books, such as those by Beauville [3], Iskovskikh and Shafarevich [22] and Barth, Peters and Van de Ven [2]. One property which makes K3 surfaces particularly suited to the computations performed here is that the Picard group is the same as the Néron–Severi group, which is finitely generated and torsion-free. The problem of finding rational points on a K3 surface defined over the rational numbers is a hard one, about which little is known; the study of the diagonal quartic surfaces (1.1) might be viewed as an attempt to gain some understanding of K3 surfaces more generally. The family of diagonal quartic surfaces is well suited to this, for it is broad enough to show some variation in characteristics of the surfaces, but narrow enough to allow much concrete computational experimentation.

One feature of K3 surfaces is that some have the structure of an *elliptic fibration*: that is, they possess a map to $\mathbb{P}^1$, the generic fibre of which is an elliptic curve. There are many such fibrations defined on the diagonal quartic surface $\bar{V}$; depending on the coefficients a_i, these fibrations may or may not be defined over the rational numbers. Where there is a fibration defined over the rational numbers, this can be of use in trying to find rational points on V.

Some of the results in this dissertation overlap with those in [32] of Pinch and Swinnerton-Dyer. There, the authors were interested in verifying the

Tate conjecture, which relates the order of a zero of a certain L-function to the rank of the Néron–Severi group of the surface. These ranks were therefore computed, using a method, similar to the one described here, of dividing the surfaces into cases. However, we are also concerned with the first Galois cohomology group of the Picard group, rather than just the invariant part; this means that our division into cases will be much finer than that in [32], making the calculations unreasonably large to perform by hand.

Approaches in the literature to studying the Brauer–Manin obstruction on K3 surfaces have arisen out of techniques using fibrations. These methods have previously been applied to various rational surfaces: see the survey by Colliot-Thélène [9] for a detailed account of this. In particular, a series of papers variously by Colliot-Thélène, Sansuc, Skorobogatov and Swinnerton-Dyer have proved that, under certain assumptions, the Brauer–Manin obstruction is the only obstruction to the Hasse principle for pencils of conics and more broadly for generalised Severi–Brauer varieties [13]. The same techniques have more recently been applied to pencils of curves of genus 1 [11, 12], of which the diagonal quartic surfaces studied in [44] are a specific example. The results obtained there make certain hypotheses on the elliptic fibrations which have an interpretation in terms of the relationship between the vertical Brauer group of the fibration and the whole Brauer group. It is hoped that the computations and methods put forward in this dissertation may be able to throw more light on the methods used there, and on the Brauer–Manin obstruction for K3 surfaces generally.

1.2 Overview

The aim of this dissertation is to show how computational methods may be used to investigate the Brauer–Manin obstruction on diagonal quartic surfaces. The algorithms and results presented here fall broadly into three related areas:

- the classification of all diagonal quartic surfaces into 546 cases, according to the Galois action on the Picard group;

- the demonstration of how Galois cohomology can be used to compute, and explicitly express, certain elements of the Brauer group of V;
- the finding of elliptic fibrations on V, where they exist, and the relating of computations in Galois cohomology to the theory of the vertical Brauer group attached to such a fibration.

The Brauer group of the variety V over $\mathbb{Q}$ has a natural filtration:

$$\mathrm{Br}_0 V \subseteq \mathrm{Br}_1 V \subseteq \mathrm{Br} V$$

where $\mathrm{Br}_0 V$ consists of constant algebras, that is, the image of $\mathrm{Br}\,\mathbb{Q}$ in $\mathrm{Br} V$; and $\mathrm{Br}_1 V$ consists of those algebras which split over the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. Now all the diagonal quartic surfaces are isomorphic over $\bar{\mathbb{Q}}$, so the part of the Brauer group which does not split over $\bar{\mathbb{Q}}$ (that is, the quotient $\mathrm{Br} V/\mathrm{Br}_1 V$) is fixed as the coefficients a_i vary. What concerns us in this dissertation is how to compute the part of the Brauer group which is dependent on the a_i, which is $\mathrm{Br}_1 V$. We will call this the *arithmetic part* of the Brauer group.

A constant algebra can give no Brauer–Manin obstruction: so we are interested in the quotient $\mathrm{Br}_1 V/\mathrm{Br}_0 V$. Now this is known to be isomorphic to the Galois cohomology group $H^1(\mathbb{Q}, \mathrm{Pic}\,\bar{V})$. We wish to calculate this cohomology group for all diagonal quartic surfaces.

One very useful observation about the surface $\bar{V}$ is that it contains many straight lines. Indeed, writing

$$a_0 X_0^4 = -a_1 X_1^4 \quad \text{and} \quad a_2 X_2^4 = -a_3 X_3^4$$

gives sixteen straight lines. These lines will be labelled L^{123}_{mn}, where m and n run through the values 1, 3, 5 and 7. In the equations of these lines, we write (as we will throughout) ϵ for a fixed primitive eighth root of unity, and α_{ij} for a fixed fourth root of a_i/a_j. We will choose the α_{ij} such that $\alpha_{ij}\alpha_{jk} = \alpha_{ik}$. The lines are then given by

$$L^{123}_{mn} : X_0 = \epsilon^m \alpha_{10} X_1, \quad X_2 = \epsilon^n \alpha_{32} X_3. \tag{1.2}$$

Similarly we define the lines

$$L_{mn}^{231} : X_0 = \epsilon^m \alpha_{20} X_2, \quad X_3 = \epsilon^n \alpha_{13} X_1 \tag{1.3}$$
$$L_{mn}^{312} : X_0 = \epsilon^m \alpha_{30} X_3, \quad X_1 = \epsilon^n \alpha_{21} X_2 \tag{1.4}$$

making 48 straight lines in all. In fact there are no other straight lines on the surface. It turns out that these 48 lines generate the Picard group of $\bar{V}$, which is a free Abelian group of rank 20. Our problem of studying the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the Picard group is reduced to studying the action on these 48 straight lines, which is very straightforward to describe. For the lines are all defined over a finite extension of $\mathbb{Q}$ of simple structure, and thus the Galois action factors through a finite group which is very amenable to computation.

The first main result of this work is to show that the Galois action on the 48 lines, and hence on the Picard group of $\bar{V}$, may take only finitely many forms, whatever the coefficients a_i. These 'cases' into which the diagonal quartic surfaces may fall correspond to subgroups of a certain Galois group Γ, up to various automorphisms which are made explicit. The cases are then described by putting various algebraic constraints on the a_i, and an algorithm is described for quickly finding the Galois action from the coefficients a_i.

A very simple example is useful to explain the concept of this approach. Suppose that we are studying the equation

$$X^2 = a$$

over the rational numbers. Clearly, this equation has solutions when a is a rational square, and has no solutions otherwise. Thus there are two cases into which this equation may fall, and they are distinguished by the algebraic condition "a is a square". The relevant Galois group here is $\mathrm{Gal}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$, which is always a subgroup of the 'generic' group $\mathrm{Gal}(\mathbb{Q}(\sqrt{x})/\mathbb{Q}(x))$, cyclic of order 2: the latter has two subgroups, being the whole group and the trivial subgroup, which correspond to the two cases. The classification of the diagonal quartic surfaces into cases follows the same lines, but the Galois group Γ is considerably larger (of order 256) and non-Abelian. There is a further complication: various different choices of roots and permutations of the coordinates can lead to different subgroups which we wish to consider as the same case.

In each case, the Galois action on the Picard group of $\bar{V}$ allows us to compute both the Picard group of V, and the structure of the arithmetic part of the Brauer group of V. However, we are using the isomorphism between $\mathrm{Br}_1 V / \mathrm{Br}_0 V$ and $H^1(\mathbb{Q}, \mathrm{Pic}\,\bar{V})$. This isomorphism must be made explicit if we are to write down elements of the Brauer group as Azumaya algebras. This is necessary in order to compute the Brauer–Manin obstruction. So the following part of this dissertation concerns the gap between the computational procedures expounded in the first part, and explicitly expressing elements of Brauer groups.

As described above, fibrations have been used to look into the Hasse principle and Brauer–Manin obstruction on various surfaces; in particular, one class of diagonal quartic surfaces (corresponding to several of our cases) was studied in depth by Swinnerton-Dyer [44]. The fibrations which may exist on K3 surfaces are morphisms to $\mathbb{P}^1$ whose generic fibre is a curve of genus 1. We discuss the geometry of such fibrations, and in particular show that an elliptic fibration, defined over the rational numbers, exists on V if and only if the intersection quadratic form on $\mathrm{Pic}\, V$ represents 0. Later, after discussing Brauer groups, we show that the vertical Brauer group attached to a fibration may be computed in terms of a cohomology group $H^1(\mathbb{Q}, \mathrm{Pic}_{\mathrm{vert}})$, where $\mathrm{Pic}_{\mathrm{vert}}$ is the subgroup of $\mathrm{Pic}\,\bar{V}$ generated by the irreducible components of the fibres. Elements of the vertical Brauer group may be expressed in a comparatively simple form, making them easier to write down than arbitrary elements of the Brauer group.

The study of the geometry of the diagonal quartic surface V is covered in Chapter 2. There various geometric facts are reviewed, both about general K3 surfaces and about the diagonal quartic specifically. We discuss fibrations over the projective line, and how divisors on V interact with such fibrations; this will be important when we come to study the vertical Brauer group. Using a particular fibration, we prove in Proposition 2.15 that the 48 straight lines on $\bar{V}$ do indeed generate the Picard group. Finally, we move away from pure geometry and look at fibrations defined over the rational numbers; in particular, we prove in Proposition 2.23 that such a fibration exists if and only if the intersection form represents zero.

Most of the computational work referred to above is described in Chapter 3. First, some general algorithms for computing with Abelian groups are recalled. The group Γ is not in fact Abelian, but is 'almost' so, having an Abelian subgroup of index 2. We must therefore demonstrate methods for representing, and computing with, elements and subgroups of Γ. Having done so, we define precisely the various automorphisms which lead to certain collections of subgroups being identified as one 'case' into which the diagonal quartic surface might fall. We then show how to list the 546 different cases, which are given in Appendix A.

After listing the various cases, certain useful computations are described: algorithms are given which implement the correspondence between subgroups of Γ and sets of coefficients (a_i). As the goal of these calculations is to study the Galois action on the Picard group of $\bar{V}$, we then review some techniques for computing cohomology groups and apply them to the 48 lines on $\bar{V}$.

Chapter 4 deals with the problem of moving between elements, computed in Chapter 3, of $H^1(\mathbb{Q}, \operatorname{Pic} \bar{V})$ and elements of the Brauer group of V. While the correspondence between these objects is easy to write down in terms of maps of cohomology groups, performing such calculations explicitly is more difficult and we go into some detail. In particular, we describe how cyclic algebras appear under this correspondence. We then move onto studying the vertical Brauer group attached to a fibration, and again show the correspondence between Azumaya algebras and elements of a certain Galois cohomology group. An example is given showing how this material relates to the calculations of Swinnerton-Dyer [44].

Finally, in Chapter 5 we turn from algebra to numerical work. Useful algorithms are described for checking local solubility of the equations, and for searching for small solutions. We present some worked examples of finding the Brauer–Manin obstruction, and show some surfaces which have no arithmetic Brauer–Manin obstruction but no small solutions. This suggests that perhaps the Brauer–Manin obstruction is not the only obstruction to the Hasse principle on diagonal quartic surfaces, and thus on K3 surfaces more generally.

At several points we will implicitly assume that the particular diagonal quartic surface under investigation has points in every completion of $\mathbb{Q}$. As this is an easily verified condition, and a necessary starting point for any search for rational points, this is a reasonable assumption and we will not always explicitly state it.

Most of the computations leading to this dissertation have been performed using the excellent number theory package PARI/GP, which is available freely under the GNU General Public License. Information on downloading and using PARI/GP is at `http://www.parigp-home.de`.

Some of the algorithms and results described here may be downloaded from `http://www.boojum.org.uk/maths/quartic-surfaces/`.

Chapter 2

Geometry of the surface

In this chapter, we review various facts about the geometry of the surface (1.1). Much of the geometry is that which applies generally to the class of *K3 surfaces*, of which our surface is an example; so we begin in Section 2.1 by gathering together some results about these surfaces. Section 2.2 discusses the geometry of fibrations over the projective line, and also includes a proof of the well-known fact on which the techniques used in the following chapters rely: that the Picard group of our surface is generated by the 48 straight lines on it. In Section 2.3 we show how fibrations on V, defined over the rational numbers, may be found.

> **Note:** In much of this chapter, we are concerned with complex surfaces. When we need to make a distinction between our surface (1.1) as a variety over $\mathbb{Q}$ and the corresponding variety over $\bar{\mathbb{Q}}$ or $\mathbb{C}$, we will refer clearly to the former variety as V and the latter as $\bar{V}$.

2.1 K3 surfaces

In this section we gather some well-known results about K3 surfaces. The concepts used in this section may all be found in Hartshorne [21]; for more detailed information about the classification of surfaces see the book by Beauville [3]. Algebraic geometry on surfaces is covered very well in [22].

A more analytic approach, including a large chapter on K3 surfaces, is given in [2].

2.1.1 Definition of K3 surfaces

Recall that a surface X has two important birational invariants: the *arithmetic genus* p_a, defined by

$$p_a(X) = \chi(X, \mathcal{O}_X) - 1 = h^2(X, \mathcal{O}_X) - h^1(X, \mathcal{O}_X);$$

and the *geometric genus* p_g, defined by

$$p_g(X) = h^0(X, \omega_X)$$

where $\omega_X = \bigwedge^2 \Omega_{X/k}$ is the canonical sheaf on X. In contrast to the situation for curves, these two quantities are not necessarily equal: we define the *irregularity* of X, written $q(X)$, to be the difference

$$q(X) = p_g(X) - p_a(X) = h^1(X, \mathcal{O}_X)$$

since by Serre duality [21, III, 7] we know that $p_g = h^2(X, \mathcal{O}_X)$.

Definition 2.1. A *K3 surface* is a surface with trivial canonical sheaf and irregularity $q = 0$.

Proposition 2.2. *The complex surface* $\bar{V}$ (1.1) *is a K3 surface.*

Proof. Any hypersurface of degree d in $\mathbb{P}^n$ has $\omega_X \cong \mathcal{O}_X(d-n-1)$ (see [21, II, 8.20.3]). Thus our particular surface has $\omega_{\bar{V}} \cong \mathcal{O}_{\bar{V}}$, that is, the canonical sheaf is trivial. To see that $H^1(\bar{V}, \mathcal{O}_{\bar{V}}) = 0$, we use the exact sequence of sheaves on $\mathbb{P}^3$

$$0 \to \mathcal{I}_{\bar{V}} \to \mathcal{O}_{\mathbb{P}^3} \to \mathcal{O}_{\bar{V}} \to 0$$

where $\mathcal{I}_{\bar{V}}$ is the ideal sheaf of $\bar{V}$. But $\mathcal{I}_{\bar{V}}$ is isomorphic to $\mathcal{O}_{\mathbb{P}^3}(4)$, so has trivial cohomology in dimension 2; and $\mathcal{O}_{\mathbb{P}^3}$ has trivial cohomology in dimension 1 [21, III, 5.1]. Thus the long exact sequence in cohomology gives

$H^1(\bar{V}, \mathcal{O}_{\bar{V}}) = 0$, as the cohomology of $\mathcal{O}_{\bar{V}}$ is the same taken on $\bar{V}$ as on $\mathbb{P}^3$. (In fact, this approach works for any complete intersection in projective space: see [21, III, Ex. 5.5].) □

2.1.2 Divisors

Here we state some properties of K3 surfaces which will be important in subsequent sections. In particular, we are interested in the Picard group of X; this turns out to be torsion-free and equal to the group of divisors modulo numerical equivalence, which makes computation in $\operatorname{Pic} X$ particularly simple.

Divisors are commonly defined in two different ways, as Weil divisors and as Cartier divisors; we will occasionally want to use both of these notions, so recall them now.

Definition 2.3. On a scheme X satisfying certain criteria (which certainly hold for a smooth projective variety), the group of *Weil divisors* is free group generated by the irreducible subschemes of codimension 1. Thus, on a surface, a prime Weil divisor is an irreducible curve, and a Weil divisor is a finite formal sum of irreducible curves. It is easy to define the *valuation* $v_D(f)$ of a rational function f at an irreducible divisor D, as the local ring $\mathcal{O}_{X,D}$ is a discrete valuation ring; hence we can define the Weil divisor associated to a function f by

$$(f) = \sum_D v_D(f) D$$

where all but finitely many of the $v_D(f)$ are non-zero. Two Weil divisors are said to be *linearly equivalent* if their difference is the divisor of a function, and the *Weil divisor class group* is defined to be the group of Weil divisors modulo linear equivalence.

Definition 2.4. On any scheme X, a *Cartier divisor* is a global section of the quotient sheaf $\mathcal{D}_X = \mathcal{K}_X^\times / \mathcal{O}_X^\times$. Here $\mathcal{K}_X$ is the sheaf of rings formed locally from $\mathcal{O}_X$ by inverting all the elements which are not zero-divisors; so for an integral scheme it is simply the sheaf of rational functions.

Hence on a variety a Cartier divisor can be described by a covering of open sets $\{U_\alpha\}$, together with rational functions f_α on each open set U_α, such that the restriction of f_α/f_β to $U_\alpha \cap U_\beta$ lies in $\mathcal{O}_X^\times(U^\alpha \cap U^\beta)$. Again we can define the divisor of a rational function f, this time simply by the quotient map $\mathcal{K}_X^\times \to \mathcal{K}_X^\times/\mathcal{O}_X^\times$. For Cartier divisors on an integral scheme, we immediately see that the class group is isomorphic to $H^1(X, \mathcal{O}_X^\times)$: this comes from the exact sequence in cohomology

$$\cdots \to H^0(X, \mathcal{K}_X^\times) \to H^0(X, \mathcal{K}_X^\times/\mathcal{O}_X^\times) \to H^1(X, \mathcal{O}_X^\times) \to H^1(X, \mathcal{K}_X^\times)$$

where, since the sheaf of rational functions is flabby, its first cohomology group is trivial. There is a straightforward correspondence between Cartier divisors and invertible sheaves on X, which shows that (at least when X is integral) the Cartier divisor class group is isomorphic to the Picard group $\operatorname{Pic} X$.

On a sufficiently nice scheme, such as a smooth projective variety, there is an isomorphism between the groups of Weil and Cartier divisors, and between the corresponding class groups [21, II, 6.11].

A notion of equivalence of divisors coarser than that of linear equivalence is given by algebraic equivalence.

Definition 2.5. Two divisors D_1, D_2 on a variety X are said to be *algebraically equivalent* if there exists a smooth curve C and a divisor D on $X \times C$ such that D_1, D_2 are the intersections of D with two fibres of the projection $X \times C \to C$.

It is clear that linearly equivalent divisors are algebraically equivalent (take $C = \mathbb{P}^1$). Algebraic equivalence is a geometric version of the topological concept of two cycles being homologous: in fact, on a variety over $\mathbb{C}$, the two notions coincide (see Griffiths & Harris [17, Lemma, page 462]).

Definition 2.6. The group of divisors modulo algebraic equivalence is called the *Néron–Severi* group of X and written $\mathrm{NS}(X)$. The subgroup of $\operatorname{Pic} X$ consisting of divisors algebraically equivalent to 0 is written $\operatorname{Pic}^0 X$; thus we have $\mathrm{NS}(X) = \operatorname{Pic} X / \operatorname{Pic}^0 X$.

Now let X be a smooth projective surface. Given any two irreducible curves D_1, D_2 in X, we can define their *intersection number* $D_1.D_2$. The construction is described in detail in [21, V, 1.1]. Briefly, if D_1 and D_2 intersect transversely, then their intersection number is the number of points of intersection; we then extend linearly to divisors which do not intersect transversely. This gives a symmetric bilinear form on $\operatorname{Div} X$. It can be shown that, if D_1 and D_1' are algebraically equivalent, then $D_1.D_2 = D_1'.D_2$ for all divisors D_2. Thus we have a symmetric bilinear form $\mathrm{NS}(X) \times \mathrm{NS}(X) \to \mathbb{Z}$.

Definition 2.7. An element of the (left or right) kernel of the intersection form, that is, a divisor having intersection number zero with every other divisor, is said to be *numerically equivalent* to 0; the subgroup of $\operatorname{Pic} X$ consisting of such divisors is written $\operatorname{Pic}^n X$.

By linearity, $\operatorname{Pic}^n X$ must contain all the torsion elements of $\mathrm{NS}(X)$; in fact, the converse is also true: $\operatorname{Pic}^n X$ consists of those divisors which are torsion in $\mathrm{NS}(X)$. (This is essentially due to the Riemann–Roch theorem: [29, V, Lemma 3.27] shows that $\operatorname{Pic}^n X / \operatorname{Pic}^0 X$ is finite, hence torsion.)

Let X be any projective K3 surface. For any divisor D on X, let $\mathcal{L}(D)$ denote the invertible sheaf associated to D. The Riemann–Roch theorem [21, V, 1.6] gives

$$\chi(X, \mathcal{L}(D)) = \frac{1}{2} D.D + 2. \tag{2.1}$$

We will write $\ell(D)$ for $\dim H^0(X, \mathcal{L}(D))$ and $s(D)$ for $\dim H^1(X, \mathcal{L}(D))$, the *superabundance* of D. It follows from Serre duality that

$$\chi(X, \mathcal{L}(D)) = \ell(D) - s(D) + \ell(-D).$$

If D is a non-zero effective divisor, then $-D$ is certainly not effective so $\ell(-D) = 0$. Let Π be the class of a plane section of X. If D is a non-zero effective divisor then $D.\Pi \geq 1$. Conversely, if $D.\Pi \geq 1$ then $-D$ cannot be equivalent to an effective divisor, so again $\ell(-D) = 0$.

If D is a non-singular curve, we can also control $s(D)$:

Lemma 2.8. *If D is a non-singular curve in X, then $H^1(X, \mathcal{L}(D)) = 0$.*

Proof. Let $i : D \to X$ be the inclusion map. We consider the exact sequence of sheaves on X

$$0 \to \mathcal{L}(-D) \to \mathcal{O}_X \to i_*\mathcal{O}_D \to 0$$

associated to the subscheme D. Tensoring this with $\mathcal{L}(D)$ and taking the long exact sequence in cohomology, we get

$$\begin{aligned} \cdots \to H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{L}(D)) \to H^1(X, \mathcal{L}(D) \otimes i_*\mathcal{O}_D) \to \\ \to H^2(X, \mathcal{O}_X) \to H^2(X, \mathcal{L}(D)) \to \cdots. \end{aligned} \tag{2.2}$$

Now X has irregularity 0, and so $H^1(X, \mathcal{O}_X) = 0$. We also know that $H^2(X, \mathcal{O}_X)$ has dimension 1 and that $H^2(X, \mathcal{L}(D)) = 0$, both by Serre duality. On the other hand, Proposition 8.20 of [21, II] states that

$$\omega_D \cong \omega_X \otimes \mathcal{L}(D) \otimes \mathcal{O}_D;$$

in our case this reduces to $\Omega_D \cong \mathcal{L}(D) \otimes \mathcal{O}_D$. But now

$$\begin{aligned} H^1(X, \mathcal{L}(D) \otimes i_*\mathcal{O}_D) &\cong H^1(D, \mathcal{L}(D) \otimes O_D) \\ &\cong H^1(D, \Omega_D) \\ &\cong H^0(D, \mathcal{O}_D) \text{ by Serre duality} \end{aligned}$$

so $H^1(X, \mathcal{L}(D) \otimes i_*\mathcal{O}_D)$ has dimension 1. Putting this into the exact sequence (2.2), we get the desired result. □

For any effective divisor D, we know that the arithmetic genus $p_a(D)$ satisfies $2p_a(D) - 2 = D.D$ and we may use this to define $p_a(D)$ when D is not effective [21, V, Ex. 1.3].

We now put all these facts together into the following useful form of the Riemann–Roch theorem:

Proposition 2.9. *Let X be any K3 surface, and let Π be a very ample divisor on X. If D is an effective divisor on X or, more generally, any divisor such that $D.\Pi > 0$, then the following inequality holds:*

$$\ell(D) \geq p_a(D) + 1 = \frac{1}{2} D.D + 2.$$

If D is equivalent to a non-singular curve, then equality holds. □

In particular, non-singular rational curves are isolated, and non-singular curves of genus 1 always lie in pencils.

We now show how the various notions of equivalence for divisors fit together on a K3 surface.

Proposition 2.10. *On a K3 surface X over $\mathbb{C}$, the following notions of equivalence of divisors are the same:*

1. *linear equivalence;*

2. *algebraic equivalence;*

3. *homology;*

4. *numerical equivalence.*

Proof. Firstly, we have already stated that algebraic equivalence and homology are the same. Now the exponential sequence of (analytic) sheaves

$$0 \to \mathbb{Z} \to \mathcal{O}_X \xrightarrow{\exp} \mathcal{O}_X^\times \to 0$$

gives rise to an exact sequence in cohomology

$$H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X^\times) \xrightarrow{\alpha} H^2(X, \mathbb{Z})$$

where the map α associates to a divisor in $\operatorname{Pic} X \cong H^1(X, \mathcal{O}_X^\times)$ its Poincaré dual cohomology class [22, 3.3]. So the kernel of α consists of the divisors homologous, and so algebraically equivalent, to 0; and the image of α is isomorphic to the Néron–Severi group of X. (In complex geometry, this is often used as the definition of the Néron–Severi group.) But for a K3 surface, $H^1(X, \mathcal{O}_X) = 0$; thus α gives an isomorphism from $\operatorname{Pic} X$ to $\operatorname{NS}(X)$.

To show that algebraic and numerical equivalence coincide, we must establish that $\operatorname{Pic} X$ is torsion-free. Suppose that D is a divisor on X such that nD is principal, for some positive integer n. Then $D.D = 0$, and putting this into the Riemann–Roch formula (2.1) gives $\chi(X, \mathcal{L}(D)) = 2$, so either D

or $-D$ is equivalent to an effective divisor. But if D is a non-zero effective divisor, then nD cannot be principal. The same holds for $-D$. So $D = 0$, and hence $\operatorname{Pic} X$ is torsion-free. $\square$

Finally, the rank of $\operatorname{Pic} X$ is easily bounded by Noether's formula (see [22], 1).

Proposition 2.11. *Let X be a K3 surface over $\mathbb{C}$; then $\operatorname{Pic} X$ is free of rank no more than 20.*

Proof. Using all the symmetries we get from Hodge theory and Serre duality, the definition of a K3 surface gives

$$h^{0,0} = h^{2,0} = h^{0,2} = h^{2,2} = 1$$
$$h^{1,0} = h^{0,1} = h^{1,2} = h^{2,1} = 0$$

and therefore Betti numbers $b_0 = b_4 = 1$, $b_1 = b_3 = 0$. Now Noether's formula shows that the topological Euler characteristic of X is 24, so $b_2 = 22$ and therefore $h^{1,1} = 20$. But the image of $\operatorname{Pic} X$ in $H^2(X, \mathbb{Z})$ lies in $H^{1,1}(X)$ [22, 3.3], so has rank at most $h^{1,1} = 20$. $\square$

2.2 Fibrations

Here we discuss fibrations of surfaces over curves. In particular, we are interested in fibrations of our surface V (1.1) over $\mathbb{P}^1$, where the fibres are curves of genus one. Some information on fibrations may be found in [2] and [22]; a more detailed treatment appears in Silverman's book on elliptic curves [39], which is aimed at the study of elliptic surfaces with a section but contains much useful information for our situation.

2.2.1 Divisors on fibrations

It will be helpful to have a good understanding of the theory of divisors on fibrations, so here we gather some relevant facts. In this section, X is any smooth complete surface over a field k, C is a smooth complete curve over k, and $\pi : X \to C$ is a non-constant morphism. If t is a point of C, we write X_t for the fibre $X \times_C t$. We will be particularly interested in the generic fibre X_η, where η is the generic point of C.

Following [39], we make the following definitions.

Definition 2.12. A prime divisor on X is *fibral* if its image under π consists of a finite number of points, and *horizontal* otherwise, that is, when the image is the whole of C.

For each point t of C, there is a natural map of groups from $\operatorname{Pic} X$ to $\operatorname{Pic} X_t$. This arises from the map of sheaves $\mathcal{O}_X^\times \to i_*\mathcal{O}_{X_t}^\times$, where i is the inclusion map $X_t \to X$; thus we have

$$H^1(X, \mathcal{O}_X^\times) \to H^1(X, i_*\mathcal{O}_{X_t}^\times)$$

where the left-hand group is $\operatorname{Pic} X$; we claim that the right-hand group is naturally isomorphic to $\operatorname{Pic} X_t$. If t is a closed point of C, then i is a closed immersion and hence i_* an exact functor (see [28, Corollary 8.4]). If t is η, the generic point of C, then the claim follows from this lemma, when combined with the Leray spectral sequence:

Lemma 2.13. *Let $j : X_\eta \to X$ be the inclusion of the generic fibre. Then $R^1 j_* \mathbb{G}_\mathrm{m} = 0$.*

Proof. See Lemma 4.4.1 of [11]. □

We study this map of Picard groups in more detail, and show that the kernel is the same in all cases.

First let t be a closed point of C. Then the fibre X_t is a curve over k. The map i is a closed immersion, so $\mathcal{O}_X \to i_*\mathcal{O}_{X_t}$ is surjective, and hence so is $\mathcal{O}_X^\times \to i_*\mathcal{O}_{X_t}^\times$. We will describe the map of Picard groups first in terms of Cartier divisors.

A Cartier divisor D on X is a covering of X by pieces of rational functions; suppose that X_t is not contained in the support of D: that is, the rational functions have no zeros or poles along the curve X_t, or equivalently that the functions are invertible elements of $\mathcal{O}_{X,X_t}$. Then restricting the functions to

X_t gives a Cartier divisor on X_t. This gives a map from most of $\operatorname{Div} X$ into $\operatorname{Div} X_t$. It is easy to see that this map respects linear equivalence. Moreover, every divisor is equivalent to one whose support does not contain X_t; so we have defined a natural map

$$\operatorname{Pic} X \to \operatorname{Pic} X_t.$$

Of course, this map also admits a description in terms of Weil divisors: any Weil divisor whose support does not contain X_t intersects X_t is a finite number of points; the image of the divisor in $\operatorname{Pic} X_t$ is just those points, taken with appropriate intersection multiplicities.

Now consider the generic fibre X_η. This is a curve over $k(C)$. The function field of X_η is the same as that of X. The sheaf of regular functions on X_η is obtained from $\mathcal{O}_X$ by inverting all the functions lying in the inverse image $\pi^*\mathcal{O}_C$; so, algebraically, it is just a localisation of $\mathcal{O}_X$. Several useful properties follow immediately: the points of X_η are a subset of those of X, and in fact the closed points of X_η correspond precisely to the horizontal divisors on X. Note that X_η may well not have any $k(C)$-valued points: such a point would be a horizontal divisor D on which π restricts to an isomorphism $D \to C$, that is, a section of π. In general, π gives a map $D \to C$ of some degree, often greater than 1; so D corresponds to a point of X_η whose residue field is some finite extension of $k(C)$.

Let j denote the inclusion $X_\eta \to X$, and let U be an open set in X. Then U is the complement of finitely many closed subschemes $\{Z_i\}$ in X, which we can split into points, fibral divisors and horizontal divisors. The inverse image $j^{-1}U$ should be an open set in X_η, that is, the complement of finitely many horizontal divisors; and following the definitions through shows that in fact $j^{-1}U$ is simply the complement of those Z_i which are horizontal divisors. Knowing how j^{-1} acts on open sets allows us to describe the induced map on Picard groups.

A Cartier divisor on X is a covering of X by open sets U_α, together with rational functions f_α on each U_α such that f_α/f_β is a regular function on $U_\alpha \cap U_\beta$ for all α, β. On the other hand, a Cartier divisor on X_η requires that the open sets U_α all be complements of finite sets of *horizontal* divisors (as opposed to complements of finite sets of arbitrary divisors); but now the f_α/f_β only have to be regular on X_η: that is, the divisor (f_α/f_β) may have fibral components but not horizontal ones. So, given a Cartier divisor on X, we can turn it into a Cartier divisor on X_η just by replacing each open set U_α by $j^{-1}U_\alpha$; this process might mean that the f_α/f_β are no longer regular on the enlarged intersections $U_\alpha \cap U_\beta$, but we can only have introduced problems along fibral divisors, which as remarked does not affect whether the f_α/f_β is regular as a function on X_η.

On Weil divisors, the map is entirely obvious: a horizontal divisor maps to itself, and a fibral divisor maps to zero.

Proposition 2.14. *The map* $\operatorname{Pic} X \to \operatorname{Pic} X_\eta$ *is surjective; its kernel is generated by the irreducible components of the fibres of* π.

Proof. Let j denote the inclusion $X_\eta \to X$. The sheaf $j_*\mathcal{O}_{X_\eta}$ consists of those rational functions on X which are regular on X_η, that is, whose divisors contain only fibral components. So the map $\mathcal{O}_X \to j_*\mathcal{O}_{X_\eta}$ is injective. As $j_*\mathcal{O}_{X_\eta}^\times$ is a subsheaf of the sheaf $\mathcal{K}_X$ of rational functions on X, so we may regard the quotient sheaf

$$\mathcal{F} = j_*\mathcal{O}_{X_\eta}^\times/\mathcal{O}_X^\times$$

as a subsheaf of $\mathcal{K}_X^\times/\mathcal{O}_X^\times$; but that is the sheaf of divisors, $\mathcal{D}_X$. In fact $\mathcal{F}$ consists precisely of the divisors of functions regular on X_η, that is, the (locally) fibral divisors. We get an exact sequence in cohomology

$$H^0(X,\mathcal{F}) \to H^1(X,\mathcal{O}_X^\times) \to H^1(X, j_*\mathcal{O}_{X_\eta}^\times) \to H^1(X,\mathcal{F})$$

where the first term is the group of fibral divisors, and the last term is zero because $\mathcal{F}$ is a direct summand of the sheaf of divisors, which has trivial 1-dimensional cohomology (see Lemma 4.3). The middle two terms are $\operatorname{Pic} X$ and $\operatorname{Pic} X_\eta$ respectively, and the kernel of the map between them therefore is the subgroup of $\operatorname{Pic} X$ generated by the fibral divisors. $\square$

When the fibration π is fixed, we will refer to the kernel of the map $\operatorname{Pic} X \to \operatorname{Pic} X_\eta$ as the *vertical* Picard group, and write it as $\operatorname{Pic}_{\mathrm{vert}}$. This group will be further studied in Section 4.4, where we will be investigating the vertical Brauer group attached to a fibration.

2.2.2 The Picard group of the surface

The information about fibrations in the previous section allows us to prove the following well-known result, which describes precisely the Picard group of our surface V (1.1).

Proposition 2.15. *The Picard group of the complex variety $\bar{V}$ is a free Abelian group of rank 20, and is generated by the classes of the 48 straight lines on $\bar{V}$.*

As we are only concerned here with the structure of $\bar{V}$ as a complex variety, the coefficients a_i make no difference and to prove Proposition 2.15 we may assume that the equation of the surface is

$$X_0^4 - X_1^4 = X_2^4 - X_3^4. \tag{2.3}$$

Let Λ denote the subgroup of $\operatorname{Div} \bar{V}$ generated by the 48 lines. We must show that the image of Λ in $\operatorname{Pic} \bar{V}$ is the whole of $\operatorname{Pic} \bar{V}$.

Firstly, it is a simple matter to calculate the intersection numbers of the 48 lines: two distinct straight lines intersect with multiplicity 1 or not at all, and the self-intersection of each line is -2. This allows us to compute the subgroup of Λ^0 of Λ consisting of those divisors numerically equivalent to 0, and hence (by Proposition 2.10) linearly equivalent to 0. The quotient Λ/Λ^0 turns out to have rank 20, so by Proposition 2.11 the image of Λ is a subgroup of finite index in $\operatorname{Pic} \bar{V}$.

Lemma 2.16.
1. *The determinant of the intersection form on the image of Λ is -64.*
2. *The index of the image of Λ in $\operatorname{Pic} \bar{V}$ is a power of 2.*

Proof. The first statement comes from a simple computation, given that we already know the intersection numbers of the 48 lines. For the second statement, observe that the index of the image Λ in $\operatorname{Pic}\bar{V}$ must divide the determinant of the image of Λ. □

We will use the fibration described in [44] and some standard results on elliptic curves to show that in fact the image of Λ is the whole of $\operatorname{Pic}\bar{V}$.

The fibration is defined as follows: we rewrite (2.3) as

$$(X_0^2 + X_1^2)(X_0^2 - X_1^2) = (X_2^2 + X_3^2)(X_2^2 - X_3^2)$$

which is then a covering in the obvious way of the quadric surface defined by the equation

$$(Y_0 + Y_1)(Y_0 - Y_1) = (Y_2 + Y_3)(Y_2 - Y_3).$$

Now this surface is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, so has two pencils of straight lines: we will use the one defined by

$$y(Y_0 + Y_1) = z(Y_2 + Y_3) \quad \text{and} \quad z(Y_0 - Y_1) = y(Y_2 - Y_3)$$

which, when lifted to $\bar{V}$, gives us the pencil of curves of genus 1 with equation

$$y(X_0^2 + X_1^2) = z(X_2^2 + X_3^2) \quad \text{and} \quad z(X_0^2 - X_1^2) = y(X_2^2 - X_3^2). \tag{2.4}$$

This is the fibration over $\mathbb{P}^1$ which we will now use to investigate the structure of $\operatorname{Pic}\bar{V}$. As in the previous section, we write η for the generic point of $\mathbb{P}^1$ and $\operatorname{Pic}_{\text{vert}}$ for the vertical Picard group, that is, the subgroup of $\operatorname{Pic}\bar{V}$ generated by the irreducible components of the fibres of π. The map from $\operatorname{Pic}\bar{V}$ to the Picard group of the generic fibre of this fibration gives us, by Proposition 2.14, an exact sequence

$$0 \to \operatorname{Pic}_{\text{vert}} \to \operatorname{Pic}\bar{V} \to \operatorname{Pic}\bar{V}_\eta \to 0$$

where $\operatorname{Pic}_{\text{vert}}$ is generated by the irreducible components of the fibres, and $\bar{V}_\eta$ is a curve of genus 1 over $\mathbb{C}(t)$ (where $t = y/z$).

Lemma 2.17. $\operatorname{Pic}_{\text{vert}}$ *is contained in the image of* Λ.

Proof. Looking at the partial derivatives of the equations (2.4) reveals that the singular fibres occur when y/z is equal to 0, ± 1, $\pm i$ and ∞. The fibres can then be found by substituting these values of y/z into (2.4), and we find that each of the singular fibres consists of four straight lines forming a skew quadrilateral. □

We must now show that the image of Λ in $\operatorname{Pic} \bar{V}_\eta$ is the whole of $\operatorname{Pic} \bar{V}_\eta$. We write Λ_{vert} for the subgroup of Λ generated by the irreducible components of the fibres. Further computations (using the methods described in Section 3.2) reveal the following facts.

Lemma 2.18. *1. the image in* $\operatorname{Pic} \bar{V}$ *of* Λ_{vert}*, that is,* $\operatorname{Pic}_{\mathrm{vert}}$*, has rank* 19*;*

2. the torsion part of the quotient $\Lambda/(\Lambda^0 + \Lambda_{vert})$ *is isomorphic to* $(\mathbb{Z}/4\mathbb{Z})^2$*;*

3. the intersection number of any element of Λ *with a fibre is even.*

□

The first of these facts means that the image of Λ in $\operatorname{Pic} \bar{V}_\eta$ has rank 1; and, as the image of Λ is of finite index, therefore $\operatorname{Pic} \bar{V}_\eta$ has rank 1. Now the degree map on $\operatorname{Pic} \bar{V}_\eta$ gives an exact sequence

$$0 \to \operatorname{Pic}^0 \bar{V}_\eta \to \operatorname{Pic} \bar{V}_\eta \xrightarrow{\deg} \mathbb{Z}$$

and we must show that $\operatorname{Pic}^0 \bar{V}_\eta$ is contained in the image of Λ, and further that the image of $\Lambda \to \operatorname{Pic} \bar{V}_\eta \to \mathbb{Z}$ is the same as the image of $\operatorname{Pic} \bar{V}_\eta$ in $\mathbb{Z}$.

It follows from the first of the above observations that the rank of $\operatorname{Pic} \bar{V}_\eta$ is 1. The degree map on a curve is non-constant; therefore the degree 0 part $\operatorname{Pic}^0 \bar{V}_\eta$ is finite and is just the torsion subgroup of $\operatorname{Pic} \bar{V}_\eta$. It is at least as large as $(\mathbb{Z}/4\mathbb{Z})^2$, since that is the part generated by Λ; we must show that this is the whole of $\operatorname{Pic}^0 \bar{V}_\eta$. On the other hand, $\operatorname{Pic}^0 \bar{V}_\eta$ is isomorphic to the group of $\mathbb{C}(t)$-valued points on the Jacobian of $\bar{V}_\eta$, which [44] shows may be described by the equation

$$E : Y^2 = X(X + (t^2 - 1)^2)(X + (t^2 + 1)^2). \tag{2.5}$$

Lemma 2.19. *The Mordell–Weil group of the curve* (2.5) *over* $\mathbb{C}(t)$ *is isomorphic to* $(\mathbb{Z}/4\mathbb{Z})^2$.

Proof. By the second statement of Lemma 2.18, the Mordell–Weil group of E contains a subgroup isomorphic to $(\mathbb{Z}/4\mathbb{Z})^2$. By the second statement of Lemma 2.16, the index of this subgroup in the whole group is a power of 2; so it suffices to find the 4-division points of E which are not 2-division points, and show that they are not divisible by 2.

Hand calculation quickly gives the non-trivial 4-division points to be

- four points with $X = \pm(t^4 - 1)$, which double to give $(0, 0)$;
- four points given by $X = -(t^2 - 1)(t \pm i)^2$, which when doubled give $(-(t^2 - 1)^2, 0)$;
- four points given by $X = -(t^2 + 1)(t \pm 1)^2$, which when doubled give $(-(t^2 + 1)^2, 0)$.

A point P on an elliptic curve having rational 2-division points P_1, P_2, P_3 is divisible by 2 if and only if the three quantities $X(P) - X(P_i)$ are all squares [38, X, §1]; but the points listed clearly do not satisfy this condition. $\square$

To complete the proof of Proposition 2.15, we must show that the image of Λ under the degree map $\operatorname{Pic} \bar{V}_\eta \to \mathbb{Z}$ is the whole of the image of $\operatorname{Pic} \bar{V}_\eta$. The degree map is the same as the intersection number with a fibre; as stated above, calculation shows that the smallest non-zero intersection number of an element of Λ with a fibre is 2. Therefore the image of $\operatorname{Pic} \bar{V}_\eta$ under the degree map may only be either $\mathbb{Z}$ or $2\mathbb{Z}$.

Lemma 2.20. *The image of the degree map* $\operatorname{Pic} \bar{V}_\eta \to \mathbb{Z}$ *is* $2\mathbb{Z}$.

Proof. Suppose that $\bar{V}_\eta$ contained a divisor of degree 1; the Riemann–Roch theorem shows that such a divisor is equivalent to an effective divisor of degree 1: that is, a $\mathbb{C}(t)$-valued point of $\bar{V}_\eta$. Then $\bar{V}_\eta$ would be isomorphic to its Jacobian E (2.5). To show that this is not the case, we use the well-known theory of 2-coverings (see [38, Chapter X]). The group $H^1(\mathbb{C}(t), E[2])$ classifies the 2-coverings of E; as all the 2-division points are defined over

$\mathbb{C}(t)$, we have $E[2] \cong \mu_2^2$ and hence $H^1(\mathbb{C}(t), E[2]) \cong (\mathbb{C}(t)^\times/(\mathbb{C}(t)^\times)^2)^2$. There is a coboundary map from $E(\mathbb{C}(t))/2E(\mathbb{C}(t))$ to $(\mathbb{C}(t)^\times/(\mathbb{C}(t)^\times)^2)^2$ given by

$$P \mapsto (X(P), X(P) + (t^2-1)^2)$$

and those 2-coverings which have a $\mathbb{C}(t)$-valued point are those lying in the image of this map. But, as stated in [44], equation (23), $\bar{V}_\eta$ is a 2-covering of E associated to the element $(t^4-1, t(t^2-1))$. On the other hand, the points of E are listed above and their images are

$$(1,1), (t^4-1, t^2-1), (t^2-1, t(t^2-1)), (t^2+1, t)$$

which form a 4-group not containing $(t^4-1, t(t^2-1))$. Hence $\bar{V}_\eta$ has no $\mathbb{C}(t)$-valued point. $\square$

Therefore $\operatorname{Pic} \bar{V}_\eta$ is indeed generated by the image of Λ, and this completes the proof of Proposition 2.15.

2.2.3 Picard groups over $\mathbb{Q}$

If X is an arbitrary variety over a number field k, then we can define $\operatorname{Pic} X$ to be the group of divisors on X modulo principal divisors. Here a divisor on X is a closed subscheme of codimension 1 which is defined over k. This is subtly different from $H^0(k, \operatorname{Pic} \bar{X})$, which consists of those divisor classes fixed by the Galois action of $\bar{k}/k$: for it is quite possible for a divisor class to be fixed by the Galois action but contain no divisors which are themselves fixed. This distinction is rather tiresome, but fortunately a standard result shows that in the interesting cases, that is, where X has a point in each completion k_v of k, the two groups $\operatorname{Pic} X$ and $H^0(k, \operatorname{Pic} \bar{X})$ are the same.

Proposition 2.21. *Let X be a smooth variety over a number field k, and suppose that $X(k_v) \neq \emptyset$ for each completion k_v of k. Then* $\operatorname{Pic} X = H^0(k, \operatorname{Pic} \bar{X})$.

Proof. Let D be a divisor on $\bar{X}$ in a class fixed by the action of $\operatorname{Gal}(\bar{k}/k)$. If Π denotes a very ample divisor on X, then there exists an integer m such that $D + m\Pi$ is effective; and $D + m\Pi$ is equivalent to a k-rational divisor if and only if D is; thus to prove the proposition we may assume that D is effective. We may also assume that the linear system $|D|$ has no fixed part: for if it does, then the fixed part is Galois-invariant and we may subtract it. Finally, if $\ell(D) = 1$ then D is the only effective divisor in its equivalence class, and is therefore defined over k; so we now assume that $\ell(D) > 1$.

Write L for $|D|$. The linear system L is parametrised by the scheme $\mathbb{P}(\mathcal{L}(D))$, making it by definition a *Severi–Brauer* variety. Such varieties were shown by Châtelet [7] to satisfy the Hasse principle. We will show that L contains a divisor defined over k_v for each v, and deduce that L contains a divisor defined over k.

Fix a place v of k. By the hypothesis, there is a point in $X(k_v)$ for each v. In fact, in a neighbourhood of such a point a local parametrisation shows that there are infinitely many more. We choose x_v to be a point of $X(k_v)$ which is not one of the finitely many base points of L. As $\dim L \geq 1$, there is some divisor D' in L, defined over a finite extension of k_v, on which x_v lies. If D' is defined over k_v, we are finished; otherwise, note that x_v also lies on each conjugate of D' over k_v; we conclude that these conjugates do not span the whole linear system L, for if they did then x_v would be a base point of L. We therefore replace L by the linear system spanned by the conjugates of D', which has dimension at least 1 but strictly less than that of L, and start again. As the dimension of L decreases each time, this process must eventually find a D' in the linear system $|D|$ and defined over k_v. □

In this dissertation we are always primarily concerned with surfaces V which are everywhere locally soluble: for otherwise there is no reason to study the Brauer–Manin obstruction. Therefore we will sometimes assume that $\operatorname{Pic} V$ and $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$ are the same without explicitly stating this.

2.3 Fibrations on V

Some K3 surfaces, in particular our surface $\bar{V}$ (1.1), may be given the structure of a fibration over $\mathbb{P}^1$, with fibres being curves of genus 1. When such a fibration is defined over the rational numbers, it may be used as in [44] to obtain information about the Brauer group of V. In this section we study such fibrations. Here V will always denote the surface considered as a variety over the rational numbers, and $\bar{V}$ the same surface as a variety over $\bar{\mathbb{Q}}$.

2.3.1 Finding fibrations

We are interested in finding fibrations $V \to \mathbb{P}^1$ defined over $\mathbb{Q}$. The calculations described in Chapter 3 allow the computation of $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$, the part of the Picard group which is defined over $\mathbb{Q}$; when V has a point in each completion $\mathbb{Q}_v$ of $\mathbb{Q}$, this is equal to $\operatorname{Pic} V$. The existence of fibrations on K3 surfaces over $\mathbb{C}$ has been much studied; in particular, an account is given in [33], where it is proved that a K3 surface has a fibration in curves of genus 1 if and only if the intersection form on the Picard group represents zero. The version of the Riemann–Roch theorem stated above in Proposition 2.9 already shows that any nonsingular curve of genus 1 occurs as part of a linear system of dimension 1; and, as such curves have self-intersection zero, the linear system has no base points; thus any nonsingular curve of genus 1 defines a fibration over $\mathbb{P}^1$. The first step in [33] is to turn this into a more useful criterion:

Lemma 2.22. *Let D be a divisor class on V such that $D^2 = 0$ and D has non-negative*[1] *intersection number with all effective divisors. Then D is equal to mF, where m is a positive integer and F a divisor such that the linear system $|F|$ defines a fibration $V \to \mathbb{P}^1$.*

Proof. See [33]. □

In fact the second condition is simpler than it might appear. In the language of [2, VIII], we require that D lie in the closure of the *Kähler cone* of divisors on V; but Corollary 3.8 there shows that the Kähler cone is characterised by the fact that $D.C$ is positive for every *rational* curve C on V.

[1] In fact, the statement in [33] requires that D have strictly positive intersection number with all effective divisors. This is clearly wrong: for a start, $D.C = 0$ where C is any component of a fibre. The proof, though, assumes that the intersection number is merely non-negative.

The second step is to show that, by using certain automorphisms of the Picard lattice called *reflections*, any divisor D satisfying $D^2 = 0$ may be transformed into one satisfying the conditions of the lemma. If C is a rational curve on V, then the reflection s_C is defined by

$$s_C(D) = D + (D.C)C.$$

One checks that this defines an involution of $\operatorname{Pic} \bar{V}$ which preserves intersection numbers. This part of the proof does not immediately work over $\mathbb{Q}$, but can be adapted to do so. I am indebted to Professor Shepherd-Barron for indicating this method of proof.

Proposition 2.23. *The surface V has a fibration $V \to \mathbb{P}^1$ in curves of genus 1, defined over $\mathbb{Q}$, if and only if the intersection form on $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$ represents zero non-trivially.*

Proof. We follow the proof of [33, §6, Theorem 1]. Let D be a non-trivial element of $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$ such that $D^2 = 0$. Then $D.\Pi$ cannot equal zero, by the Hodge index theorem, so we assume (replacing D by $-D$ if necessary) that $D.\Pi > 0$. Then D is effective, by the Riemann–Roch theorem (Proposition 2.9).

If D does not satisfy the conditions of Lemma 2.22, then there is a rational curve C on V such that $D.C < 0$. Let $C_{i,j}$ be the conjugates of C over $\mathbb{Q}$, numbered such that $\{C_{1,j}\}$ form one connected component, $\{C_{2,j}\}$ another, and so on. Each connected component is defined over the same finite extension $K/\mathbb{Q}$. We will now use the theory of the fundamental cycle, as introduced in [1]. Consider first the connected component $\{C_{1,j}\}$. As D is defined over $\mathbb{Q}$, we have that $D.C_{1,j} < 0$ for all j. Therefore, by Proposition 2 of [1], the intersection form on the components $\{C_{1,j}\}$ is negative definite; in other words, this connected component is an A-D-E curve, as defined in [2, III.3]. The *fundamental cycle* Z_1 of this connected component is defined to be the unique minimal effective divisor

$$Z_1 = \sum_j a_j C_{1,j}$$

such that Z_1 has non-positive intersection number with each $C_{1,j}$. It turns out that $Z_1^2 = -2$ (see [2, III, Proposition 3.6]). Also, Z_1 is defined over K: for otherwise its conjugates over K would have the same properties, contradicting uniqueness. Similarly we define Z_i for each connected component $\{C_{i,j}\}$; it is clear that the Z_i are the complete set of conjugates over $\mathbb{Q}$ of Z_1.

Note that $D.Z_1 < 0$: otherwise, we would have $\sum_j a_j < 0$, so $Z_1.\Pi < 0$, contradicting that Z_1 is effective.

Now the proof proceeds as in [33]. We replace D by

$$D' = D + (D.Z_1)\sum_i Z_i$$

which is the result of applying the reflections s_{Z_i} in turn: as the Z_i do not intersect, these reflections commute. Then D' is defined over $\mathbb{Q}$. Since reflections preserve intersection number and the positive cone, we still have $(D')^2 = 0$ and $D'.\Pi > 0$. Moreover,

$$D'.\Pi = D.\Pi + (D.Z_1)\sum_i Z_i.\Pi < D.\Pi$$

as each Z_i is effective. Repeating this procedure, we must eventually reach a D which satisfies the conditions of Lemma 2.22. □

As the lattice $\operatorname{Pic} V$ is of a very specific type, we can give more detail about exactly when a pencil of curves of genus 1 exists.

We begin with a simple lemma about lattices.

Definition 2.24. A *lattice* is a free Abelian group equipped with a non-degenerate symmetric bilinear form, written $(\quad,\quad)$. The *determinant* of a lattice Λ, written $\det \Lambda$, is the determinant of the matrix (e_i, e_j) where (e_i) is any basis for Λ.

Lemma 2.25. *Let Λ be a lattice. Suppose that a finite group G acts on Λ preserving the bilinear form. Then the determinant of $H^0(G,\Lambda)$ divides $|G|^{\dim \Lambda} \det \Lambda$.*

Proof. We write A for $H^0(G,\Lambda)$. Denote by $A^\perp$ the orthogonal complement of A, that is, the group of elements x of Λ such that $(x,y) = 0$ for all y in A.

Since the bilinear form is non-degenerate, A and $A^{\perp}$ have trivial intersection. Now, as vector spaces, we have

$$\Lambda \otimes \mathbb{Q} = (A \otimes \mathbb{Q}) \oplus (A^{\perp} \otimes \mathbb{Q})$$

essentially by the Gram–Schmidt algorithm. We will show that $|G|\Lambda$ is contained in $A \oplus A^{\perp}$, and hence of finite index in $A \oplus A^{\perp}$.

Let x be any element of Λ; then, as the action of G preserves the bilinear form, $x - gx$ lies in $A^{\perp}$ for all $g \in G$. Summing over all g gives

$$|G|x - Nx \in A^{\perp}$$

where Nx denotes $\sum_{g \in G} gx$. But Nx lies in A, so therefore $|G|x$ is in $A + A^{\perp}$.

This shows that $|G|\Lambda$ is of finite index in $A \oplus A^{\perp}$. Therefore

$$\begin{aligned} \det(A \oplus A^{\perp}) &\quad \text{divides} \quad \det |G|\Lambda \\ \text{i.e. } \det A \times \det A^{\perp} &\quad \text{divides} \quad |G|^{\dim \Lambda} \det \Lambda \\ \text{so } \det A &\quad \text{divides} \quad |G|^{\dim \Lambda} \det \Lambda. \end{aligned}$$

□

We use this lemma to find the discriminant of the intersection form, which by definition is the determinant of the lattice $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$.

Corollary 2.26. *Let ρ denote the rank of $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$. If $\rho = 1$, then the determinant of $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$ is 4. If $\rho > 1$, then the determinant of $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$ is of the form $(-1)^{\rho+1} 2^k$ for some integer k.*

Proof. If $\rho = 1$ then $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$ is generated by the class Π of a plane section, which has self-intersection 4.

Suppose that $\rho > 1$. We shall see in Chapter 3 that the Galois action on $\operatorname{Pic} \bar{V}$ factors through a finite group G which is a subgroup of a certain group Γ of order 2^8. The determinant of $\operatorname{Pic} \bar{V}$ is -2^6, as is easily found by writing down a set of generators. Lemma 2.25 shows that the determinant of $H^0(G, \operatorname{Pic} \bar{V})$ divides $-64 \times 2^{8 \times 20}$; and the Hodge index theorem gives the sign. □

Corollary 2.27. *Let V be a diagonal quartic surface, and let ρ denote the rank of* $\operatorname{Pic} V$.

- *If $\rho = 1$, then V does not have a fibration in curves of genus* 1.
- *If $\rho = 2$, then V has a fibration in curves of genus* 1 *if and only if* $-\det H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$ *is a square.*
- *If $\rho \geq 3$, then V always has a fibration in curves of genus* 1.

Proof. By Proposition 2.23, we must decide when the intersection form on $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$ represents 0.

The cases $\rho = 1, 2$ are trivial. For $\rho \geq 5$, by [36, Chapter IV, 3.2, Corollary 2], all we need show is that the form is indefinite; but this is true, as the discriminant is negative. This leaves $\rho = 3, 4$.

If $\rho = 3$, then [36, Chapter IV, 3.2, Corollary 3] shows that it is enough to show that the intersection form represents 0 in $\mathbb{Q}_v$ for all v *except one.* But the discriminant is a unit at all odd primes, so the form does represent 0 in all $\mathbb{Q}_p$ for $p \neq 2$, and also in $\mathbb{R}$. Therefore it represents 0 in $\mathbb{Q}$.

If $\rho = 4$, then we must show that the intersection form represents 0 in every $\mathbb{Q}_v$. In $\mathbb{Q}_p$, p an odd prime, and $\mathbb{R}$ this is trivial. In $\mathbb{Q}_2$, by [36, Chapter IV, 2.2, Theorem 6] it is enough to show that the discriminant is not a square in $\mathbb{Q}_2$. But the determinant is -1×2^k for some k; and -1 and 2 are independent elements of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ (see, for example, [36, Chapter II, 3.3, Corollary to Theorem 4]). Hence the discriminant is not a square in $\mathbb{Q}_2$, and the result follows. □

2.3.2 Finding the singular fibres

Suppose that we are given an element $F \in \operatorname{Pic} \bar{V}$ which is the class of the fibres of a fibration $V \to \mathbb{P}^1$. In order to study the vertical Brauer group attached to this fibration (see Section 4.4), we need to know generators for the group $\operatorname{Pic}_{\text{vert}}$, that is, we must find the irreducible components of each singular fibre. It is possible, though rather messy, to write down an explicit formula for the morphism from V to $\mathbb{P}^1$; and given such a formula, one can solve certain equations in partial derivatives to find the singular fibres. However, there is a more efficient way to find these fibres, which we now describe.

The possible structures which can be taken by singular fibres of an elliptic fibration are described by the Kodaira–Néron classification [39, Theorem 8.2]. A rather more elementary observation is that the singular fibres may only contain rational curves. Moreover, the degree of the rational curves which may occur in singular fibres is bounded, since any fibre may be described by a set of equations of fixed degree.

Lemma 2.28. *There are only finitely many rational curves on $\bar{V}$ of a given degree.*

Proof. The set of rational curves on $\bar{V}$ of degree d corresponds to the set of divisor classes in $\operatorname{Pic}\bar{V}$ satisfying

$$D^2 = -2 \quad \text{and} \quad D.\Pi = d \tag{2.6}$$

where Π is the class of a plane section. We work in $\operatorname{Pic}\bar{V} \otimes \mathbb{R}$, and let $D_0 = (d/\Pi^2)\Pi$; then D_0 satisfies the second equation, and writing $D = D_0 + D'$ we must solve

$$(D' - D_0)^2 = -2 \quad \text{and} \quad D'.\Pi = 0. \tag{2.7}$$

The second equation defines a plane through the origin, and rearranging the first gives

$$(D')^2 = -2 - (d^2/\Pi^2).$$

Now the Hodge Index Theorem [21, V, Theorem 1.9] states that the intersection form is negative definite on the set of D' satisfying $D'.\Pi = 0$; thus the solution set of (2.7) is compact, so is that of (2.6), and the set of points of $\operatorname{Pic}\bar{V}$ lying in the solution set is discrete and hence finite. □

This proof indicates how all the rational curves of a given degree may be enumerated: the problem is to find all D' in $\operatorname{Pic}\bar{V} \otimes \mathbb{R}$ such that $(D')^2$ is equal to a certain constant, and $D' + D_0$ lies in $\operatorname{Pic}\bar{V}$.

More generally, we consider the following problem: given a positive definite quadratic form Q on $\mathbb{R}^n$, a vector $\boldsymbol{\alpha} \in \mathbb{R}^n/\mathbb{Z}^n$ and a bound C, find all vectors $\mathbf{v} \in \mathbb{Z}^n + \boldsymbol{\alpha}$ such that $Q(\mathbf{v}) \leq C$. When $\boldsymbol{\alpha} = 0$, this is the problem solved by the algorithm of Fincke and Pohst described in [16] and [8]. The algorithm is easily modified to cope with the offset $\boldsymbol{\alpha}$.

To apply such an 'inhomogeneous' Fincke–Pohst algorithm to the problem of finding divisors with prescribed degree and self-intersection, we construct the following algorithm. In this form it can also be used when working over $\mathbb{Q}$ instead of over $\bar{\mathbb{Q}}$. We assume that there is a standard basis chosen for $\operatorname{Pic} \bar{V}$, and that we already have a matrix $\mathbf{N}$ whose columns represent, in this standard basis, a basis for $\operatorname{Pic} V$. Such a matrix is computed using the algorithms of Chapter 3.

> **Note:** For the purposes of this algorithm, we assume that the first column of $\mathbf{N}$, that is, the first generator of $\operatorname{Pic} V$, represents the class of a plane section.

Algorithm 2.29. Given a $20 \times \rho$ matrix $\mathbf{N}$ whose columns describe a basis for $\operatorname{Pic} V$, a 20×20 matrix $\mathbf{Q}$ representing the intersection form on $\operatorname{Pic} \bar{V}$, and integers d and n, this algorithm produces a matrix whose columns describe all elements of $\operatorname{Pic} V$ with degree d and self-intersection at least n.

1. If $d^2/4 < n$ then return an empty matrix.
2. If $\rho = 1$, then the plane section Π generates $\operatorname{Pic} V$. In this case, return a 1-column matrix representing $(d/4)\Pi$ if d is divisible by 4, and an empty matrix otherwise.
3. Let $\mathbf{d_0} \leftarrow (d/4)\boldsymbol{\pi}$, where $\boldsymbol{\pi}$ is the column vector representing the class of Π.
4. Let $\mathbf{a} \leftarrow \boldsymbol{\pi}^T\mathbf{Q}\mathbf{N}$.
5. Using a standard algorithm, find: an integer vector $\mathbf{d_1}$ such that

$$\mathbf{a}^T\mathbf{d_1} = d;$$

and an integer matrix $\mathbf{A}$ whose columns generate the solution set of $\mathbf{a}^T\mathbf{x} = 0$. [2] If no such $\mathbf{d_1}$ exists, return an empty matrix.

6. Let $\mathbf{B}$ be any left inverse matrix to $\mathbf{NA}$.

7. Let $\mathbf{Q'} \leftarrow \mathbf{A}^T\mathbf{N}^T\mathbf{QNA}$.

8. Let $\boldsymbol{\alpha} \leftarrow \mathbf{B}(\mathbf{Nd_1} - \mathbf{d_0})$.

9. Apply the inhomogeneous Fincke–Pohst algorithm to find all vectors $\mathbf{x} \in \mathbb{Z}^\rho + \boldsymbol{\alpha}$ such that $\mathbf{x}^T\mathbf{Q'}\mathbf{x} \leq d^2/4 - n$.

10. Return the matrix whose columns are $\mathbf{NAx} + \mathbf{d_0}$ for each such vector $\mathbf{x}$.

Being able to list all rational curves of a given degree makes it straightforward to find the irreducible components of the fibres of a given fibration. If we know the class F in $\operatorname{Pic} V$ of a fibre, then we start by listing all the rational curves of degree 1, say, which have intersection number 0 with F. Each fibre must be connected (Zariski's Main Theorem, [21, III, Corollary 11.4]) and disjoint from each other fibre; using this it is easy to search for connected sets of rational curves which together add to the class of F. If curves of degree 1 do not provide sufficient singular fibres, we continue by looking at rational curves of degree 2, and so on; the process is guaranteed to terminate because the total degree of the components of a singular fibre is simply $F.\Pi$.

There is a formula described in [2, III, Proposition 11.4] which shows that the (complex) Euler characteristics of the singular fibres must sum to 24. It is a simple exercise in topology to compute the Euler characteristic of each of the possible fibre types in the Kodaira–Néron classification, and so this formula provides an easy way to determine when all the singular fibres of a fibration have been found.

The rank of the group $\operatorname{Pic}_{\text{vert}}$ and thence of the Jacobian of the generic fibre may be found without computing a set of generators for $\operatorname{Pic}_{\text{vert}}$.

[2] In PARI, this is accomplished by using the function `matsolvemod` to solve the equation $\sum_{i=2}^{\rho} \mathbf{a}_i\mathbf{x}_i \equiv d \pmod{\mathbf{a}_1}$.

Proposition 2.30. *Suppose that all the singular fibres have type I_n, where $n \geq 2$. Then the rank of* $\mathrm{Pic}_{\mathrm{vert}}$ *is*

$$24 - (\textit{number of singular fibres}) + 1$$

and the rank of the Jacobian of the generic fibre is

$$(\textit{number of singular fibres}) - 5.$$

Proof. Note that the Euler characteristic of a fibre of type I_n is n, and these must therefore sum to 24. We then apply the results of Shioda [37, §1]. □

This algorithm may also be used to list divisor classes of given degree and self-intersection zero, and therefore to list the fibrations on V. In general, there is a better way to do this, but this algorithm is nonetheless useful.

2.3.3 An example

As an example, we consider those cases where $\mathrm{Pic}\, V$ has rank 2; here V has a fibration if and only if the determinant of the lattice $\mathrm{Pic}\, V$ is minus a square. The fibration is easy to find, as solving a quadratic form in two variables is trivial.

The fibrations which arise on V when $\mathrm{Pic}\, V$ has rank 2 fall into three distinct types, up to various Galois actions and permutations of variables. These three types may be summarised as follows:

- Fibrations having a fibre which looks like

$$L_{11}^{123} + L_{15}^{123} + L_{51}^{123} + L_{55}^{123}$$

  defined over $\mathbb{Q}(\sqrt{a_0 a_1 a_2 a_3})$. These are the fibrations studied in [44]. Such a fibration exists in case A1 of Appendix A and all its subcases. The six singular fibres each consist of four straight lines, arranged as a fibre of type I_4. The $\mathrm{Pic}_{\mathrm{vert}}$ has rank 19 and, as shown in the proof of Proposition 2.15, the generic fibre is a 2-covering of its Jacobian, which has finite Mordell–Weil group.

- Fibrations with a fibre which looks like

$$L_{11}^{123} + L_{17}^{123} + L_{51}^{123} + L_{57}^{123}.$$

  This fibre and a similar one are the two fibres of type I_4, consisting each of four straight lines. There are eight other singular fibres, each of which is of type I_2 made up of two rational curves of degree 2. This fibration does have a section: in fact, any line L_{mn}^{231} or L_{mn}^{312} has intersection number 1 with the fibre. The $\mathrm{Pic}_{\mathrm{vert}}$ is of rank 15, and therefore the generic fibre is an elliptic curve of rank 4. (This fits with the results given in [37].) This particular fibration is defined, for example, in case A212 of our classification.

- Fibrations with a fibre which looks like

$$L_{11}^{123} + L_{17}^{123} + L_{31}^{123} + L_{33}^{123} + L_{53}^{123} + L_{55}^{123} + L_{75}^{123} + L_{77}^{123}.$$

  This fibre and another similar one are of type I_8, consisting each of eight straight lines arranged in an octagon. There are four more singular fibres, each of type I_2 consisting of two rational curves of degree 4. The fibration does not have a section; the $\mathrm{Pic}_{\mathrm{vert}}$ is of rank 19, indicating that the Jacobian of the generic fibre is an elliptic curve of rank zero. The particular fibration given here is defined, for example, in case A176 of our classification.

In fact, these fibrations which are defined for surfaces V of Picard rank 2 between them cover almost all surfaces which have a fibration. That is, there are only a small number of cases in which V has a fibration, but not one of the types listed above. Further calculation reveals that every surface possessing a fibration has one of degree at most 8.

Having found some fibrations defined on V, we may go on to investigate the associated vertical Brauer group. An example of how this can be computed is given in Section 4.5.

Chapter 3

Galois theory of the Picard group

This chapter describes techniques for investigating the structure of $\operatorname{Pic} \bar{V}$ as a Galois module. By Proposition 2.15 this depends only on knowing the Galois action on the 48 lines on $\bar{V}$. We show in Section 3.1 that all possible Galois actions for varying parameters a_0, a_1, a_2, a_3 may be studied by considering subgroups of a 'generic' Galois group Γ. We then, in Section 3.2, review some basic algorithms for computing with finitely generated Abelian groups. Sections 3.3 to 3.6 demonstrate algorithms for performing various computations using the Galois action on the 48 lines. The results of these computations are given in the tables in Appendix A.

The main reference for this chapter is [8]. We will make use of some general results on the Galois theory of rings and schemes, which may be found in [5] (Chapter 5) and in [19] respectively.

3.1 The 'generic' Galois group and its action

The 48 lines on the surface $\bar{V}$ were defined in equations (1.2)–(1.4). Firstly, we note that the 48 lines are all defined over a finite extension of $\mathbb{Q}$, so that the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on them factors through a finite group. Recall that α_{ij} denotes a fourth root of a_i/a_j, chosen such that $\alpha_{ij}\alpha_{jk} = \alpha_{ik}$.

Lemma 3.1. *The field* $\mathbb{Q}(\alpha_{10}, \alpha_{20}, \alpha_{30}, \epsilon)$ *is the least field of definition for the 48 lines* L_{mn}^{pqr}.

Proof. All 48 lines are clearly defined over this field. Conversely, let K be the least field of definition of the 48 lines. Then K contains $\epsilon^m \alpha_{pq}$ for all $p \neq q$ and all odd m. In particular, K contains $\epsilon\alpha_{12}$ and $\epsilon\alpha_{02}$; dividing these, we see that K contains α_{10}. Similarly, K contains α_{20} and α_{30}. But now K contains both α_{10} and $\epsilon\alpha_{10}$, so must also contain ϵ. □

How does the Galois action on the 48 lines vary as the coefficients a_0, a_1, a_2, a_3 are changed? To answer this we will construct a 'generic' diagonal quartic surface.

Let U be the (affine) subscheme of $\mathbb{P}^3_{\mathbb{Q}}$, with homogenous coordinates S_i, defined by $S_0S_1S_2S_3 \neq 0$. This will be the space in which the parameter $a = (a_0 : a_1 : a_2 : a_3)$ lives. Let X be the scheme in $\mathbb{P}^3_U$ defined by

$$X : S_0X_0^4 + S_1X_1^4 + S_2X_2^4 + S_3X_3^4 = 0$$

which is our 'generic' surface. For any $a \in U(\mathbb{Q})$, the fibre X_a is the diagonal quartic surface over $\mathbb{Q}$ given by (1.1). The 48 lines are given by the closed subscheme $L \subset X$ defined by

$$\begin{aligned} L : \{S_0X_0^4 = -S_1X_1^4,\ S_2X_2^4 = -S_3X_3^4\} \\ \cup \{S_0X_0^4 = -S_2X_2^4,\ S_3X_3^4 = -S_1X_1^4\} \\ \cup \{S_0X_0^4 = -S_3X_3^4,\ S_1X_1^4 = -S_2X_2^4\} \end{aligned}$$

which has 3 irreducible components as a scheme over $\mathbb{Q}$ (and, indeed, over $\bar{\mathbb{Q}}$).

To split L into its 48 components, we consider a scheme $\tilde{U} \to U$ constructed as follows. Let $\tilde{U}$ be the subscheme of $\mathbb{P}^3_{\mathbb{Q}(\epsilon)}$, with homogeneous coordinates T_i, defined by $T_0T_1T_2T_3 \neq 0$. Define a map $\tilde{U} \to U$ by $T_i^4 = S_i$. Then $\tilde{U}$ is an étale covering of U, and in fact the covering is Galois of degree 256 (degree 4 for the base field extension, and degree 64 for the geometric covering). We will call the group of this covering Γ, and it will play a central rôle in the rest of this chapter.

We can explicitly write down a set of generators for Γ, for it is the same as the Galois group of the extension of function fields $k(\tilde{U})/k(U)$. Writing s_i for S_i/S_0 and t_i for T_i/T_0, this extension is

$$\mathbb{Q}(\epsilon, t_1, t_2, t_3)/\mathbb{Q}(s_1, s_2, s_3) \tag{3.1}$$

where again $t_i^4 = s_i$. We note here that $\mathbb{Q}(\epsilon) = \mathbb{Q}(i, \sqrt{2})$, which will be useful for calculations. Kummer theory then shows that the Galois group Γ of (3.1) fits into an exact sequence

$$0 \to \Gamma' \to \Gamma \to \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \to 0$$

and that Γ' is Abelian. We see that a system of generators for Γ is given by

$$\begin{aligned} \sigma_1 &: t_1 \mapsto it_1 \\ \sigma_2 &: t_2 \mapsto it_2 \\ \sigma_3 &: t_3 \mapsto it_3 \\ \sigma_4 &: \sqrt{2} \mapsto -\sqrt{2} \\ \tau &: i \mapsto -i \end{aligned} \tag{3.2}$$

where each generator fixes those of $\{t_1, t_2, t_3, \sqrt{2}, i\}$ not mentioned. The multiplication in Γ is as follows: all the σ_i commute with each other; and $\tau\sigma_i = \sigma_i^{-1}\tau$.

What effect does the base change $\tilde{U} \to U$ have on the 48 lines L? Let $\tilde{L}$ denote the fibre product $L \times_U \tilde{U}$. Then $\tilde{L}$ is the scheme defined over $\mathbb{Q}(\epsilon)$ by the equations

$$\begin{aligned} \tilde{L} : \{T_0^4X_0^4 = -T_1^4X_1^4,\ T_2^4X_2^4 = -T_3^4X_3^4\} \\ \cup \{T_0^4X_0^4 = -T_2^4X_2^4,\ T_3^4X_3^4 = -T_1^4X_1^4\} \\ \cup \{T_0^4X_0^4 = -T_3^4X_3^4,\ T_1^4X_1^4 = -T_2^4X_2^4\} \end{aligned} \tag{3.3}$$

and each quartic equation now splits into four linear factors: $\tilde{L}$ is the union of 48 straight lines. The group Γ acts on $\tilde{L}$ in the obvious way, permuting the lines within their three sets.

Now let $a = (a_0 : a_1 : a_2 : a_3)$ be a rational point of U. The inverse image of a in $\tilde{U}$ is étale over a, and so consists of finitely many points; and, as the covering is Galois, these points are permuted transitively by Γ and so are isomorphic. We let b be one of these points, and denote by Γ_b the decomposition group of b, that is, the subgroup of Γ which fixes b ([19], Section 2). The residue field $k(b)$ is then generated over $\mathbb{Q}$ by ϵ and fourth roots of the a_i/a_0, and has Galois group Γ_b. In fact, $k(b)/\mathbb{Q}$ is easily checked to be the extension described in Lemma 3.1. Note that different choices of b will give rise to conjugate groups Γ_b; in terms of the extension $k(b)/\mathbb{Q}$ this simply means a different choice of the various fourth roots and square roots. For an example of how this works, see the beginning of Section 3.4.

Considering the 48 lines on the surface X_a, we now have a Galois covering $\tilde{L}_b \to L_a$ which is simply the covering we obtain by extending the base field of L_a from $\mathbb{Q}$ to $k(b)$: in other words, by the smallest extension such that the 48 lines are all individually defined. The corresponding Galois action on the 48 lines is that induced by Γ_b acting on the generic lines $\tilde{L}$.

We may summarise all this discussion in the following statement:

Proposition 3.2. *For any choice of a_0, a_1, a_2, a_3, the action of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *on the 48 lines of V factors through a finite quotient G. This group G, and its action on the 48 lines, are isomorphic to a subgroup of Γ and its action on the generic 48 lines $\tilde{L}$.* □

All the groups Γ_b which arise in this way will have the property that $\mathbb{Q}(\epsilon)^{\Gamma_b} = \mathbb{Q}$, for the residue field at a is $\mathbb{Q}$. Although we are primarily interested in the case where the base field is $\mathbb{Q}$, the above discussion makes sense when the base field is any number field k; and the Galois structure of $\mathrm{Pic}\,\bar{V}$ depends on k only in that it depends on $k \cap \mathbb{Q}(\epsilon)$. It is no extra effort for us to study such cases, and indeed will be useful. The tables in Appendix A are divided into one section for each possibility for $k \cap \mathbb{Q}(\epsilon)$.

It follows from Proposition 3.2 that to study all possible actions of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the 48 lines on $\bar{V}$, it is necessary to study the subgroups of Γ. Specifically, this chapter will address the following problems:

- to list all the subgroups of Γ;
- to find equivalences between the subgroups of Γ which correspond to various trivial rearrangements of the coefficients a_i, and list the different equivalence classes;
- given non-zero rational numbers a_i, to find the subgroup of Γ associated to the surface V;
- given a subgroup H of Γ, to find conditions on the coefficients a_i which imply that the group G of Proposition 3.2 is contained in H;
- given a subgroup of Γ, to find the part of $\operatorname{Pic} \bar{V}$ which is defined over $\mathbb{Q}$;
- given a subgroup of Γ, to compute the corresponding cohomology group $H^1(\mathbb{Q}, \operatorname{Pic} \bar{V})$.

Before we embark on these computations in Section 3.3, we review some theory of finitely generated Abelian groups in the following section.

3.2 Computing with Abelian groups

In this section we gather some results and algorithms for dealing with finitely generated Abelian groups. Of course our group Γ is not Abelian, but it is "almost" Abelian, and we will be able to use the techniques described in this chapter to deal with it. A standard reference for the algorithms used is Cohen's book [8].

All the matrices we will consider are integer matrices, and a matrix is invertible if it has an inverse which is also an integer matrix.

3.2.1 Groups and matrices

We will always think of Abelian groups in a concrete way as $\mathbb{Z}$-modules. Every finitely generated $\mathbb{Z}$-module has a resolution by free modules: let G

be a finitely generated Abelian group; then we can find an exact sequence

$$\mathbb{Z}^m \xrightarrow{\alpha} \mathbb{Z}^n \to G \to 0 \tag{3.4}$$

of $\mathbb{Z}$-modules. We may always assume either that $m = n$ or that α is of maximal rank; if G is finite, we may assume both. What we are doing here is expressing G as a quotient of $\mathbb{Z}^n$ by a lattice, the image of α. Any set of generators of $\mathbb{Z}^n$ also generates G, though the converse is not true.

By choosing bases for the $\mathbb{Z}^m$ and $\mathbb{Z}^n$ in (3.4), we obtain a matrix $\mathbf{A}$ for the linear map α.

Definition 3.3. Any matrix for the linear map α with respect to some choice of bases is a *realisation* of the group G.

Given a choice of basis for $\mathbb{Z}^n$ in (3.4), we may represent a subgroup of G by giving its generators as elements of $\mathbb{Z}^n$. We will often represent such a subgroup by a matrix whose columns form a set of generators. Note that there are thus two very different meanings we can attach to a matrix: it may be a realisation of a finitely generated Abelian group, or it may be a set of generators for a subgroup of such a group.

3.2.2 Normal forms for matrices

There are two well-known normal forms for matrices, the Hermite normal form and the Smith normal form, which have relevance to the use of matrices to describe Abelian groups. We describe both of these normal forms and explain how they will be used in our algorithms. Both the Hermite and Smith normal forms relate to choosing bases for the $\mathbb{Z}^m$ and $\mathbb{Z}^n$ in (3.4).

The Hermite normal form

Here we think of the basis for $\mathbb{Z}^n$ as fixed in some way: perhaps it has some special significance in the problem being studied. We are interested in properties of the lattice $\Lambda = \operatorname{im} \alpha$ and the quotient $\mathbb{Z}^n/\Lambda$. In particular, we would like to be able to tell whether two lattices, specified by generating sets, are equal. The Hermite normal form allows us to do this.

As before, $\mathbf{A}$ is the matrix representing the map α with respect to our chosen basis of $\mathbb{Z}^n$, and with respect to some basis of $\mathbb{Z}^m$. The columns of $\mathbf{A}$ form a generating set for Λ. What we would like to have is a canonical ordered set of generators for Λ, and the Hermite normal form provides just that: every lattice has precisely one ordered set of generators which form a matrix in Hermite normal form. The Hermite normal form is discussed in greater detail in section 2.4.2 of [8], and we do not prove its existence or uniqueness here; we simply recall some properties.

Proposition 3.4.

1. *Given an $n \times m$ integer matrix $\mathbf{A}$, there exists a unique $m \times m$ invertible integer matrix $\mathbf{U}$ such that $\mathbf{AU}$ is in Hermite normal form.*

2. *A square matrix $\mathbf{M}$ in Hermite normal form satisfies the following properties:*

   (a) $\mathbf{M}$ *is upper triangular;*

   (b) All the elements of $\mathbf{M}$ *are non-negative;*

   (c) Each element on the diagonal of $\mathbf{M}$ *is the largest element in its row.*

   An $n \times m$ matrix, where $m > n$, in Hermite normal form has the first $m - n$ columns equal to zero, and the remaining n columns form a square matrix in Hermite normal form.

$\square$

The columns of the matrix $\mathbf{U}$ give the new basis for Λ in terms of the old generating set. Choosing a unique ordered basis for a lattice will be useful in several ways in our calculations.

The Smith normal form

When discussing the Hermite normal form, we assumed that the basis chosen for $\mathbb{Z}^n$ in (3.4) was special in some way. We now relax that assumption: all that interests us is the structure of the quotient G as an abstract $\mathbb{Z}$-module. We assume here that $m = n$. The structure theorem for finitely generated modules over a principal ideal domain states that G is isomorphic to a product of a free group by some cyclic groups, and moreover that the orders of these cyclic groups may be chosen to satisfy certain properties; the Smith normal form of a matrix provides a concrete interpretation of that theorem.

An integer matrix $\mathbf{M}$ is said to be in Smith normal form if it is of the form

$$\mathbf{M} = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d_n \end{pmatrix} \tag{3.5}$$

where $d_i \mid d_{i+1}$ for $i = 1, \ldots, n-1$. It is then immediately clear that the group realised by the matrix $\mathbf{M}$ is isomorphic to

$$\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z} \times \mathbb{Z}^{n-r} \tag{3.6}$$

where $d_1, \ldots, d_r$ are the non-zero diagonal entries of $\mathbf{M}$.

A simple algorithm (given in [8]) proves:

Proposition 3.5. *Given a square integer matrix* $\mathbf{A}$*, there exist invertible matrices* $\mathbf{U}, \mathbf{V}$ *such that* $\mathbf{D} = \mathbf{UAV}$ *is in Smith normal form. The resulting diagonal matrix* $\mathbf{D}$ *is unique.* □

The columns of $\mathbf{U}^{-1}$ give generators for G, in terms of the old basis, which are generators of the cyclic groups in (3.6). Such a system of generators for G will be called a *Smith normal form basis* for G.

3.2.3 Subgroups and quotients

Here we apply the Hermite and Smith normal forms to some problems which we will have to solve in future sections. We are always working in the context of a finitely generated Abelian group G, and assume we have been given a matrix $\mathbf{A}$ which is a realisation of G. Let Λ denote the lattice which is the image of $\mathbf{A}$ in $\mathbb{Z}^n$, so that $G \cong \mathbb{Z}^n/\Lambda$. We are interested in certain subgroups and subquotients of G. Both the algorithms we describe here are very simple, almost trivial, but deserve proper explanation.

The first problem is this: given a set of generators for a subgroup H of G, we wish to find a canonical set of generators for H. Now the subgroups H are in 1-1 correspondence with the lattices Λ' of $\mathbb{Z}^n$ containing Λ: given a set of generators for H, we adjoin a basis for Λ to obtain a set of generators for Λ'. Conversely, any generating set for Λ' is also a generating set for H. This leads to the following short algorithm:

Algorithm 3.6. Given a matrix $\mathbf{A}$ which is a realisation of a group G, and a matrix $\mathbf{B}$ whose columns are generators for a subgroup H of G, find a unique canonical matrix whose columns generate H.

1. Let $\mathbf{B} \leftarrow (\mathbf{B} \mid \mathbf{A})$, the concatenation of $\mathbf{B}$ and $\mathbf{A}$.
2. Put $\mathbf{B}$ into Hermite normal form.

This description of subgroups also allows us to make a further observation. Given that $\Lambda \subseteq \Lambda'$, and given a choice of basis for Λ' as a matrix $\mathbf{B}$, we may write down a matrix $\mathbf{C}$ whose columns are the coordinates, in this basis, of a basis for Λ. Then the the columns of the product matrix $\mathbf{A} = \mathbf{BC}$ are the coordinates of the basis for Λ, but now given in the standard basis of $\mathbb{Z}^n$; so $\mathbf{A}$ is a realisation of G. Conversely, any such factorisation $\mathbf{A} = \mathbf{BC}$ arises in this way from a subgroup H of G. This means that to list the subgroups of G, it is enough to list the matrices in Hermite normal form which divide $\mathbf{A}$ on the left: and this is precisely the method adopted by PARI.

The second problem which we will need to solve is the following. Given two subgroups $K \subset H$ of G, we wish to know the structure of the quotient H/K. The Smith normal form is how one discovers the abstract structure of an Abelian group, so we must apply it here.

Let Λ', Λ'' be the lattices which are the liftings of H and K, respectively, to $\mathbb{Z}^n$. Then $\Lambda'' \subset \Lambda'$, and

$$\frac{H}{K} \cong \frac{\Lambda'/\Lambda}{\Lambda''/\Lambda} \cong \frac{\Lambda'}{\Lambda''}$$

If we let $\mathbf{B}$ and $\mathbf{C}$ be matrices whose columns are bases for Λ' and Λ'' respectively, then $\mathbf{C} = \mathbf{BE}$ for some matrix $\mathbf{E}$; and the columns of $\mathbf{E}$ are the coordinates of the basis for Λ'' with respect to the chosen basis of Λ'. So the matrix $\mathbf{E}$ is a realisation of the group Λ'/Λ'', and its Smith normal form shows the structure of this group, which is isomorphic to H/K.

Algorithm 3.7. Given matrices $\mathbf{B}, \mathbf{C}$ whose columns are generators for H and K respectively, subgroups of a group G, find: a matrix $\mathbf{B'}$ whose columns are generators for H; and a matrix $\mathbf{D}$ in Smith normal form, such that the columns of $\mathbf{B'D}$ generate K. Then $\mathbf{D}$ contains the structure of the quotient H/K, and the columns of $\mathbf{B'}$ form a Smith normal form basis for H/K.

1. Let $\mathbf{E} \leftarrow \mathbf{B}^{-1}\mathbf{C}$.
2. Use the Smith normal form algorithm to find matrices $\mathbf{U}, \mathbf{V}$ such that $\mathbf{D} = \mathbf{UEV}$ is in Smith normal form.
3. Let $\mathbf{B'} \leftarrow \mathbf{BU}^{-1}$.

3.3 Listing the cases

We now turn to the problem of finding all the different cases into which our surface (1.1) might fall. As described in Section 3.1, this involves listing all of the subgroups of the generic Galois group Γ, up to certain equivalences which we must describe exactly.

3.3.1 Representation of subgroups

We choose how a subgroup of Γ will be described in a canonical way. We fix the generators of Γ listed in (3.2), and denote by Γ' the Abelian subgroup generated by $\sigma_1, \ldots, \sigma_4$. The matrix for this realisation of Γ' is

$$\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}.$$

Firstly we consider subgroups of Γ'. Any element g of Γ' may be represented uniquely as an integer column vector using this basis: the first three coordinates, corresponding to σ_1, σ_2 and σ_3, are considered modulo 4; and the fourth coordinate, corresponding to σ_4, is considered modulo 2. Now if G is a subgroup of Γ', let $\mathbf{M}$ be a matrix whose columns represent generators of G. Algorithm 3.6 gives a way of turning $\mathbf{M}$ into a canonical 4×4 matrix whose columns generate G.

The quotient Γ/Γ' has order 2 and is generated by the element τ, so any element of Γ is either an element of Γ' or is τ multiplied by an element of Γ'. Let H be a subgroup of Γ, and write H' for the intersection of H with Γ'. Either H is entirely contained in Γ', in which case $H = H'$; or else H/H' is of order 2, and H is generated by a set of generators for H', together with any element of H which is not in H'. In other words, we have shown

Proposition 3.8. *Any subgroup H of Γ can be expressed in one of the two forms*

- $H = \langle h_1, h_2, h_3, h_4 \rangle$
- $H = \langle h_1, h_2, h_3, h_4, \tau h_5 \rangle$

where the h_i are elements of Γ'. □

In calculations, we will represent H by a 4×4 matrix $\mathbf{M}$ of generators for H', together with another optional element $\mathbf{v}$ of $\mathbb{Z}^4$ representing h_5. This pair $(\mathbf{M}, \mathbf{v})$ will be called a *matrix-vector* representation of H. If there is no fifth generator h_5, then $\mathbf{v}$ will be an "empty" vector (represented in PARI as `[]`).

This representation is far from unique: when choosing h_5, we could have picked any element of H not in H'. But we can take advantage of the upper triangular shape of the Hermite normal form to come up with the following algorithm:

Algorithm 3.9. Given a set of generators for a subgroup H of the Galois group Γ, this algorithm produces a uniquely defined canonical set of generators for H. Let $(\mathbf{M}, \mathbf{v})$ be a set of generators for H, where $\mathbf{M}$ is a 4×4 matrix whose columns generate H' over the basis $\sigma_1, \ldots, \sigma_4$ and $\mathbf{v}$ is a column vector representing an element h_5 of Γ' (given in the same basis) such that τh_5 is a fifth generator of H.

1. Apply Algorithm 3.6 to $\mathbf{M}$.

2. Set $i \leftarrow 4$.

3. Let $\mathbf{v} \leftarrow \mathbf{v} - \lfloor \mathbf{v}_i / \mathbf{M}_{ii} \rfloor \times \mathbf{M}_{(i)}$.

4. Let $i \leftarrow i - 1$.

5. If $i > 0$, go to step 3.

Here $\mathbf{M}_{(i)}$ denotes the ith column of $\mathbf{M}$. This algorithm is listed in Section D.1.1.

It is clear that the resulting representation does indeed represent the same subgroup H: we have simply chosen a canonical basis for H', and then changed h_5 only by subtracting elements of H'. And the representation is unique: for the ith element of $\mathbf{v}$ lies in the interval $[0, \mathbf{M}_{ii})$; adding any multiple of the ith column of $\mathbf{M}$ to $\mathbf{v}$ would violate this condition. This, together with the fact that $\mathbf{M}$ is upper triangular, proves the uniqueness.

We note that it is easy to find the order of H:

$$|H| = \begin{cases} 128/\det \mathbf{M} & \text{if } v \text{ is empty;} \\ 256/\det \mathbf{M} & \text{otherwise.} \end{cases}$$

As $\mathbf{M}$ will usually be upper triangular, calculating its determinant is particularly simple.

3.3.2 Listing subgroups

Having fixed a canonical way to represent subgroups of Γ, we are now in a position to list them.

There exists a function in PARI which lists the subgroups of an Abelian group given in Smith normal form (or, equivalently, lists the Hermite normal form left divisors of a diagonal integer matrix). This gives a simple way of listing all the subgroups of Γ:

1. List all the subgroups of Γ'.
2. For each subgroup H' of Γ' and each element h_5 of Γ', reduce the subgroup generated by H' and τh_5 to canonical form using Algorithm 3.9.
3. Remove the many repeated entries from the list of subgroups.

This method of course counts large subgroups many times; but this was not a problem.

There are 10,095 distinct subgroups of Γ.

3.3.3 Equivalences between subgroups

We have been listing subgroups of Γ, but what we are interested in is listing the different possible Galois actions on the 48 lines of our surface (1.1). The relation between subgroups and cases is described in Section 3.1, but we should decide which cases we will consider to be "the same" as each other. This will allow us to reduce the 10,095 subgroups to a more manageable number of cases.

Firstly, the subgroup of Γ associated to a surface depends on choices of roots, and so is defined only up to conjugacy class. Therefore any two subgroups which are conjugate to each other will belong to the same case.

Secondly, permuting the coefficients a_0, a_1, a_2, a_3 results in a new surface isomorphic over $\mathbb{Q}$ to the original one, and we will consider any two such surfaces to belong to the same case.

Choice of roots

In Section 3.1 we saw that the subgroup of Γ associated to a given surface is only determined up to conjugacy class, because we have choices of ϵ and of the α_{ij}. Accordingly, any two subgroups of Γ which differ only by such choices will be considered equivalent.

Let H be a subgroup of Γ, with a set of generators labelled as in Proposition 3.8. Replacing t_1 by it_1 has the effect of conjugating H by σ_1. This has no effect on the subgroup H' of H (it is Abelian), but the 'other' generator τh_5 becomes $\tau\sigma_1^2 h_5$. Similarly, conjugating by σ_2 or σ_3 has the effect of multiplying h_5 by σ_2^2 or σ_3^2 respectively. If $(\mathbf{M}, \mathbf{v})$ is a matrix-vector representation of H, we are adding 2 to the appropriate elements of $\mathbf{v}$.

We must also consider choice of ϵ. Replacing $\sqrt{2}$ by $-\sqrt{2}$ is conjugation by σ_4, which has no effect at all. Replacing i by $-i$ is conjugation by τ. The element τh_5 becomes τh_5^{-1}; in other words, our vector $\mathbf{v}$ is negated. But we are already only considering it modulo 2, so that makes no difference. Conjugation by τ also replaces each σ_i by σ_i^{-1}; but that is the same as replacing H by H^{-1}, which is the same thing. So there is nothing more to consider to cope with the choice of ϵ.

Permuting the coefficients

In terms of the generic Galois group, we want any two subgroups of Γ which are related only by permuting the parameters T_i to be equivalent. To do this, it is useful to consider firstly those permutations which fix T_0, and then the transposition of T_0 and T_1. Between them, these generate the whole permutation group (of order 24).

Any permutation fixing T_0 simply permutes the generators σ_1, σ_2, σ_3 of Γ. If $(\mathbf{M}, \mathbf{v})$ is a matrix-vector representation of a subgroup H, the effect of the permutation is to permute the first three rows of $\mathbf{M}$ and of $\mathbf{v}$.

Now consider the effect of interchanging T_0 and T_1. The inhomogeneous coordinates t_i, from which our generators σ_i are defined, are changed as follows:

$$(t_1, t_2, t_3) \mapsto (1/t_1, t_2/t_1, t_3/t_1)$$

and the effect on the Galois group is to replace $(\sigma_1, \sigma_2, \sigma_3)$ with

$$(\sigma_1^{-1}, \sigma_2\sigma_1^{-1}, \sigma_3\sigma_1^{-1}).$$

Let H be a subgroup of Γ, and let $(\mathbf{M}, \mathbf{v})$ be a matrix-vector representation of H. The effect of this substitution is to multiply both $\mathbf{M}$ and $\mathbf{v}$ on the left by the matrix

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{3.7}$$

It is readily verified that the matrix (3.7), together with the matrices representing permutation of the first three rows, generate a group isomorphic to S_4 which acts on our subgroups H. We will consider any two subgroups lying in the same orbit under this action to be equivalent.

3.3.4 Finding a canonical representative

Having explained when two subgroups are to be equivalent to each other, we must now produce an algorithm for finding a canonical representative of each equivalence class. This will be approached in two steps: firstly, finding a canonical subgroup in each conjugacy class; and secondly, finding a canonical subgroup in each equivalence class. Note that we may do this, because permutation of the a_i followed by conjugation is equal to (some other) conjugation followed by permutation.

We already have Algorithm 3.9 to produce a canonical representation of a subgroup H of Γ. Let $(\mathbf{M}, \mathbf{v})$ be a matrix-vector representation of H; in Section 3.3.3 we saw that conjugation has the effect of changing the elements of $\mathbf{v}$ by a multiple of 2. To get a canonical representative for a conjugacy class of subgroups, it might appear that all we have to do is take a canonical representation $(\mathbf{M}, \mathbf{v})$ of a subgroup H (which already has $\mathbf{v}$ "as small as possible") and then reduce $\mathbf{v}$ modulo 2. Unfortunately this does not quite work, for it may be possible to change $\mathbf{v}$ by adding or subtracting columns of $\mathbf{M}$ to produce a "smaller" $\mathbf{v}$ than we have already. However, we can change Algorithm 3.9 to do as we want, to get the following:

Algorithm 3.10. Given a set of generators for a subgroup H of the Galois group Γ, this algorithm produces a uniquely defined canonical set of generators for a canonical subgroup conjugate to H. Let $(\mathbf{M}, \mathbf{v})$ be a matrix-vector representation of H.

1. Apply Algorithm 3.6 to $\mathbf{M}$.
2. Let $\mathbf{N} \leftarrow (\mathbf{M} \mid 2\mathbf{I_4})$.
3. Put $\mathbf{N}$ into Hermite normal form.
4. Set $i \leftarrow 4$.
5. Let $\mathbf{v} \leftarrow \mathbf{v} - \lfloor \mathbf{v}_i/\mathbf{N}_{ii} \rfloor \times \mathbf{N}_{(i)}$.
6. Let $i \leftarrow i - 1$.
7. If $i > 0$, go to step 5.

Here $\mathbf{I_4}$ is the 4×4 identity matrix, and $\mathbf{N}_{(i)}$ denotes the ith column of $\mathbf{N}$. This algorithm is listed in Section D.1.2.

Now we must choose a unique representative modulo permutation of the a_i. We do this in the following, unsophisticated, way: by listing representatives of all 24 conjugacy classes which are equivalent to the given one, and by choosing the one which comes first in some arbitrary ordering (we use the lexicographic order). The implementation of this is listed in Section D.1.3. There are 546 different equivalence classes of subgroups, which are listed individually in the tables in Appendix A.

3.4 Finding the subgroup associated to a surface

We have now listed all possible cases into which the Galois action on the 48 lines on V might fall. However, this information is still not in a very helpful format: all we have is a list of subgroups of a large group. This section and the following one describe algorithms to perform two useful functions: given a surface, to find the subgroup of Γ which is associated to it; and given a subgroup, to describe in general the coefficients a_i which give rise to that subgroup.

In these two sections, we illustrate the algorithms with a running example. This will be the same surface as in the worked example of Section 5.3. It is defined by the equation

$$X_0^4 + X_1^4 = 6X_2^4 + 12X_3^4 \tag{3.8}$$

and so $(a_0, a_1, a_2, a_3) = (1, 1, -6, -12)$. In this section we will compute the subgroup of Γ associated to this surface, and in the following section we will derive a general formula for surfaces with that subgroup.

Suppose we are given non-zero rational numbers a_0, a_1, a_2 and a_3, or in other words a point a of the scheme U described in Section 3.1. We wish to find the subgroup of Γ associated to the diagonal quartic surface defined by the a_i; that is, to find a point b of $\tilde{U}$ lying above a, and the subgroup Γ_b of Γ which fixes b. In more concrete terms, we fix fourth roots α_{i0} of a_i/a_0 for $i = 1, 2, 3$ and ask what subgroup of Γ, acting via $t_i \mapsto \alpha_{i0}$, takes each α_{i0} to a conjugate of itself over $\mathbb{Q}$.

In our running example, the inverse image of a in $\tilde{U}$ is given by the ideal

$$\mathfrak{a} = (t_1^4 - 1, t_2^4 + 6, t_3^4 + 12)$$

in $\mathbb{Q}(\epsilon)[t_1, t_2, t_3]$. This decomposes into eight maximal ideals, of which a typical one is

$$\mathfrak{b} = (t_1 - 1, \sqrt{2}t_2^2 - t_3^2, t_3^4 + 12)$$

and the others are obtained by replacing 1 with another fourth root of unity, and maybe replacing $\sqrt{2}$ with $-\sqrt{2}$. We choose b to be the point associated to the maximal ideal $\mathfrak{b}$. Each element of Γ either fixes $\mathfrak{b}$ or takes it to one its conjugate maximal ideals. An example of an element of Γ which does not fix $\mathfrak{b}$ is σ_1, which takes $t_1 \mapsto it_1$. Examples of elements which do fix $\mathfrak{b}$ are σ_2^2, taking $t_2 \mapsto -t_2$; and $\sigma_2\sigma_3$, taking $t_2 \mapsto it_2$ and $t_3 \mapsto it_3$. Those elements which do fix $\mathfrak{b}$ induce automorphisms on the quotient

$$\mathbb{Q}(\epsilon)[t_1, t_2, t_3]/\mathfrak{b} = \mathbb{Q}(\epsilon, \sqrt[4]{-6}, \sqrt[4]{-12})$$

fixing $\mathbb{Q}$, and so are identified with elements of the Galois group of this field over $\mathbb{Q}$.

The object is to find a matrix $\mathbf{M}$ and vector $\mathbf{v}$ which represent the desired subgroup H of Γ. We will produce $\mathbf{M}$ in an upper triangular form, which comes from building up our field extension piece by piece.

Consider the tower of field extensions

$$\begin{array}{c} K_1 = \mathbb{Q}(\alpha_{10}, \alpha_{20}, \alpha_{30}, \epsilon) \\ | \\ K_2 = \mathbb{Q}(\alpha_{20}, \alpha_{30}, \epsilon) \\ | \\ K_3 = \mathbb{Q}(\alpha_{30}, \epsilon) \\ | \\ K_4 = \mathbb{Q}(\epsilon) = \mathbb{Q}(\sqrt{2}, i) \\ | \\ K_5 = \mathbb{Q}(i) \end{array}$$

Each extension is cyclic over the previous one; a generator for $\mathrm{Gal}(K_i/K_{i+1})$ is given by the image of a suitable power (1, 2 or 4) of σ_i. In what follows, we will identify H with $\mathrm{Gal}(K_1/\mathbb{Q})$ in the obvious manner. Let $h_1, \ldots, h_5$ be the generators for H as in Proposition 3.8, represented by $\mathbf{M}$ and $\mathbf{v}$. We will choose them as follows:

- h_1 is a generator for $\mathrm{Gal}(K_1/K_2)$. In our example, $K_1 = K_2$ and so h_1 is the identity.

- h_2 is a lifting of a generator for $\mathrm{Gal}(K_2/K_3)$. In our example, K_2 is of degree 2 over K_3 and so h_2 is of the form $\sigma_2^2\sigma_1^a$.

- h_3 is a lifting of a generator for $\mathrm{Gal}(K_3/K_4)$. On the example, K_3 is of degree 4 over K_4 and h_3 is therefore of the form $\sigma_3\sigma_2^b\sigma_1^c$.

- h_4 is a lifting of the generator for $\mathrm{Gal}(K_4/K_5)$; this is always of the form $\sigma_4\sigma_3^d\sigma_2^e\sigma_1^f$.

- τh_5 is a lifting of the generator for $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. Here h_5 is an element of Γ' which we must find.

It is the lifting of each generator to $\mathrm{Gal}(K_1/\mathbb{Q})$ which requires some thought; the rest is simple. In other words, finding the diagonal elements of $\mathbf{M}$ is straightforward, but finding the elements above the diagonal is less so.

We may immediately fill in two elements of $\mathbf{M}$ and $\mathbf{v}$, as K_4 and K_5 are fixed. We get

$$(\mathbf{M}, \mathbf{v}) = \left(\begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} * \\ * \\ * \\ 0 \end{pmatrix} \right)$$

Suppose that K is a number field containing a primitive fourth root of unity. It is well-known that the cyclic extensions of K of degree dividing 4 are given by $K(\sqrt[4]{d})$, where d is an element of K, and that they are classified by the class of d in $K^\times/(K^\times)^4$. The degree of the extension is the order of d in the quotient group. If in addition we know that d lies in $\mathbb{Q}$, we may work in $\mathbb{Q}^\times/(\mathbb{Q}^\times \cap (K^\times)^4)$: this has the advantage that, as $\mathbb{Q}$ has unique factorisation, $\mathbb{Q}^\times$ is the free group generated by -1 and all the primes. By abuse of language, we will call -1 a prime.

For calculations we work with the part of $\mathbb{Q}^\times$ generated by -1, 2 and all the primes dividing any of the a_i. Write F for this free group, and write F_i for the intersection of $(K_i^\times)^4$ with F. We then have

$$\mathbf{M}_{ii} = 4/[F_i : F_{i+1}] \quad \text{for } i = 1, \ldots, 3.$$

After applying this, we have

$$(\mathbf{M}, \mathbf{v}) = \left(\begin{pmatrix} \square & * & * & * \\ 0 & \square & * & * \\ 0 & 0 & \square & * \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} * \\ * \\ * \\ 0 \end{pmatrix} \right)$$

where $\square$ denotes either 1, 2 or 4 in each case.

Consider our running example. The primes we need to consider are -1, 2 and 3, so let F be the free group generated by these three elements. In $\mathbb{Q}(i)$, the non-trivial fourth powers are 1 and -4; so F_5 is generated by $(-1)^2$ and $(-1) \times 2^2$ together with 2^4 and 3^4. Continuing with the other F_i gives

$$\begin{aligned} F_5 &= \langle (-1)^2, (-1) \times 2^2, 2^4, 3^4 \rangle \\ F_4 &= \langle -1, 2^2, 3^4 \rangle \\ F_3 &= \langle -1, 2^2, 3 \rangle \\ F_2 &= \langle -1, 2, 3 \rangle \\ F_1 &= F_2. \end{aligned}$$

This gives the diagonal elements of $\mathbf{M}$ to be 4, 2, 1, 1.

Next we come to the off-diagonal elements. Consider first $\mathbf{M}_{12}$. The second column of $\mathbf{M}$ represents an element h_2 of Γ which, when mapped to $\mathrm{Gal}(K_2/\mathbb{Q})$, gives $\sigma_2^{\mathbf{M}_{22}}$. That is, $h_2 = \sigma_1^n \sigma_2^{\mathbf{M}_{22}}$ for some integer n. To find n, we consider the action of h_2 on α_{10}. Let m be the least power (1, 2 or 4) of α_{10} which lies in K_2. We know the action of h_2 on K_2, so get

$$h_2 \alpha_{10}^m = (i^n \alpha_{10})^m = i^r \alpha_{10}^m$$

whence $n = r/m$. This will be an integer, as α_{10}^4 always lies in $\mathbb{Q}$. A similar process allows us to discover $\mathbf{M}_{23}$, and thence $\mathbf{M}_{13}$. The same argument gives the fourth column of $\mathbf{M}$.

The running example works as follows:

1. We already know that $h_2 = \sigma_2^2 \sigma_1^a$ for some a, and wish to compute a. Now $\alpha_{10} = 1$, which must be fixed by any Galois action; so $a = 0$ and $h_2 = \sigma_2$.

2. Now we consider $h_3 = \sigma_3 \sigma_2^b \sigma_1^c$. The degree computations we have already done show that α_{20}^2 lies in K_3, and linear algebra in F gives

$$(-6)^2 = (-12)^2/4$$
$$\text{and so } \alpha_{20}^2 = \alpha_{30}^2/\sqrt{2}.$$

We know the effect of h_3 on the right hand side of this expression: $\sqrt{2}$ is fixed and α_{30}^2 negated. Therefore h_3 negates α_{20}^2 and so b is either 1 or 3 (it does not matter which). As before, we find $c = 0$.

3. For h_4, we know that the smallest power of α_{30} lying in K_4 is the fourth power; so h_4 may have any effect on α_{30}, and we choose that α_{30} should be fixed by h_4. The above expression for α_{20}^2 then implies that h_4 should change the sign of α_{20}^2, and we end up with $h_4 = \sigma_4\sigma_2$.

Calculating the entries of $\mathbf{v}$ is rather easier, as $\mathbb{Q}(i)/\mathbb{Q}$ only has degree 2, and we are only interested in the values modulo 2 (see Section 3.3.3). We get

$$\mathbf{v}_i = \begin{cases} 0 & \text{if } a_i/a_0 \text{ is positive;} \\ 1 & \text{if } a_i/a_0 \text{ is negative.} \end{cases}$$

Combining all these calculations, the example we are studying ends up with

$$(\mathbf{M}, \mathbf{v}) = \left(\begin{pmatrix} 4 & 0 & 0 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right).$$

Putting these steps all together results in the following algorithm. We assume the existence of a function which, given a finite ordered set $p_1, \ldots, p_n$ of primes and a rational number $a = p_1^{r_1} \cdots p_n^{r_n}$, returns the vector $(r_1, \ldots, r_n)$. The matrices $\mathbf{K_i}$ in this algorithm are bases for the groups $(K_i^\times)^4 \cap F$, where F as above is the free group on the primes in S.

Algorithm 3.11. Given rational numbers a_0, a_1, a_2 and a_3, this algorithm calculates a matrix $\mathbf{M}$ and a vector $\mathbf{v}$ which are a matrix-vector representation of the subgroup H of Γ corresponding to the diagonal quartic surface defined by the a_i.

1. Let S be the ordered set of primes occurring in the prime factorisations of the a_i, together with -1 and 2. Let $n \leftarrow |S|$.

2. Let
$$\mathbf{K_4} \leftarrow \begin{pmatrix} 0 & 1 & \mathbf{0} \\ 2 & 2 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 4\mathbf{I_{n-2}} \end{pmatrix}.$$

3. Let vectors $\mathbf{f_i}$ $(i = 1, 2, 3)$ be the factorisations of a_i/a_0 in terms of the primes in S.

4. Let $\mathbf{K_3} \leftarrow (\mathbf{f_3} \mid \mathbf{K_4})$, $\mathbf{K_2} \leftarrow (\mathbf{f_2} \mid \mathbf{K_3})$ and $\mathbf{K_1} \leftarrow (\mathbf{f_1} \mid \mathbf{K_2})$.

5. Let d_i $(i = 1, \ldots, 4)$ be the determinant of the Hermite normal form of $\mathbf{K_i}$.

6. Let $\mathbf{M}_{ii} \leftarrow d_i/d_{i+1}$ $(i = 1, 2, 3)$. Let $\mathbf{M}_{44} \leftarrow 1$.

7. Let $\mathbf{w_i}$ $(i = 1, 2, 3)$ be solutions of $\mathbf{K_i w_i} \equiv \mathbf{f_i} \pmod 4$.

8. Let $i \leftarrow 2$.

9. Let $j \leftarrow i - 1$.

10. Let $\mathbf{M}_{ij} \leftarrow \sum_{k=j+1}^{i} \mathbf{M}_{ik}(\mathbf{w_i})_k \times \mathbf{M}_{ii}/4$.

11. Let $j \leftarrow j - 1$. If $j \geq 1$, go to step 9.

12. Let $i \leftarrow i + 1$. If $i \leq 4$, go to step 8.

13. Reduce $\mathbf{M}$ to Hermite normal form.

14. For each i from 1 to 3, let $\mathbf{v}_i$ be either 0 if a_i/a_0 is positive, or 1 if a_i/a_0 is negative. Let $\mathbf{v}_4 \leftarrow 0$.

The implementation of this algorithm is listed in Section D.2.1.

3.5 Finding surfaces from subgroups

In this section we address the following problem: given a subgroup H of Γ, find conditions on the coefficients a_i which imply that the subgroup attached to the surface defined by the a_i is contained in H. What we will find is that, for example, a certain subgroup H might give the condition "a_1/a_0 is a square"; a smaller subgroup $H' \subset H$ might then give the condition "a_1/a_0 is 4 times a fourth power", which is clearly a narrowing of the first condition.

Whenever the a_i are rational numbers, the subgroup H associated to the surface defined by the a_i must satisfy $\mathbb{Q}(\epsilon)^H = \mathbb{Q}$. The arguments and algorithms developed here will be equally applicable to other base fields, but for the sake of clarity we will assume that the base field is $\mathbb{Q}$. A short function to find the constant field fixed by H is listed in Section D.2.2.

To set out the problem, we return to the situation described in Section 3.1. A set of coefficients a_i is described by a rational point a of the open subscheme U of 3-dimensional projective space; and this point has several points lying above it in $\tilde{U}$; we pick one of them and call it b. The question now is: what conditions must we impose on a to ensure that the decomposition group Γ_b of b be contained in H?

Let

$$A = \mathbb{Q}[s_1^{\pm}, s_2^{\pm}, s_3^{\pm}] \tag{3.9}$$

be the coordinate ring of U, and let

$$B = \mathbb{Q}(\epsilon)[t_1^{\pm}, t_2^{\pm}, t_3^{\pm}] \tag{3.10}$$

be the coordinate ring of $\tilde{U}$. Then Γ acts on B, and we write B^H for the subring of B fixed by H. The spectrum of B^H is the quotient scheme $\tilde{U}/H$ ([19], 1.1), and we let b' be the image of b in this quotient.

Lemma 3.12. *The decomposition group Γ_b of b is contained in H if and only if b' is a rational point of $\tilde{U}/H$.*

Proof. The Galois group of $k(b)/k(a)$ is Γ_b, and the Galois group of $k(b)/k(b')$ is $\Gamma_b \cap H$, both by ([19], 1.1). If b' is a rational point of $\tilde{U}/H$, then $k(b')$ is $\mathbb{Q}$ and the two Galois groups are the same; that is, Γ_b is contained in H. Conversely, if Γ_b is contained in H then by ([19], 2.2) the completed local rings at b' and a are isomorphic, and hence so are the residue fields, giving $k(b') = \mathbb{Q}$. $\square$

We have reduced the question to the following problem: which points of U are the images of rational points on $\tilde{U}/H$?

A rational point of $\tilde{U}/H$ is given by a homomorphism $B^H \to \mathbb{Q}$: that is, by a point in projective space $(1 : \alpha_{10} : \alpha_{20} : \alpha_{30})$, with the α_{i0} elements of $\bar{\mathbb{Q}}^\times$, such that the image of B^H under the map $t_i \mapsto \alpha_{i0}$ lies in $\mathbb{Q}$. The image of this point in U is a point $(a_0 : a_1 : a_2 : a_3)$, with the a_i non-zero and rational, such that the image of B^H under the map $t_i \mapsto a_i/a_0$ is contained in the set $(\mathbb{Q}^\times)^4$. Thus our conditions on the a_i will be of the form "certain monomials in the a_i lie in $(\mathbb{Q}^\times)^4$".

3.5.1 Computing B^H

Let H be a subgroup of Γ. The coordinate rings of the affine schemes U and $\tilde{U}$ are called A and B and were defined in (3.9) and (3.10) above. The group Γ acts on B by automorphisms; the subring fixed by this action is precisely equal to A. We now wish to find a set of elements which generate B^H, the subring of B fixed by H, as an algebra over A.

While B is conceptually a simple object, it can be regarded in several different ways: as an A-module; as an A-algebra; as a Γ-module; or as an $A[\Gamma]$-module.

First consider B as a module over A. A set of generators is given by the 256 elements of the form

$$x = t_1^{m_1} t_2^{m_2} t_3^{m_3} \sqrt{2}^{m_4} i^{m_5} \tag{3.11}$$

where m_1, m_2 and m_3 take values from 0 to 3; and m_4 and m_5 take values 0 or 1. Now the action of any of the generators of Γ given in (3.2) is to take x to either x, $-x$, ix or $-ix$. Thus the A-submodule of B generated by x and ix is fixed under the action of Γ, which we may write as the following lemma.

Lemma 3.13. *As an $A[\Gamma]$-module, B is the direct sum of 128 submodules; these are each generated by an element x, of the form* (3.11) *with $m_5 = 0$.* $\square$

This means that to find B^H, it is enough to find the fixed part of each submodule separately.

Let x be an element of the form (3.11) with $m_5 = 0$, and let H be a subgroup of Γ given by a set of generators as in Proposition 3.8. Let B_x denote the $A[\Gamma]$-module generated by x, that is, the free A-module generated by x and ix. An element of B_x is fixed by H if and only if it is fixed by each generator of H.

First, we consider the four generators $h_1, \ldots, h_4$ which fix i. The subgroup of H they generate is called H' and is Abelian.

Lemma 3.14. *The submodule of B_x fixed by H' is*

$$B_x^{H'} = \begin{cases} B_x & \text{if } H' \text{ fixes } x \\ \{0\} & \text{otherwise} \end{cases}$$

Proof. Since H' commutes with multiplication by i, we can (compatibly with the action of H') think of B_x as the rank-1 free module over $A[i]$ generated by x. A rank-1 free module is fixed by a group action if and only if its single generator is fixed. □

We return to the running example of the previous section, where the group H is given by (3.4). Let x be a general element of the form (3.11). We find:

- Every x is fixed by h_1, which equals the identity.
- x is fixed by $h_2 = \sigma_2^2$ if and only if m_2 is even.
- x is fixed by $h_3 = \sigma_2\sigma_3$ if and only if $m_2 + m_3 = 0 \pmod 4$.
- x is fixed by $h_4 = \sigma_2\sigma_4$ if and only if $2m_2 + m_4 = 0 \pmod 4$.

Combining these results, those x which are fixed by the whole of H' have either $m_2 = m_3 = m_4 = 0$; or $m_2 = m_3 = 2$ and $m_4 = 1$. That is,

$$x = \begin{cases} t_1^{m_1} i^{m_5} \\ t_1^{m_1} t_2^2 t_3^2 \sqrt{2} i^{m_5} \end{cases} . \tag{3.12}$$

Next we must find the part of B_x which is fixed by τh_5, the remaining generator of H. Enumerating the possible cases gives the following:

Lemma 3.15. *The submodule of B_x fixed by τh_5 is*

$$B_x^{\tau h_5} = \begin{cases} Ax & \textit{if } h_5 x = x \\ Aix & \textit{if } h_5 x = -x \\ A(1-i)x & \textit{if } h_5 x = ix \\ A(1+i)x & \textit{if } h_5 x = -ix \end{cases}$$

□

We note, for computational use, that an alternative statement is this: if $h_5 x = i^k x$, then the part of B_x fixed by τh_5 is generated over A by $(1+i)^{-k}x$.

In the example, the elements (3.12) are fixed by the automorphism $h_5 = \tau\sigma_2\sigma_3$ if and only if $m_5 = 0$. Therefore B^H is generated as a module over A by the eight elements $\{t_1^{m_1} \mid m_1 = 0, \ldots, 3\}$ and $\{\sqrt{2}t_1^{m_1}t_2^2t_3^2 \mid m_1 = 0, \ldots, 3\}$.

These two lemmas together allow us to find a generating set for B^H as a module over A. With very little extra effort, we can turn this into a generating set for B^H as an algebra over A.

Lemma 3.16. *Let X be the finite subgroup of $B^\times/A^\times$ generated by the five elements t_1, t_2, t_3, $\sqrt{2}$ and $(1+i)$. Any generating set for X^H also generates B^H as an algebra over A.*

Proof. From the previous two lemmas, we may find a generating set for B^H as a module over A with all generators contained in X: that is, X^H generates B^H as a module over A. So any multiplicative generating set for X^H must therefore generate B^H as an algebra over A. □

In the example, B^H is generated as an algebra over A by the two elements t_1 and $\sqrt{2}t_2^2t_3^2$.

To write down an algorithm for computing a generating set for B^H, let x be as in (3.11) with $m_5 = 0$, and suppose that σ is an element of Γ' given by

$$\sigma = \sigma_1^{n_1}\sigma_2^{n_2}\sigma_3^{n_3}\sigma_4^{n_4}.$$

Then the action of σ on x is to multiply x by $\exp(k(\sigma,x)\pi/2)$, where

$$k(\sigma,x) = n_1m_1 + n_2m_2 + n_3m_3 + 2n_4m_4.$$

The following algorithm accomplishes these computations.

Algorithm 3.17. Given a matrix-vector representation $(\mathbf{M},\mathbf{v})$ of a subgroup H of Γ, this algorithm finds a matrix $\mathbf{N}$ whose columns are the coordinates, on the ordered basis $(1+i, \sqrt{2}, t_1, t_2, t_3)$, of a set of generators for B^H as an algebra over A.

1. Let $\mathbf{N}$ be the 5×5 diagonal matrix with diagonal entries 4, 2, 4, 4, 4.

2. Let $m_i \leftarrow 0$ $(i = 1,\dots,4)$.

3. If

$$m_1\mathbf{M}_{j1} + m_2\mathbf{M}_{j2} + m_3\mathbf{M}_{j3} + 2m_4\mathbf{M}_{j4} \equiv 0 \pmod 4$$

   for all $j = 1,\dots,4$, then go to step 4; else go to step 6.

4. If $\mathbf{v}$ is empty, let $k \leftarrow 0$. Otherwise, let

$$k \leftarrow m_1\mathbf{v}_1 + m_2\mathbf{v}_2 + m_3\mathbf{v}_3 + 2m_4\mathbf{v}_4$$

5. (Apply Lemma 3.15.) Let

$$\mathbf{N} \leftarrow \left(\begin{array}{cc} & -k \\ & m_4 \\ \mathbf{N} & m_1 \\ & m_2 \\ & m_3 \end{array}\right)$$

6. Repeat steps 3–5 for m_1, m_2,m_3 taking all values between 0 and 3, and for m_4 taking values 0 and 1.

7. If $\mathbf{v}$ is empty, let

$$\mathbf{N} \leftarrow \begin{pmatrix} & 2 \\ & 0 \\ \mathbf{N} & 0 \\ & 0 \\ & 0 \end{pmatrix}$$

8. Put N into Hermite normal form.

The implementation of this algorithm is listed in Section D.2.3.

3.5.2 Giving examples

Once a set of conditions on the coefficients a_i is given, a convenient and simple extension is to give 'generic' coefficients which satisfy the conditions. For example, the condition "a_1/a_0 is a square, and a_3/a_2 is 4 times a fourth power" is satisfied by any numbers of the form $(1, c_1^2, c_2, 4c_2)$, where c_1 and c_2 are arbitrary rational numbers; conversely, up to projective equivalence and multiplication by fourth powers, any set of coefficients satisfying the conditions must be of this form. Of course, taking c_1 and c_2 to be insufficiently 'general' may give coefficients whose surface falls into a more specific case than the general one under consideration: thus the surface $(1, 1, 1, 4)$ has rather different properties from the general surface satisfying these conditions.

From Algorithm 3.17 we obtain a matrix in Hermite normal form, whose columns represent monomials in the α_{i0} which must lie in $\mathbb{Q}$. Assuming that the constant field for the subgroup under consideration is $\mathbb{Q}$, the first two columns will always represent $(1+i)^4$ and $\sqrt{2}^2$; the remaining three columns contain the information we need. As remarked above, we may take fourth powers of these monomials to obtain monomials in the a_i which we will require to lie in $(\mathbb{Q}^\times)^4$.

The last three columns of the matrix give us conditions of this form:

$$\begin{aligned} (-1)^{n_{13}} 4^{n_{23}} a_1^{n_{33}} &\in (\mathbb{Q}^\times)^4 \\ (-1)^{n_{14}} 4^{n_{24}} a_1^{n_{34}} a_2^{n_{44}} &\in (\mathbb{Q}^\times)^4. \\ (-1)^{n_{15}} 4^{n_{25}} a_1^{n_{35}} a_2^{n_{45}} a_3^{n_{55}} &\in (\mathbb{Q}^\times)^4 \end{aligned} \tag{3.13}$$

To turn these conditions into general forms for the a_i, we simply:

- set each expression in (3.13) equal to a rational fourth power c_i^4;
- solve each equation in turn to express each a_i in terms of the c_i;
- cast out any fourth powers.

In our example, the previous algorithm produces three expressions which generate B^H: t_1, t_2^4 (a trivial generator) and $\sqrt{2}t_2^2t_3^2$. This means that, for the surface with coefficients $(1, a_1, a_2, a_3)$ to give rise to a subgroup contained in H, the following conditions must be satisfied:

$$\begin{aligned} \alpha_{10} &\in \mathbb{Q} \\ \alpha_{20}^4 &\in \mathbb{Q} \\ \sqrt{2}\alpha_{20}^2\alpha_{30}^2 &\in \mathbb{Q}. \end{aligned}$$

Setting these expressions equal to rational numbers c_1, c_2, c_3, setting $a_0 = 1$ and taking appropriate powers, we get

$$\begin{aligned} a_1 &= c_1^4 \\ a_2 &= c_2 \\ 2a_2a_3 &= c_3^2. \end{aligned}$$

We can now rearrange these equations and cast out fourth powers to get

$$(a_0, a_1, a_2, a_3) = (1, 1, c_2, 2c_3^2c_2^3).$$

Substituting any sufficiently general values for c_2 and c_3 will give a surface whose associated subgroup is H. For example, we can recover the surface (3.8) by taking $c_2 = -6$ and $c_3 = 1/6$.

The algorithm is as follows.

Algorithm 3.18. Given a subgroup H of Γ as a matrix-vector representation $(\mathbf{M}, \mathbf{v})$, such that $\mathbb{Q}(\epsilon)^H = \mathbb{Q}$, this algorithm computes monomials $P_1(X)$,

$P_2(X, Y)$, $P_3(X, Y, Z)$ such that, for sufficiently general rational constants c_i, the surface defined by the coefficients

$$(1, P_1(c_1), P_2(c_1, c_2), P_3(c_1, c_2, c_3))$$

gives rise to the subgroup H.

1. Compute $\mathbf{N}$ using Algorithm 3.17.

2. Let
$$\mathbf{N} \leftarrow \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ & & \mathbf{N} & & \end{pmatrix}$$

3. Let $i \leftarrow 3$.

4. Let $\mathbf{N}_{(i)} \leftarrow \mathbf{N}_{(i)} \times 4/\mathbf{N}_{i+3,i}$.

5. For each $3 \leq j < i$, let $\mathbf{N}_{(i)} \leftarrow \mathbf{N}_{(i)} - (\mathbf{N}_{j+3,i}/\mathbf{N}_{j+3,j})\mathbf{N}_{(j)}$.

6. Let $i \leftarrow i + 1$. If $i \leq 5$, go to step 3.

7. For each $i = 1, \ldots, 3$, let
$$P_i \leftarrow (1+i)^{\mathbf{N}_{4i}} \sqrt{2}^{\mathbf{N}_{5i}} X^{\mathbf{N}_{1i}} Y^{\mathbf{N}_{2i}} Z^{\mathbf{N}_{3i}}.$$

8. Cast out any powers of 4 from each P_i.

An implementation of this algorithm is shown in Section D.2.4.

3.6 Cohomology of the Picard group

Our goal in studying the Picard group of the surface V is to be able to compute certain cohomological invariants of it. Specifically, we are interested in $H^0(\mathbb{Q}, \operatorname{Pic} \bar{V})$, which is the part of the Picard group defined over $\mathbb{Q}$; and in $H^1(\mathbb{Q}, \operatorname{Pic} \bar{V})$, which is related to the Brauer group of V and will be discussed further in the following chapter. Here we present the algorithms for calculating these invariants.

3.6.1 Computing with G-modules

In this section we present some general routines for performing calculations on free Abelian groups with a group action. Here G will be a finitely generated group, and M a free $\mathbb{Z}$-module of finite rank on which G acts by automorphisms. We will be concerned with calculating the first two cohomology groups $H^0(G, M)$ and $H^1(G, M)$.

The concrete representation of a G-action used is as follows: first pick generators $g_1, \ldots, g_n$ for G; then let $\mathbf{M_i}$ be the matrix for the action of g_i on M, with respect to some previously chosen basis. The vector $(\mathbf{M_i})_{i=1}^n$ is the object which will be used in algorithms to represent the G-module M.

The calculation of $H^0(G, M)$, the part of M fixed by the action of G, is extremely simple, and is given here only for completeness. We assume that we already have the basic algorithms to perform basic matrix calculations, as provided for example by PARI.

Algorithm 3.19. Given a vector $(\mathbf{M_i})_{i=1}^n$ of matrices representing a group action on a free $\mathbb{Z}$-module M of rank r, this algorithm calculates a matrix $\mathbf{U}$ whose columns form a basis for $H^0(G, M)$.

1. Let $\mathbf{U}$ be a matrix whose columns form a basis for the kernel of $\mathbf{M_1} - \mathbf{I_r}$.

2. If $n = 1$, terminate. Otherwise, let $i \leftarrow 2$.

3. Let $\mathbf{V}$ be a matrix whose columns form a basis for the kernel of $\mathbf{M_i} - \mathbf{I_r}$.

4. Let $\mathbf{U}$ be a matrix whose columns form a basis for the intersection of the two lattices generated by the columns of $\mathbf{U}$ and $\mathbf{V}$, respectively.

5. Let $i \leftarrow i + 1$. If $i \leq n$, go to step 3.

This algorithm is listed in Section D.3.1.

We now turn to calculating the $H^1(G, M)$. We do this by dimension-shifting. The sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

of $\mathbb{Z}$-modules is exact. M is torsion-free, hence flat, and so tensoring the previous sequence with M gives another exact sequence

$$0 \to M \to M \otimes \mathbb{Q} \to M \otimes \mathbb{Q}/\mathbb{Z} \to 0. \tag{3.14}$$

The long exact sequence in cohomology associated to (3.14) is

$$\cdots H^0(G, M \otimes \mathbb{Q}) \to H^0(G, M \otimes \mathbb{Q}/\mathbb{Z}) \xrightarrow{\partial} H^1(G, M) \to 0 \tag{3.15}$$

that is, every element of $H^1(G, M)$ is of the form

$$\sigma \mapsto \sigma x - x$$

for some x in $M \otimes \mathbb{Q}$ which is fixed modulo M by the action of G; such an element is a coboundary if and only if we may take the corresponding x to lie in $M + H^0(G, M \otimes \mathbb{Q})$. This is exactly the same description of $H^1(G, M)$ as that given in [43], and may be written as

$$H^1(G, M) \cong \frac{H^0(G, M \otimes \mathbb{Q}/\mathbb{Z})}{\operatorname{im} H^0(G, M \otimes \mathbb{Q})}. \tag{3.16}$$

The inverse map, from $H^1(G, M)$ to $H^0(G, M \otimes \mathbb{Q}/\mathbb{Z})$, is given by

$$\alpha \mapsto \frac{1}{|G|} \sum_{\sigma \in G} \alpha(\sigma) \tag{3.17}$$

which is clearly a left inverse to the coboundary.

For computation, we use the well-known fact that $H^1(G, M)$ is killed by the order of G, which we will write as m. Thus $H^0(G, M \otimes \mathbb{Q}/\mathbb{Z})$ is actually contained in the m-torsion subgroup, and (multiplying through by m) we can rewrite (3.16) as

$$H^1(G,M) = H^1(G,M)[m] \cong \frac{H^0(G, M \otimes \mathbb{Z}/m\mathbb{Z})}{\operatorname{im} H^0(G,M)}. \tag{3.18}$$

This isomorphism can equally well be derived from the exact sequence

$$0 \to M \xrightarrow{\times m} M \to M \otimes \mathbb{Z}/m\mathbb{Z} \to 0$$

and is valid for any G-module M with no m-torsion.

We will calculate the top and bottom of the quotient (3.18), and then apply Algorithm 3.7 to find generators for the quotient. The bottom expression is essentially already found by Algorithm 3.19; for the top we will adapt that algorithm slightly to work modulo m. The only change necessary is to calculate the kernel of a matrix modulo m, and this is performed by the PARI function `matsolvemod`. The modified algorithm is listed in Section D.3.2.

The whole algorithm for calculating $H^1(G,M)$ is described below. We work in $M \otimes \mathbb{Z}/m\mathbb{Z}$; all matrices represent subgroups of this group.

Algorithm 3.20. Given a vector $(\mathbf{M_i})_{i=1}^n$ of matrices representing a group action on a free $\mathbb{Z}$-module M of rank r, this algorithm calculates a matrix $\mathbf{U}$ whose columns represent elements of $M \otimes \mathbb{Q}$, the coboundaries of which form a Smith normal form basis for the m-torsion of $H^1(G,M)$; and a diagonal matrix D in Smith normal form describing the orders of those generators.

1. Let $\mathbf{V}$ be a matrix whose columns form a basis for $H^0(G,M)$, using Algorithm 3.19.

2. Let $\mathbf{V} \leftarrow (\mathbf{V} \mid m\mathbf{I_r})$.

3. Put $\mathbf{V}$ into Hermite normal form. This is in fact Algorithm 3.6.

4. Let $\mathbf{W}$ be a matrix whose columns form a basis for $H^0(G, M \otimes \mathbb{Z}/m\mathbb{Z})$, using the modified version of Algorithm 3.19.

5. Apply Algorithm 3.7 to $\mathbf{V}$ and $\mathbf{W}$ to obtain a matrix $\mathbf{U}$, whose columns form a Smith normal form basis for the quotient in (3.18), and a matrix $\mathbf{D}$ in Smith normal form describing the orders of these generators.

6. Let $\mathbf{U} \leftarrow \mathbf{U}/m$.

This algorithm is listed in Section D.3.3.

3.6.2 The action on the Picard group

In order to apply the general results of the previous section to the group $\operatorname{Pic} \bar{V}$, we must find the matrices representing generators of a subgroup H of Γ. This section describes that simple procedure.

The Picard group is generated by the 48 straight lines L_{mn}^{pqr} on V, as defined in (1.2)–(1.4). The action of $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the lines is the same as the action on the generic lines $\tilde{L}$, defined in (3.3), of the subgroup H of Γ associated to the surface V. We will use the same names to refer to the generic lines as the specific ones:

$$L_{mn}^{pqr} : \{X_0 = \epsilon^m t_p X_p,\ X_q = \epsilon^n (t_r/t_q) X_r\}. \tag{3.19}$$

The action of Γ is simply that induced by its action on B, the coordinate ring of $\tilde{U}$:

$$\sigma L_{mn}^{pqr} : \{X_0 = \sigma(\epsilon^m t_p) X_p,\ X_q = \sigma(\epsilon^n (t_r/t_q)) X_r\}$$

which is another line, of the form $L_{m'n'}^{pqr}$. Let σ be the element of Γ' defined by

$$\sigma = \sigma_1^{n_1} \sigma_2^{n_2} \sigma_3^{n_3} \sigma_4^{n_4} \quad ; \tag{3.20}$$

then, remembering that $\epsilon = (1+i)/\sqrt{2}$, we see that

$$\begin{aligned} m' &\equiv m + 2(2n_4 + n_p) \pmod 8 \\ n' &\equiv n + 2(2n_4 - n_q + n_r) \pmod 8. \end{aligned} \tag{3.21}$$

Also, $\tau L_{mn}^{pqr} = L_{-m,-n}^{pqr}$. Let Λ denote the free $\mathbb{Z}$-module of rank 48 generated by the lines, which is a subgroup of $\operatorname{Div} \bar{V}$. We have shown that Λ, as a Γ-module, is the direct sum of three Γ-modules Λ^1, Λ^2, Λ^3: here Λ^1 is generated by the 16 lines L_{mn}^{123}, and similarly for the other two cases. Now Λ^1 is isomorphic to the free $\mathbb{Z}$-module generated by the 16 elements $(\epsilon^m t_1, \epsilon^n (t_3/t_2))$, with the obvious Γ-action; and this in turn is the tensor product, over $\mathbb{Z}$, of two free modules of rank 4, the first generated by the $\epsilon^m t_1$ and the second by the $\epsilon^n(t_3/t_2)$. The representation of the element σ, defined by (3.20), on this module is then given easily by (3.21).

Lemma 3.21. *Let M be the free $\mathbb{Z}$-module generated by the four elements $\epsilon^m(t_i/t_j)$, where i and j are fixed and m takes the values 1, 3, 5, 7; and let Γ act on M by permuting these generators in the natural way. Let σ be defined by (3.20). Then the matrix for the action of σ on M is given by*

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}^{2n_4+n_i-n_j}$$

and the matrix for the action of τ on M is given by

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

□

It is then straightforward to calculate the matrix for an element of Γ acting on, say, Λ^1 as follows: take the two 4×4 matrices for the action on the modules generated by the $\epsilon^m t_1$ and the $\epsilon^n(t_3/t_2)$ respectively, and then compute the tensor product of the two matrices. The matrix for that element of Γ acting on the whole of Λ is formed simply by combining the matrices for Λ^1, Λ^2 and Λ^3 diagonally into one 48×48 matrix.

When implementing the algorithm, we may order the 48 lines L_{mn}^{pqr} first by p, then by m, and finally by n: thus the basis is

$$L_{11}^{123}, L_{13}^{123}, \ldots, L_{75}^{312}, L_{77}^{312}. \tag{3.22}$$

Algorithm 3.22. Given an element $\tau^{n_5}\sigma$ of Γ, where n_5 is either 0 or 1 and σ is given by (3.20) and so lies in Γ', this algorithm computes a matrix $\mathbf{M}$ which represents the action of this element of Γ on the module Λ, where the basis for Λ consists of the 48 lines ordered as in (3.22).

1. Let $p \leftarrow 1$.

2. Let
$$\mathbf{A} \leftarrow \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}^{2n_4+n_p}.$$

3. Let
$$\mathbf{B} \leftarrow \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}^{2n_4-n_{p+1}+n_{p+2}}$$
where the indices $p+1$, $p+2$ are taken modulo 3, to lie in the set $\{1,2,3\}$.

4. If $n_5 = 1$, let
$$\mathbf{A} \leftarrow \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}\mathbf{A} \quad , \quad \mathbf{B} \leftarrow \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}\mathbf{B}.$$

5. Let $\mathbf{M_p}$ be the 16×16 matrix such that
$$(\mathbf{M_p})_{i+4(k-1),j+4(l-1)} = \mathbf{A}_{ij}\mathbf{B}_{kl}.$$

6. Let $p \leftarrow p+1$. If $p \leq 3$, go to step 2.

7. Let
$$\mathbf{M} \leftarrow \begin{pmatrix} \mathbf{M_1} & 0 & 0 \\ 0 & \mathbf{M_2} & 0 \\ 0 & 0 & \mathbf{M_3} \end{pmatrix}.$$

The implementation of this algorithm is listed in Section D.3.4.

We now must choose a basis for $\operatorname{Pic} \bar{V}$ and a surjective map α from Λ to $\operatorname{Pic} \bar{V}$, and thence represent elements of Γ acting on $\operatorname{Pic} \bar{V}$. As every surjective map of vector spaces has an injective left inverse, we may take $\operatorname{Pic} \bar{V}$ to be embedded in $\Lambda \otimes \mathbb{Q}$.

We recall from Proposition 2.10 that linear and algebraic equivalence of divisors on K3 surfaces are both the same as numerical equivalence: thus if Λ^0 denotes the kernel of the intersection form on Λ, then $\operatorname{Pic} \bar{V}$ is isomorphic to the quotient Λ/Λ^0. The intersection pairing is easily calculated from the explicit equations of the 48 lines:

$$(L^{pqr}_{mn}, L^{pqr}_{ij}) = \begin{cases} -2 & \text{if } m = i \text{ and } n = j \\ 1 & \text{if } m = i \text{ or } n = j \text{, but not both} \\ 0 & \text{otherwise;} \end{cases}$$
$$(L^{pqr}_{mn}, L^{qrp}_{ij}) = \begin{cases} 1 & \text{if } n - m \equiv i + j \pmod 8 \\ 0 & \text{otherwise.} \end{cases}$$

Let Q be the 48×48 matrix representing this quadratic form; then Λ^0 is the (left or right) kernel of Q. We now consider the properties we would like our basis of $\operatorname{Pic} \bar{V}$ to have. It is helpful to take the class of a plane section, denoted by Π, to be the first basis vector. Now ideally the remaining basis vectors would be orthogonal to Π with respect to the intersection pairing; but this is impossible, as the resulting lattice is of finite index in $\operatorname{Pic} \bar{V}$ but is not the whole of it. Instead, we do the following:

1. Choose a $\mathbb{Q}$-basis for Λ^0.
2. Extend this to a $\mathbb{Q}$-basis for $\langle \Pi \rangle^\perp$; call the vector space spanned by the new basis vectors A.

3. The chosen basis for $\operatorname{Pic} \bar{V}$ will be the Hermite normal form basis for the image of Λ when projected along Λ^0 onto $\Pi \oplus A$.

We will consider the lattice spanned by this basis to be our concrete representation of $\operatorname{Pic} \bar{V}$. The implementation of the algorithm for calculating this basis is listed in Section D.3.5.

Finally, we can represent an element of Γ on this basis of $\operatorname{Pic} \bar{V}$. Let $\mathbf{D}$ be the matrix whose columns are our chosen basis for $\operatorname{Pic} \bar{V}$, expressed as elements of $\Lambda \otimes \mathbb{Q}$; and let $\mathbf{E}$ be the matrix representing the projection map along Λ^0 onto $\operatorname{Pic} \bar{V}$, with respect to this basis. If σ is an element of Γ, and $\mathbf{M}$ is the matrix produced by Algorithm 3.22 corresponding to σ, then the matrix representing the action of σ on our basis of $\operatorname{Pic} \bar{V}$ is given by $\mathbf{EMD}$. This allows us to represent any subgroup H of Γ in the form needed to apply the algorithms of Section 3.6.1 to H acting on $\operatorname{Pic} \bar{V}$.

Chapter 4

The Brauer group

Here we investigate the Brauer group of the surface V. After recalling the definition and properties of the Brauer group of a scheme, we relate it in Section 4.1 to the cohomology of the Picard group of $\bar{V}$. This enables us in Section 4.2 to apply the computational machinery of the previous chapter to calculate the Brauer group of V according to the parameters a_0, a_1, a_2, a_3. The case of cyclic algebras is studied in greater detail in Section 4.3. In Section 4.4, we look at the so-called vertical Brauer group attached to a fibration $V \to \mathbb{P}^1$. The chapter concludes with a worked example of the case studied by Swinnerton-Dyer in [44], showing how the theory described in the chapter relates to the calculations given there.

Background on the Brauer groups of fields may be found in Serre [35] or, in an earlier but more explicit form, in Deuring's book [15]. The canonical reference for Brauer groups of schemes is the set of three articles by Grothendieck [18]. An account is also given in Milne's book [29]. Section 1 of [13] recounts much of the theory which we will use here.

4.1 Background

The Brauer group of a field k, written $\mathrm{Br}\, k$, is a well-known object, the group of equivalence classes of central simple algebras over that field. It features heavily in the study of the arithmetic of the field; in particular, much of class field theory is concerned with Brauer groups. It is easily shown that $\operatorname{Br} k$ is isomorphic to the cohomology group $H^2(k, \bar{k}^\times)$.

The definition of the Brauer group may be extended to an arbitrary scheme, as described in detail in [18]. The idea is as follows.

Definition 4.1. An *Azumaya algebra* on a scheme X is a coherent $\mathcal{O}_X$-module $\mathcal{A}$, with the structure of an algebra over $\mathcal{O}_X$, such that the specialisation of $\mathcal{A}$ at each point x of X is a central simple algebra over the residue field at x. Equivalently, $\mathcal{A}$ is locally (for the étale topology) isomorphic to a matrix algebra. An Azumaya algebra is *trivial* if it is isomorphic to the sheaf of endomorphisms of some locally free $\mathcal{O}_X$-module. The *Brauer group* of X, written $\operatorname{Br} X$, is the group of equivalence classes of Azumaya algebras modulo trivial ones.

When X is $\operatorname{Spec} K$ for some field K, this definition agrees with the usual definition of the Brauer group of a field.

There is a natural map $\operatorname{Br} X \to \operatorname{Br} \bar{X}$. We will be entirely concerned with the part of $\operatorname{Br} X$ which vanishes under this map, which we will call the *arithmetic* part of the Brauer group of X, and denote by $\operatorname{Br}_1(X)$. This consists of those Azumaya algebras on X which are split by some finite extension of the base field.

There is always an injection $\operatorname{Br} X \to H^2(X, \mathbb{G}_\mathrm{m})$; under certain conditions this is known to be an isomorphism. In particular, this is true when X is a smooth surface. We will use this cohomological description of the Brauer group to produce alternative descriptions of Azumaya algebras.

4.1.1 Cohomological theory

In this section, X is a connected smooth projective variety over a field k of characteristic 0. The algebraic closure of k will be denoted by $\bar{k}$, and $\bar{X}$ will mean $X \times_k \bar{k}$. The field of rational functions on X will be denoted by $k(X)$.

The machinery used in this section is described in many texts. The canonical reference is [14], and other useful accounts may be found in the books by Milne [29] and Tamme [45], and also the lecture notes by Milne [28].

We will study the cohomology of the sheaf $\mathbb{G}_m$ on X and also of the sheaf of divisors on X. In this section and later, a useful tool will be the following form of the Hochschild–Serre spectral sequence:

Lemma 4.2. *Let k' be a (possibly infinite) Galois extension of k. Write G for $\mathrm{Gal}(k'/k)$, and X' for $X \times_k k'$. Let $\mathcal{F}$ be a sheaf on X. Then there is a spectral sequence*

$$E_2^{pq} = H^p(G, H^q(X', \mathcal{F})) \implies H^{p+q}(X, \mathcal{F}).$$

Proof. See [29] or any of several other references. □

Applying this to $k' = \bar{k}$ and $\mathcal{F} = \mathbb{G}_m$, we get a filtration on $H^2(X, \mathbb{G}_m)$:

$$0 \subseteq \operatorname{im} \operatorname{Br} k \subseteq \ker(H^2(X, \mathbb{G}_m) \to H^2(\bar{X}, \mathbb{G}_m)) \subseteq H^2(X, \mathbb{G}_m). \tag{4.1}$$

Here the successive quotients of the filtration are isomorphic to: the image of $\operatorname{Br} k$; $H^1(k, \operatorname{Pic} \bar{X})$; and some subgroup of $H^0(k, H^2(\bar{X}, \mathbb{G}_m))$. These three pieces of $H^2(X, \mathbb{G}_m)$ might be described as follows.

- The image of $\operatorname{Br} k$ is the *constant* Brauer group of X, written $\operatorname{Br}_0 X$. Constant elements can produce no Brauer–Manin obstruction. The study of Brauer groups of fields is an essential part of class field theory.

- The group consisting of those elements which split over some finite extension of the base field k is written $\operatorname{Br}_1 X$. The second piece of the filtration is $\operatorname{Br}_1 X / \operatorname{Br}_0 X$. This is the arithmetic part, in which we are interested. The isomorphism between this part of the Brauer group and $H^1(k, \operatorname{Pic} \bar{X})$ will be our means of calculating this part of the group.

- The final piece of $H^2(X, \mathbb{G}_m)$ consists of elements of $H^2(\bar{X}, \mathbb{G}_m)$. These have been studied in a geometric context, being related to those homology classes on $\bar{X}$ which do not contain an algebraic cycle. This might be described as the *geometric* part of the Brauer group of X. These elements can under some circumstances give rise to non-trivial Brauer–Manin obstructions: see Harari's example [20].

We now prove some general and well-known results about the cohomology of various sheaves.

Let $\eta = \operatorname{Spec} k(X)$ denote the generic point of X, and j the inclusion map $\eta \to X$. The direct image sheaf $j_*\mathbb{G}_\mathrm{m}$ is simply the sheaf of rational functions on X; there is a canonical inclusion, of sheaves on X, of $\mathbb{G}_\mathrm{m}$ into $j_*\mathbb{G}_\mathrm{m}$. The quotient sheaf is by definition the sheaf of Cartier divisors on X, denoted by $\mathcal{D}_X$. In the case we are considering, this is isomorphic to the sheaf of Weil divisors on X:

$$\mathcal{D}_X \cong \bigoplus_{x \in X^{(1)}} i_{x*}\mathbb{Z}$$

where $X^{(1)}$ is the set of points of X of codimension 1 (that is, generic points of closed subschemes of codimension 1) and i_x is the inclusion $x \to X$. The short exact sequence

$$0 \to \mathbb{G}_\mathrm{m} \to j_*\mathbb{G}_\mathrm{m} \to \mathcal{D}_X \to 0$$

gives rise to a long exact sequence in cohomology, part of which is

$$H^1(X, \mathcal{D}_X) \to H^2(X, \mathbb{G}_\mathrm{m}) \to H^2(X, j_*\mathbb{G}_\mathrm{m}) \to H^2(X, \mathcal{D}_X) \tag{4.2}$$

The second term of this sequence is the one which interests us. We will now describe the other terms.

Lemma 4.3. $H^1(X, \mathcal{D}_X) = 0$.

Proof. Cohomology commutes with direct sums of sheaves, so it is enough to show that $H^1(X, i_{x*}\mathbb{Z}) = 0$ for all points $x \in X^{(1)}$. The Leray spectral sequence [28, Theorem 12.8] shows that $H^1(X, i_{x*}\mathbb{Z})$ injects into $H^1(x, \mathbb{Z})$; and this last group is a Galois cohomology group which is equal to

$$\operatorname{Hom}(\operatorname{Gal}(\overline{k(x)}/k(x)), \mathbb{Z})$$

and therefore is zero, as the Galois group is by definition profinite and $\mathbb{Z}$ is free. $\square$

Corollary 4.4. *The map* $H^2(X, \mathbb{G}_m) \to H^2(X, j_*\mathbb{G}_m)$ *in* (4.2) *is injective.* $\square$

Lemma 4.5. $H^i(X, j_*\mathbb{G}_m) = H^i(k(X), \mathbb{G}_m)$ *for all* $i \geq 0$.

Proof. By the Leray spectral sequence, it is enough to show that $R^i j_*\mathbb{G}_m = 0$ for all $i \geq 1$. If $\bar{x}$ is any geometric point of X, then the stalk of $R^i j_*\mathbb{G}_m$ at $\bar{x}$ is given by $H^i(\operatorname{Spec} \mathcal{O}_{X,\bar{x}} \times_X \eta, \mathbb{G}_m)$. Now the fibre product in that expression is simply the spectrum of the field of fractions of $\mathcal{O}_{X,\bar{x}}$; and by a theorem of Lang [28, 13.5] such fields are quasi-algebraically closed, hence the result. $\square$

Corollary 4.6. *The exact sequence* (4.2) *becomes*

$$0 \to H^2(X, \mathbb{G}_m) \to \operatorname{Br} k(X) \to H^2(X, \mathcal{D}_X). \quad \square$$

We now suppose that X is such that $\operatorname{Br} X = H^2(X, \mathbb{G}_m)$. As stated above, we are primarily interested in the arithmetic part $\operatorname{Br}_1 X$ of the Brauer group of X. It turns out that to study this part of the Brauer group we only have to use Galois cohomology:

Corollary 4.7. *There is an exact sequence*

$$0 \to \operatorname{Br}_1 X \to \operatorname{Br}(k(\bar{X})/k(X)) \to H^2(k, \operatorname{Div} \bar{X})$$

that is, a central simple algebra over $k(X)$*, which is split by some finite extension of the base field* k*, is Azumaya if and only if it maps to zero in* $H^2(k, \operatorname{Div} \bar{X})$.

Proof. By Corollary 4.6 applied to X and $\bar{X}$, we have a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \operatorname{Br} X & \longrightarrow & \operatorname{Br} k(X) & \longrightarrow & H^2(X, \mathcal{D}_X) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \operatorname{Br} \bar{X} & \longrightarrow & \operatorname{Br} k(\bar{X}) & \longrightarrow & H^2(\bar{X}, \mathcal{D}_{\bar{X}}) \end{array}$$

where the kernels of the vertical maps are, from left to right: $\operatorname{Br}_1 X$ (by definition); $\operatorname{Br}(k(\bar{X})/k(X))$ (by the inflation-restriction exact sequence); and

$H^2(k, \operatorname{Div} \bar{X})$ (by Lemma 4.3 and the Hochschild–Serre spectral sequence). Hence the exact sequence of kernels is the desired result. □

Since we are interested in studying the Brauer–Manin obstruction, we only wish to consider elements of $\operatorname{Br} X$ up to constant algebras. There is an exact sequence of Galois cohomology

$$H^2(k, \bar{k}^\times) \to H^2(k, k(\bar{X})^\times) \to H^2(k, k(\bar{X})^\times/\bar{k}^\times) \to H^3(k, \bar{k}^\times)$$

and Tate has proved [46, p. 199] that the last group is always trivial when k is a number field; thus the middle map is surjective. Moreover, the map $k(\bar{X})^\times \to \operatorname{Div} \bar{X}$ is zero on $\bar{k}^\times$ and so factors through $k(\bar{X})^\times/\bar{k}^\times$. We may therefore define the following group, whose calculation will concern us in this chapter:

$$H^2_{\mathrm{Az}}(X) := \ker\left(H^2(k, k(\bar{X})^\times/\bar{k}^\times) \to H^2(k, \operatorname{Div} \bar{X})\right). \tag{4.3}$$

4.1.2 Change of fields

It will sometimes be necessary to consider how the various groups defined above vary as the base field of X changes. We state here some simple results. If X is defined over a field k, and K/k is a field extension, we write X_K for $X \times_k K$.

Lemma 4.8. *Let L/K be a Galois extension of fields. Then the following two conditions are equivalent:*

1. $\operatorname{Pic} X_K = H^0(L/K, \operatorname{Pic} X_L)$;
2. $H^1(L/K, k(X_L)^\times/L^\times) = 0$.

Proof. We consider the long exact sequence in cohomology

$$\begin{aligned} 0 \to H^0(L/K, k(X_L)^\times/L^\times) &\to H^0(L/K, \operatorname{Div} X_L) \\ &\to H^0(L/K, \operatorname{Pic} X_L) \to H^1(L/K, k(X_L)^\times/L^\times) \to 0. \end{aligned}$$

Firstly, $H^0(L/K, k(X_L)^\times/L^\times)$ is identified with the group of principal divisors on X_K: this follows from the fact that $H^1(L/K, L^\times) = 0$. The next term is equal to $\operatorname{Div} X_K$. The sequence therefore becomes

$$0 \to \operatorname{Pic} X_K \to H^0(L/K, \operatorname{Pic} X_L) \to H^1(L/K, k(X_L)^\times/L^\times) \to 0$$

which implies the result. □

Note that, in particular, these equivalent conditions hold when X has points in every completion of k (see Proposition 2.21).

We now note a consequence of these conditions.

Lemma 4.9. *Let $L/K/k$ be Galois extensions, and let X be a scheme over k as above. If the equivalent conditions of Lemma 4.8 are satisfied, then the following two results hold:*

1. *The map $H^1(K/k, \operatorname{Pic} X_K) \to H^1(L/k, \operatorname{Pic} X_L)$ is injective;*
2. *The map $H^2(K/k, k(X_K)^\times/K^\times) \to H^2(L/k, k(X_L)^\times/L^\times)$ is injective.*

Proof. Each result is an immediate consequence of the conditions together with the appropriate inflation-restriction exact sequence. □

4.2 Explicit descriptions

We now return to the surface V, as defined in (1.1). The coefficients a_i are fixed, and we write α_{ij} for a fourth root of a_i/a_j. We define

$$k = \mathbb{Q}$$
$$K = \mathbb{Q}(\alpha_{10}, \alpha_{20}, \alpha_{30}, \epsilon)/\mathbb{Q}$$
$$G = \operatorname{Gal}(K/\mathbb{Q})$$

The previous section shows that there are isomorphisms

$$\begin{array}{c} \operatorname{Br}_1 V/\operatorname{Br} k \\ \updownarrow \\ \ker(H^2(k, k(\bar{V})^\times) \to H^2(k, \operatorname{Div} \bar{V}))/\operatorname{Br} k \\ \updownarrow \\ H^2_{\mathrm{Az}}(V) \\ \updownarrow \\ H^1(k, \operatorname{Pic} \bar{V}) \end{array}$$

In this section, we will make these isomorphisms explicit; this will allow the calculation of elements of $\operatorname{Br}_1 V$. The procedure is not entirely satisfactory, because lifting elements from $k(\bar{V})^\times/k^\times$ (the group of principal divisors) to $k(\bar{V}^\times)$ is a rather tedious process; in the case discussed in Section 4.4, where a fibration exists from V to $\mathbb{P}^1$, we will see that this step may be avoided.

4.2.1 Calculation of $H^1(k, \operatorname{Pic} \bar{V})$

Firstly we consider the group $H^1(k, \operatorname{Pic} \bar{V})$. As in Section 3.6.2, we let Λ denote the subgroup of $\operatorname{Div} \bar{V}$ generated by the 48 lines on $\bar{V}$, and Λ^0 the group consisting of those divisors linearly equivalent to 0; then $\operatorname{Pic} \bar{V}$ is isomorphic to the quotient Λ/Λ^0. Lemma 3.1 shows that the least field of definition of Λ is K. Then the inflation-restriction exact sequence gives:

Lemma 4.10. *The map*

$$H^1(G, \Lambda/\Lambda^0) \xrightarrow{\text{inf}} H^1(k, \operatorname{Pic} \bar{V})$$

is an isomorphism. □

This group may therefore be calculated using the algorithms described in Chapter 3.

4.2.2 Calculation of $H^2_{\mathrm{Az}}(V)$

We now describe the isomorphism between $H^1(k, \operatorname{Pic} \bar{V})$, which we can compute, and $H^2_{\mathrm{Az}}(V)$. This comes from the exact sequence

$$0 \to k(\bar{V})^\times/\bar{k}^\times \to \operatorname{Div} \bar{V} \to \operatorname{Pic} \bar{V} \to 0$$

where we think of $k(\bar{V})^\times/\bar{k}^\times$ as being the group of principal divisors on $\bar{V}$. Part of the long exact sequence in cohomology associated to this sequence is

$$H^1(k, \operatorname{Div} \bar{V}) \to H^1(k, \operatorname{Pic} \bar{V}) \xrightarrow{\partial} H^2(k, k(\bar{V})^\times/\bar{k}^\times) \to H^2(k, \operatorname{Div} \bar{V})$$

and Lemma 4.3 shows that $H^1(k, \operatorname{Div} \bar{V}) = 0$; thus ∂ gives an isomorphism from $H^1(k, \operatorname{Pic} \bar{V})$ to $H^2_{\mathrm{Az}}(V)$. The definition of this coboundary map is well known, and may be explicitly described as follows:

1. Given a 1-cocycle with values in $\operatorname{Pic} \bar{V}$, lift it to a 1-cochain with values in $\operatorname{Div} \bar{V}$.
2. Take the coboundary of this cochain to get a 2-coboundary with values in $\operatorname{Div} \bar{V}$.
3. This 2-coboundary maps to 0 in $\operatorname{Pic} \bar{V}$; thus it may be pulled back to obtain a 2-cochain with values in $k(\bar{V})^\times/\bar{k}^\times$.

Computationally, how should this be accomplished? We are representing the group $H^1(k, \operatorname{Pic} \bar{V})$ by the isomorphic, but easily computable, group $H^1(G, \Lambda^0/\Lambda)$. Is there a more manageable group with which we might replace $H^2_{\mathrm{Az}}(V)$?

Lemma 4.11. *$H^2_{\mathrm{Az}}(V)$ is isomorphic to the kernel of*

$$H^2(G, \Lambda^0) \to H^2(G, \Lambda).$$

In other words, every class in $H^2_{\mathrm{Az}}(V)$ contains a cocycle whose support is contained in Λ^0, and which is obtained by inflation from G; and two such cocycles lie in the same class if and only if they differ by a coboundary satisfying the same criteria.

Proof. There is a commutative diagram with exact rows

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1(G,\Lambda/\Lambda^0) & \xrightarrow{\partial} & H^2(G,\Lambda^0) & \longrightarrow & H^2(G,\Lambda) \\
 & & \alpha\big\downarrow & & \beta\big\downarrow & & \gamma\big\downarrow \\
0 & \longrightarrow & H^1(k,\operatorname{Pic}\bar V) & \xrightarrow{\partial} & H^2(k,k(\bar V^\times)/k^\times) & \longrightarrow & H^2(k,\operatorname{Div}\bar V)
\end{array}$$

where the vertical maps all come from inflation and inclusion of modules. The map α is, as we have seen above, an isomorphism. The map γ is the composite

$$H^2(G,\Lambda) \xrightarrow{i_*} H^2(G,\operatorname{Div} V_K) \xrightarrow{\inf} H^2(k,\operatorname{Div}\bar V)$$

where V_K means $V \times_{\operatorname{Spec} k} \operatorname{Spec} K$ and i is the inclusion of Λ into $\operatorname{Div} V_K$. Now Λ is a direct summand of $\operatorname{Div} V_K$, so i_* is injective; and the inflation map is also injective, by the inflation-restriction exact sequence. Thus γ is injective, and hence so is β. Now, by the commutativity of the left-hand square, β identifies the images of the two coboundary maps ∂; hence the result. □

It is easy to see that if we follow through the explicit definition of ∂ given above, starting from an element of $H^1(G,\Lambda/\Lambda^0)$, then we will obtain an element of $H^2(G,\Lambda^0)$.

The inverse mapping ∂^{-1} is slightly harder to compute, but still presents no real problem. The explicit description is as follows:

1. Any 2-cocycle lying in $H^2_{\mathrm{Az}}(V)$ by definition maps to a coboundary in $H^2(k,\operatorname{Div}\bar V)$; so it may be written as $d\alpha$ say, for some 1-cochain α with values in $\operatorname{Div}\bar V$.

2. Now consider α as a 1-cochain with values in $\operatorname{Pic}\bar V$; since $d\alpha$ takes values in the principal divisors, α is a 1-cocycle for $\operatorname{Pic}\bar V$.

There is what looks like a problem in step 1: given an element of $H^2(k,\operatorname{Div}\bar V)$ which we know to be a coboundary, we must find a suitable element α. This may however be reduced to a smaller problem. Write $\bar G$ for the absolute Galois group of k. Now $\operatorname{Div}\bar V$ is the direct sum of the Galois modules $\mathbb{Z}[\bar G]D$, where D runs through a set of non-conjugate prime divisors on $\bar V$. These modules are all of finite rank over $\mathbb{Z}$. Any element of $H^2(k,\operatorname{Div}\bar V)$ factors through a finite quotient H of $\bar{G}$, hence has support containing only finitely many prime divisors, and so takes values in some finite direct sum $\sum_i \mathbb{Z}[H]D_i$. Cohomology commutes with direct sums, so we are looking for an element $\alpha \in \sum_i C^1(H, \mathbb{Z}[H]D_i)$ with the desired coboundary. This gives a finite system of equations to be solved.

More concretely, this means that we can take the divisors of V one at a time when calculating ∂^{-1}. Each divisor D on V splits over $\bar{V}$ into divisors D_j. We start with a 2-cocycle c in $H^2_{\mathrm{Az}}(V)$, which by definition maps to 0 in $H^2(k, \operatorname{Div} \bar{V})$ and hence maps to 0 in $H^2(k, \sum \mathbb{Z}D_j)$, which is the smallest submodule of $\operatorname{Div} \bar{V}$, fixed by the Galois action, which contains the D_j. So we can write the image of c (a 2-cocycle with values in $\sum \mathbb{Z}D_j$) as $d\alpha$, where α is a 1-cochain with values in $\sum \mathbb{Z}D_j$; searching for a suitable α is a small and simple problem. The image of α in $\operatorname{Pic} \bar{V}$ will not necessarily be a cocycle: but when we add together all the α from all the divisors D on V, the sum will indeed be a cocycle.

We state here a variation on the usual description by cochains of the first cohomology group, which is useful in light of the above discussion.

Lemma 4.12. *Let M be a torsion-free Abelian group acted on by a group G. As usual, we write $C^i(G,M)$, $Z^i(G,M)$, $B^i(G,M)$ for the groups of i-cochains, -cocycles and -coboundaries respectively with values in M. Then*

$$H^1(G,M) \cong \frac{Z^1(G,M) + C^1(G,M^G)}{B^1(G,M) + C^1(G,M^G)}. \tag{4.4}$$

Proof. This is the usual isomorphism theorem: if K is a normal subgroup of a group H, and H' is any subgroup of H, then $H'K/K \cong H'/(H' \cap K)$. We take H' to be $Z^1(G,M)$ and K to be the sum of $B^1(G,M)$ and $C^1(G,M^G)$. Then

$$H' \cap K = B^1(G,M) + (Z^1(G,M) \cap C^1(G,M^G)) = B^1(G,M) + Z^1(G,M^G)$$

but M^G is a torsion-free G-module with trivial G-action, so $Z^1(G,M^G) = \operatorname{Hom}(G,M^G) = 0$. $\square$

Corollary 4.13. *When calculating the map from $H^2_{\mathrm{Az}}(V)$ to $H^1(k, \operatorname{Pic}\bar{V})$, we may use this description of $H^1(k, \operatorname{Pic}\bar{V})$ and then forget the contributions at any divisors on $\bar{V}$ which are defined over k.*

Proof. Such divisors give rise to cochains in $\operatorname{Pic}\bar{V}$ which take values in $H^0(k, \operatorname{Pic}\bar{V})$; thus they lie in the bottom half of the quotient (4.4). ☐

Recall that, in Section 3.6.1, we computed $H^1(G, M)$ for a torsion-free G-module M by the isomorphism

$$H^1(G, M) \cong \frac{H^0(G, M \otimes \mathbb{Q}/\mathbb{Z})}{\operatorname{im} H^0(G, M \otimes \mathbb{Q})}.$$

The right hand side here is a quotient of a subgroup of $M \otimes \mathbb{Q}$; so we will often be storing elements of $H^1(k, \operatorname{Pic}\bar{V})$, after lifting, as elements of $\operatorname{Pic}\bar{V} \otimes \mathbb{Q}$. Now $k(\bar{V})^\times/\bar{k}^\times$ is also a torsion-free group: this is easily seen to be true, as any element of $\bar{k}$ already has as many roots as possible. Hence there is an isomorphism

$$H^1(k, (k(\bar{V})^\times/\bar{k}^\times) \otimes \mathbb{Q}/\mathbb{Z}) \cong H^2(k, k(\bar{V})^\times/\bar{k}^\times).$$

By the functorial properties of cohomology, the diagram

$$\begin{tikzcd}
\operatorname{Pic}\bar{V} \otimes \mathbb{Q} \arrow[r, "\partial"] \arrow[d] & H^1(k, (k(\bar{V})^\times/\bar{k}^\times) \otimes \mathbb{Q}/\mathbb{Z}) \arrow[d] \\
H^1(k, \operatorname{Pic}\bar{V}) \arrow[r, "\partial"] & H^2(k, k(\bar{V})^\times/\bar{k}^\times)
\end{tikzcd}$$

commutes: we may compute the coboundary either way, and the comments above still apply.

4.2.3 From H^2 to algebras

As mentioned in the introduction to this section, it is not always straightforward to lift elements from $H^2_{\mathrm{Az}}(V)$ to $H^2(k, k(\bar{V})^\times)$. In specific cases, this can be accomplished by hand: given a principal divisor, we need to find the function (unique up to a constant multiple) whose divisor it is. Now the only divisors whose functions we can instantly write down are those which are hyperplane sections or, more generally, intersections of V with some hypersurface in $\mathbb{P}^3$. So we must express the given principal divisor as a difference of sums of hypersurface sections, which is always possible, and then it is possible to write down the required function. The function will in general be a messy ratio of high-degree polynomials.

The correspondence between $H^2(k, k(\bar{V})^\times)$ and $\operatorname{Br} k(\bar{V})$, on the other hand, is well-known and is reproduced here only for reference. This material is taken from Chapter V of [15], which has the advantage that the calculations are very explicit.

Briefly, let A be a central simple algebra over a field K; then it is known that A contains a maximal subfield L, of degree n, say, over K; and A is then a vector space of dimension n over L. Now let σ be an element of $\mathrm{Gal}(L/K)$; then it can be shown that the action of σ on L is the same as conjugating by an element u_σ of A:

$$\sigma a = u_\sigma a u_\sigma^{-1} \quad \text{for all } a \in L. \tag{4.5}$$

If we now define $\phi : \mathrm{Gal}(L/K)^2 \to L$ by

$$\phi(\sigma, \tau) = u_\sigma u_\tau u_{\sigma\tau}^{-1} \tag{4.6}$$

then it is easily checked that the values do indeed lie in L, and that ϕ defines a 2-cocycle. Different choices of u_σ change ϕ by a coboundary, so we have defined a map from $\mathrm{Br}(L/K)$ to $H^2(L/K, L^\times)$.

The inverse to this correspondence is simple to construct. Given a 2-cocycle $\phi \in H^2(L/K, L^\times)$, we take A to be the vector space over L generated by the symbols u_σ, and define multiplication in A to satisfy the equations (4.5) and (4.6). It turns out that A is indeed a central simple algebra over K, as required.

4.3 Cyclic algebras

We now investigate in detail the situation for cyclic algebras on V. Apart from being generally instructive, this case will be important when we consider algebras arising from fibrations in Section 4.4. The details of the Galois cohomology used in this section may be found in several places, for example the on-line notes [27] of Milne.

Temporarily, we let L/K be any finite cyclic extension of fields; let G be the Galois group of L/K, which has order n and is generated by some element σ. Let u denote a symbol such that $u^n = b$ lies in $K^\times$; then we may define an algebra $\mathcal{A}$ as follows:

- As a vector space over L, $\mathcal{A}$ has basis $\{u^i \mid i = 0, \ldots, n-1\}$;
- Multiplication is defined by

$$(\sigma x)u = ux \quad \text{for all } x \in L.$$

This algebra $\mathcal{A}$ is by definition a *cyclic algebra* over K, which is its centre. This algebra will be denoted by $(L/K, b)$; we will now see exactly how it depends on both L/K and b.

4.3.1 Cohomology of cyclic groups

If G is any finite group, then $H^i(G, \mathbb{Q}) = 0$ for all $i \geq 1$; this gives us, in particular, an isomorphism $H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$. Now $H^1(G, \mathbb{Q}/\mathbb{Z})$ is simply the character group of G; if G is cyclic of order n, then so is its character group. We obtain the following result:

Lemma 4.14. *Let G be cyclic of order n. Then $H^2(G, \mathbb{Z})$ is cyclic of order n, and a generator is given by*

$$w(\sigma^i, \sigma^j) = \begin{cases} 0 & \textit{if } i + j < n; \\ 1 & \textit{if } i + j \geq n. \end{cases}$$

Proof. A generator for $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ is given by the homomorphism χ mapping σ to $1/n$. To calculate the image of χ in $H^2(G, \mathbb{Z})$, we first imagine that χ is now mapping into $\mathbb{Q}$, and then take its coboundary:

$$\begin{aligned} d\chi(\sigma^i, \sigma^j) &= \sigma^i \chi(\sigma^j) + \chi(\sigma^i) - \chi(\sigma^{i+j}) \\ &= (i + j - (i + j \bmod n))/n \end{aligned}$$

which gives the result stated. $\square$

The next result, which is the well-known and fundamental result on the cohomology of cyclic groups, is best stated in terms of the Tate cohomology groups. Let M be any G-module, and let N denote the norm element $\sum_{i=0}^{n-1} \sigma^i$ in $\mathbb{Z}[G]$. The Tate cohomology groups are defined as follows:

$$\hat{H}^i(G, M) = \begin{cases} H^i(G, M) & i \geq 1; \\ H^0(G, M)/NM & i = 0; \\ {}_N M/(\sigma - 1)M & i = -1; \\ H_{-i-1}(G, M) & i \leq -2. \end{cases}$$

Here ${}_N M$ denotes the kernel of $N : M \to M$. The norm map takes the place of the coboundary in dimension 0. The result we need is this:

Lemma 4.15. *Let G be cyclic of order n, and let M be any G-module. Then, for each i, there is an isomorphism*

$$\hat{H}^i(G, M) \xrightarrow{\sim} \hat{H}^{i+2}(G, M).$$

This isomorphism is given by the cup-product with the generator of $H^2(G, \mathbb{Z})$ given in Lemma 4.14.

The proof is omitted here; it is Proposition 2.11 in [27]. We will need the explicit construction of the isomorphism, given there, later.

This result immediately shows that, for L/K as at the beginning of this section, $H^2(G, L^\times)$ is isomorphic to $\hat{H}^0(G, L^\times)$. In fact, we have

Lemma 4.16. *Let L/K be a cyclic extension with Galois group G. Then*

$$H^2(G, L^\times) \cong K^\times/NL^\times$$

where the isomorphism identifies an element b of $K^\times$ with the 2-cocycle $b \cup w$. The algebra associated to this cocycle is the cyclic algebra $(L/K, b)$.

Proof. The first statement follows immediately from the preceding lemma. The second statement is a consequence of the definition of $(L/K, b)$ and the correspondence between algebras and 2-cocycles described in Section 4.2.3. □

More generally, let χ be any homomorphism from $\mathrm{Gal}(\bar{K}/K)$ to $\mathbb{Q}/\mathbb{Z}$, and b be any element of $K^\times$; then we can form an element of $H^2(K, \bar{K}^\times)$ by letting $(\chi, b) := b \cup d\chi$. The element $(L/K, b)$ which we have been examining is the special case of this when χ is chosen to the cyclic character associated to the extension L/K.

4.3.2 Cyclic algebras on V

We now apply the general study of cyclic algebras in the previous section to the surface V, and in particular describe the elements of $H^1(G, \mathrm{Pic}\,\bar{V})$ corresponding to cyclic Azumaya algebras. In this section, k is once again the field of definition of V (normally $\mathbb{Q}$, but the theory is quite general). We let L be some cyclic extension of k, with Galois group G, and we will study those Azumaya algebras on V which split when the base field is extended to L.

The inflation-restriction sequence says that an algebra on V splits over L if and only if the corresponding 2-cocycle lies in $H^2(L/k, k(V_L)^\times)$. Now, we are considering algebras modulo elements of the image of $\mathrm{Br}\,k$; but it is not in general true that an algebra which splits over L, and is equivalent to a constant algebra over $\bar{k}$, is therefore equivalent to a constant algebra over

L. The diagram looks like this:

$$\begin{array}{ccccccc}
\mathrm{Br}(L/k) & \longrightarrow & \mathrm{Br}(k(V_L)/k(V)) & \longrightarrow & H^2(L/k, k(V_L)^\times/L^\times) & \longrightarrow & H^3(L/k, L^\times) \\
\downarrow & & \downarrow & & \downarrow & & \\
\mathrm{Br}(k) & \longrightarrow & \mathrm{Br}(k(\bar{V})/k(V)) & \longrightarrow & H^2(k, k(\bar{V})^\times/\bar{k}^\times) & \longrightarrow & 0
\end{array}$$

where the two leftmost vertical arrows are injective. The right-hand vertical arrow has no reason to be injective, unless the conditions of Lemma 4.8 are satisfied: for example, when V has points in every completion of k. We do know, however, that $H^3(L/k, L^\times) = 0$, for by Lemma 4.15 this is isomorphic to $H^1(L/k, L^\times)$, which is trivial.

There are no problems with deciding whether an algebra is Azumaya. For the map from $H^2(L/k, \mathrm{Div}\, V_L)$ to $H^2(k, \mathrm{Div}\, \bar{V})$ is injective by the inflation-restriction sequence; therefore an element of $H^2(L/k, k(V_L)^\times/L^\times)$ is Azumaya if and only if it maps to 0 in $H^2(L/k, \mathrm{Div}\, V_L)$. We define

$$H^2_{\mathrm{Az}}(L/k, V) := \ker(H^2(L/k, k(V_L)^\times/L^\times) \to H^2(L/k, \mathrm{Div}\, V_L)).$$

In light of the discussion in the preceding paragraph, we keep in mind that the map from $H^2_{\mathrm{Az}}(L/k, V)$ to $H^2_{\mathrm{Az}}(V)$ is not necessarily injective.

A cyclic algebra which is split by L/k can be written as $(L/k, f)$ for some rational function f in $k(V)$. We will now answer two questions about such algebras: when are they Azumaya, and what do such algebras map to in $H^1(k, \mathrm{Pic}\, \bar{V})$?

The isomorphism described in Lemma 4.15 commutes with the coboundary morphism, so we have a commutative diagram

$$\begin{array}{ccccc}
\hat{H}^{-1}(L/k, \mathrm{Pic}\, V_L) & \xrightarrow{\partial} & \hat{H}^0(L/k, k(V_L)^\times/L^\times) & \longrightarrow & \hat{H}^0(L/k, \mathrm{Div}\, V_L) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(L/k, \mathrm{Pic}\, V_L) & \xrightarrow{\partial} & H^2(L/k, k(V_L)^\times/L^\times) & \longrightarrow & H^2(L/k, \mathrm{Div}\, V_L)
\end{array} \tag{4.7}$$

where the vertical arrows are all isomorphisms, given by cup-product with the generator w of $H^2(L/k, \mathbb{Z})$. By Lemma 4.16, the cyclic algebra $(L/k, f)$ corresponds to the element f of $\hat{H}^0(L/k, k(V_L)^\times/L^\times)$. The question of whether $(L/k, f)$ is Azumaya can be answered immediately, and we get the following generalisation of Lemma 11 of [44]:

Proposition 4.17. *Let $\mathcal{A} = (L/k, f)$ be a cyclic algebra on V, where L is a cyclic extension of the base field k and f is some rational function in $k(V)$. Then $\mathcal{A}$ is Azumaya if and only if the divisor (f) is the norm of some divisor D defined over L. If moreover we assume that V has points in every completion of k, then $\mathcal{A}$ is equivalent to a constant algebra if and only if we can take D to be principal.*

Proof. For the first statement, we need only recall the definition of the Tate cohomology group:

$$\hat{H}^0(L/k, \operatorname{Div} V_L) = \operatorname{Div} V / N \operatorname{Div} V_L.$$

The result then comes straight from the diagram (4.7). The second statement is similar, but we must also apply Lemma 4.9 to show that in this case the map from $H^2_{\mathrm{Az}}(L/k, V)$ to $H^2_{\mathrm{Az}}(V)$ is injective. □

The first step towards calculating the image of $(L/k, f)$ in $H^1(k, \operatorname{Pic} \bar{V})$ is to work out the corresponding element of $\hat{H}^{-1}(L/k, \operatorname{Pic} V_L)$. Recall the definition:

$$\hat{H}^{-1}(L/k, \operatorname{Pic} V_L) = {}_N \operatorname{Pic} V_L / (\sigma - 1) \operatorname{Pic} V_L$$

where σ is a generator for $\operatorname{Gal}(L/k)$.

Lemma 4.18. *The element of $\hat{H}^{-1}(L/k, \operatorname{Pic} V_L)$ corresponding to the algebra $(L/k, f)$ is simply the class of D from Proposition 4.17.*

Proof. First of all, we note that $ND = (f)$, which is principal, so D does indeed lie in ${}_N \operatorname{Pic} V_L$. We then apply the definition of the coboundary morphism: lift to $\operatorname{Div} V_L$ to obtain the divisor D; take coboundary, which in this case is the norm, to obtain (f); and pull back to $\hat{H}^0(L/k, k(V_L)^\times/L^\times)$ to regain the function f. By Lemma 4.16, this corresponds to the algebra $(L/k, f)$ in $H^2_{\mathrm{Az}}(L/k, V)$. □

The next step is to describe the isomorphism between $H^1(L/k, \operatorname{Pic} V_L)$ and $\hat{H}^{-1}(L/k, \operatorname{Pic} V_L)$. One definition of this isomorphism can be found in [27], in the proof of Proposition 2.11. Let G be a cyclic group, generated by an element σ, and let M be a G-module. We consider the exact sequence

$$0 \to M \xrightarrow{a \mapsto N \otimes a} \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \xrightarrow{\sigma - 1} \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \xrightarrow{\epsilon} M \to 0 \tag{4.8}$$

where N is the norm element of $\mathbb{Z}[G]$, the middle arrow is multiplication by $(\sigma - 1)$, and ϵ is the augmentation map which takes $\sigma^i \otimes a$ to a for all i. The group action on $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M$ is the diagonal action:

$$\sigma(g \otimes a) = \sigma g \otimes \sigma a.$$

The sequence (4.8) defines a "double coboundary" map from $\hat{H}^i(G, M)$ to $\hat{H}^{i+2}(G, M)$ for all i. Simple arguments (which we will not need) show that $\mathbb{Z}[G] \otimes_{\mathbb{Z}} M$ has trivial cohomology, so this map is an isomorphism. The map may be explicitly described.

1. Given an i-cocycle with values in M, lift it to an i-cochain with values in $\mathbb{Z}[G] \otimes M$.

2. Take the coboundary of this i-cochain.

3. This $(i + 1)$-coboundary maps to 0 under ϵ, so may be written as the product of $(\sigma - 1)$ with another $(i+1)$-cochain with values in $\mathbb{Z}[G] \otimes M$.

4. Take the coboundary of this $(i + 1)$-cochain.

5. The resulting $(i+2)$-coboundary maps to 0 when multiplied by $(\sigma - 1)$, so may be written as the norm tensored with an $(i + 2)$-cocycle with values in M.

We now unpick this definition to get the following result.

Lemma 4.19. *Let a be an element of $\hat{H}^{-1}(G, M)$. Then the image of a in*

$H^1(G, M)$ is represented by the cocycle α, defined by

$$\alpha(1) = 0$$
$$\alpha(\sigma^r) = \sum_{i=0}^{r-1} \sigma^i a \qquad \text{for } r \geq 1.$$

Proof. We simply follow the definition of the "double coboundary" map given above.

1. Lift a to $1 \otimes a$ in $\mathbb{Z}[G] \otimes M$.

2. The coboundary in this case is the norm: we get

$$N(1 \otimes a) = \sum_{i=0}^{n-1} (\sigma^i \otimes \sigma^i a).$$

3. As $Na = 0$, we may subtract $1 \otimes Na$ to get

$$\begin{aligned} N(1 \otimes a) &= \sum_{i=1}^{n-1} (\sigma^i - 1) \otimes \sigma^i a \\ &= (\sigma - 1) \sum_{i=1}^{n-1} \sum_{j=0}^{i-1} (\sigma^j \otimes \sigma^i a) \end{aligned}$$

4. Dividing by $(\sigma - 1)$ and taking the coboundary, we obtain the 1-cocycle

$$\sigma^r \mapsto \sum_{i=1}^{n-1} \sum_{j=0}^{i-1} (\sigma^{j+r} \otimes \sigma^{i+r} a - \sigma^j \otimes \sigma^i a). \tag{4.9}$$

5. Now we must do some tedious manipulation of (4.9) to show that it can be written in the form $N \otimes \alpha$. If $r = 0$, this is trivial; so assume

that $r \geq 1$. We split the sum up into four separate sums:

$$\begin{aligned}
\sigma^r \mapsto & \sum_{i=1}^{n-r-1} \sum_{j=0}^{i-1} (\sigma^{j+r} \otimes \sigma^{i+r} a) + \sum_{i=n-r}^{n-1} \sum_{j=0}^{n-r-1} (\sigma^{j+r} \otimes \sigma^{i+r} a) \\
& + \sum_{i=n-r+1}^{n-1} \sum_{j=n-r}^{n-1} (\sigma^{j+r} \otimes \sigma^{i+r} a) - \sum_{i=1}^{n-1} \sum_{j=0}^{i-1} (\sigma^j \otimes \sigma^i a) \\
= & \sum_{i=r}^{n-1} \sum_{j=r}^{i-1} (\sigma^j \otimes \sigma^i a) + \sum_{i=0}^{r-1} \sum_{j=r}^{n-1} (\sigma^j \otimes \sigma^i a) \\
& + \sum_{i=1}^{r-1} \sum_{j=0}^{i-1} (\sigma^j \otimes \sigma^i a) - \sum_{i=1}^{n-1} \sum_{j=0}^{i-1} (\sigma^j \otimes \sigma^i a) \\
= & \sum_{i=0}^{r-1} \sum_{j=r}^{n-1} (\sigma^j \otimes \sigma^i a) - \sum_{i=r}^{n-1} \sum_{j=0}^{r-1} (\sigma^j \otimes \sigma^i a).
\end{aligned}$$

Now once again $Na = 0$, so we may add

$$0 = \sum_{j=0}^{r-1} (\sigma^j \otimes Na) = \sum_{j=0}^{r-1} \sum_{i=0}^{n-1} (\sigma^j \otimes \sigma^i a)$$

to the expression above to obtain

$$\begin{aligned}
\sigma^r \mapsto & \sum_{i=0}^{r-1} \sum_{j=0}^{n-1} (\sigma^j \otimes \sigma^i a) \\
& = N \otimes \sum_{i=0}^{r-1} \sigma^i a
\end{aligned}$$

as desired.

□

Corollary 4.20. *Let $(L/k, f)$ be a cyclic Azumaya algebra on V. Then the element of $H^1(L/k, \operatorname{Pic} V_L)$ corresponding to the algebra $(L/k, f)$ is repre-*

sented by the cocycle

$$\begin{aligned} 1 &\mapsto 0 \\ \sigma^r &\mapsto \sum_{i=0}^{r-1} \sigma^i D \qquad \textit{for } r \geq 1. \end{aligned}$$

where D is the divisor from Proposition 4.17. □

4.4 The vertical Brauer group

We now consider the case when V is equipped with a fibration $\pi : V \to \mathbb{P}^1$. The geometry of this situation was discussed in Section 2.2, and in this section we will investigate how such a fibration might be used to give other ways of computing the Brauer group of V. Specifically, we will show how the methods used in [44] for computing Brauer groups fit in with the rest of this chapter.

Let η denote the generic point of $\mathbb{P}^1$, so that V_η is the generic fibre of the fibration, a curve of genus 1 over $k(\mathbb{P}^1)$. We recall from Section 2.2 that the vertical Picard group, denoted $\mathrm{Pic}_{\mathrm{vert}}$, associated to this fibration is defined by

$$\mathrm{Pic}_{\mathrm{vert}} = \ker(\mathrm{Pic}\,\bar{V} \to \mathrm{Pic}\,\bar{V}_\eta).$$

Any Azumaya algebra on $\mathbb{P}^1$ can be lifted to an Azumaya algebra on V. This is not very useful, however, as the Brauer group of $\mathbb{P}^1$ consists only of the classes of the constant algebras $\mathrm{Br}\,k$. Instead, we consider those elements of $\mathrm{Br}\,k(\mathbb{P}^1)$ which, although not Azumaya over $\mathbb{P}^1$, give Azumaya algebras when lifted to V. The group of these algebras modulo constant algebras will be written as B:

$$B = \{\mathcal{A} \in \mathrm{Br}\,k(\mathbb{P}^1) \mid \pi^*\mathcal{A} \in \mathrm{Br}\,V\} / \mathrm{Br}\,k.$$

Any such algebra must necessarily split over $\bar{k}$, since $\mathrm{Br}\,k(\mathbb{P}^1_{\bar{k}})$ is trivial by Tsen's theorem [28, 13.5]. We identify $k(\mathbb{P}^1)$ with $k(t)$. Since once again $H^3(k, \bar{k}^\times) = 0$, we have that $\mathrm{Br}\,k(t)/\mathrm{Br}\,k$ is isomorphic to $H^2(k, \bar{k}(t)^\times/\bar{k}^\times)$.

Therefore, by Corollary 4.7,

$$B \cong \ker\left(H^2(k, \bar{k}(t)^\times/\bar{k}^\times) \xrightarrow{\pi^*} H^2(k, k(\bar{V})^\times/\bar{k}^\times) \to H^2(k, \operatorname{Div}\bar{V})\right). \quad (4.10)$$

As with $H^2_{\mathrm{Az}}(V)$, this isomorphism is not straightforward to calculate in general, although in some specific cases it can be done without too much trouble. However, we will see below that in the vertical case it is possible to write down the elements of B without coming through this isomorphism.

We can calculate the structure of B by cohomological methods, just as for $H^2_{\mathrm{Az}}(V)$.

Proposition 4.21. *There is an isomorphism $B \cong H^1(k, \mathrm{Pic}_{\mathrm{vert}})$, such that the diagram*

$$\begin{tikzcd}
H^1(k, \mathrm{Pic}_{\mathrm{vert}}) \arrow[r, "\sim"] \arrow[d] & B \arrow[d] \\
H^1(k, \operatorname{Pic}\bar{V}) \arrow[r, "\sim"] & H^2_{\mathrm{Az}}(V)
\end{tikzcd}$$

commutes.

Proof. Consider the commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \bar{k}(t)^\times/\bar{k}^\times \arrow[r] \arrow[d] & \mathrm{Div}_{\mathrm{vert}} \arrow[r] \arrow[d] & \mathrm{Pic}_{\mathrm{vert}} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & k(\bar{V})^\times/\bar{k}^\times \arrow[r] \arrow[d, "\alpha"'] & \operatorname{Div}\bar{V} \arrow[r] \arrow[d, "\beta"'] & \operatorname{Pic}\bar{V} \arrow[r] \arrow[d, "\gamma"'] & 0 \\
0 \arrow[r] & k(\bar{V}_\eta)^\times/\bar{k}(t) \arrow[r] & \operatorname{Div}\bar{V}_\eta \arrow[r] & \operatorname{Pic}\bar{V}_\eta \arrow[r] & 0
\end{tikzcd}$$

where the top row consists simply of the kernels of the maps α, β, γ; and the exactness of the top row comes from the Snake Lemma and the surjectivity of α. Taking cohomology of the top two rows gives us the diagram

$$\begin{array}{ccccccc} H^1(k, \mathrm{Div}_{\mathrm{vert}}) & \longrightarrow & H^1(k, \mathrm{Pic}_{\mathrm{vert}}) & \longrightarrow & H^2(k, \bar{k}(t)^\times/\bar{k}^\times) & \longrightarrow & H^2(k, \mathrm{Div}_{\mathrm{vert}}) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & H^1(k, \mathrm{Pic}\,\bar{V}) & \longrightarrow & H^2(k, k(\bar{V})^\times/\bar{k}^\times) & \longrightarrow & H^2(k, \mathrm{Div}\,\bar{V}) \end{array}$$

with exact rows. Now $\mathrm{Div}_{\mathrm{vert}}$ is a direct summand of $\mathrm{Div}\,\bar{V}$, so therefore $H^1(k, \mathrm{Div}_{\mathrm{vert}}) = 0$ and $H^2(k, \mathrm{Div}_{\mathrm{vert}})$ injects into $H^2(k, \mathrm{Div}\,\bar{V})$. The result then follows from the form (4.10) of B. □

As was the case with $H^2_{\mathrm{Az}}(V)$, we may calculate $H^1(k, \mathrm{Pic}_{\mathrm{vert}})$ using the 48 lines on V as generators. The difficulty with this approach is that it is not always straightforward to calculate the classes of the irreducible components of the reducible fibres in terms of the 48 lines.

4.4.1 Identifying B

We now turn to trying to write down the group B, defined in (4.4). The material in this section is well known, and indeed is quoted by Swinnerton-Dyer in [44] to write down Azumaya algebras on V. Following Section 1 of [13], we will write elements of $\mathrm{Br}\,k(t)$ in a unique way; for this we need some notation.

Let P be any closed point of $\mathbb{P}^1_k$; then, over the normal closure of the residue field $k(P)$, P splits into geometric points $P_1, \ldots, P_n$, where n is the degree of the extension $k(P)/k$. We fix P_1 and choose $t_P \in k(P)$ such that P_1 is the point given by $t = t_P$; then the original point P is defined over k by the equation $N_{k(P)/k}(t - t_P) = 0$. Here we abuse notation slightly by writing $N_{k(P)/k}$ instead of $N_{k(P)(t)/k(t)}$. If now c_P is an element of $H^1(k(P), \mathbb{Q}/\mathbb{Z})$ and f an element of $k(P)(t)^\times$, denote the element $f \cup dc_P$ of $\mathrm{Br}\,k(P)(t)$ by (c_P, f). In this manner we obtain an element of $\mathrm{Br}\,k(t)$ by the formula $\mathrm{cores}_{k(P)/k}(c_P, (t - t_P))$. The result we now quote is this:

Lemma 4.22. *Let $\mathcal{A}$ be a central simple algebra over $k(t)$. Then $\mathcal{A}$ is equiv-*

alent to an algebra of the form

$$\sum_P n_P \operatorname{cores}_{k(P)/k}(c_P, (t - t_P)) + a \tag{4.11}$$

where the sum is over finitely many distinct closed points P of $\mathbb{P}^1_k$, the n_P are integers, c_P is a non-trivial element of $H^1(k(P), \mathbb{Q}/\mathbb{Z})$, t_P is as above and a is a constant algebra, that is, an element of $\operatorname{Br} k$.

Proof. See [13]. □

The problem in identifying B is to compute the image of an algebra (4.11) in $H^2(k, \operatorname{Div} \bar{V})$. The constant algebra a does not interest us. Now the cup product commutes with the map $k(P)(t) \to \operatorname{Div} \bar{V}$, so we must find the value of

$$\operatorname{cores}_{k(P)/k}((\pi^* P_1 - \pi^* \infty) \cup dc_P) \in H^2(k, \operatorname{Div} \bar{V}) \tag{4.12}$$

where ∞ is the point at infinity on $\mathbb{P}^1_{k(P)}$.

Let Div_P and $\operatorname{Div}_\infty$ denote the subgroups of $\operatorname{Div} \bar{V}$ generated by the irreducible components of the geometric fibres above P and ∞, respectively. We assume that coordinates have been chosen such that the fibre at infinity is geometrically irreducible. Both Div_P and $\operatorname{Div}_\infty$ are direct summands of $\operatorname{Div} \bar{V}$, so we may treat the two terms of (4.12), in $\pi^* P_1$ and in $\pi^* \infty$, separately.

First we consider the fibre at infinity. We can treat this fibre easily, for the point ∞ is defined over k. So $\operatorname{Div}_\infty$ is simply a copy of $\mathbb{Z}$, and $\pi^* \infty$ is the element 1 in this copy of $\mathbb{Z}$. The restriction map

$$\operatorname{res} : H^0(k, \operatorname{Div}_\infty) \to H^0(k(P), \operatorname{Div}_\infty)$$

is the identity, and we therefore have

$$\operatorname{cores}_{k(P)/k}(\pi^* \infty \cup dc_P) = \operatorname{cores}_{k(P)/k}(\operatorname{res}(1) \cup dc_P) = 1 \cup \operatorname{cores}_{k(P)/k} dc_P.$$

This gives the following lemma:

Lemma 4.23. *The algebra* (4.11) *maps to* 0 *in* $H^2(k, \mathrm{Div}_\infty)$ *if and only if*

$$\sum_P n_P \operatorname{cores}_{k(P)/k} c_P = 0.$$

□

Now we consider the term $\operatorname{cores}_{k(P)/k}(\pi^* P_1 \cup dc_P)$. It turns out that the corestriction here generates no problems: for, if Div_{P_1} denotes the subgroup of $\operatorname{Div} \bar{V}$ generated by the irreducible components of the fibre over P_1, then Div_P as a module is induced from Div_{P_1}. Formally, let G be the absolute Galois group of k, and H the subgroup of G which is the absolute Galois group of $k(P)$. Then we define the induced module

$$\operatorname{Ind}_G^H \mathrm{Div}_{P_1} = \operatorname{Hom}_H(\mathbb{Z}[G], \mathrm{Div}_{P_1})$$

with the action of G given by $g\phi(x) = \phi(xg)$. Then we have the following lemma:

Lemma 4.24. *Let $g_1, \dots, g_n$ be a set of left coset representatives of H in G. Then the map $\phi \mapsto \sum g_i \phi(g_i^{-1})$ is an isomorphism of G-modules from $\operatorname{Ind}_G^H \mathrm{Div}_{P_1}$ to Div_P.*

Proof. The map is injective: for the image of ϕ lies in Div_{P_1}, and so the n elements $g_i\phi(g_i^{-1})$ each lie above a different one of the P_i; if their sum is zero, it therefore follows that each $\phi(g_i^{-1})$ is zero; and as ϕ is determined by its values on a single element of each coset, so ϕ is zero. The map is surjective: given an irreducible divisor D in D_P, choose j such that D lies above $g_j P_1$; then define ϕ such that $g_j\phi(g_j^{-1}) = D$, and ϕ is zero on the other cosets of H in G; then ϕ clearly maps to D. Finally, the map commutes with the action of G: first note that, as ϕ commutes with elements of H, our map is independent of the choice of coset representatives g_i; then the image of $g\phi$ is

$$\sum g_i(g\phi)(g_i^{-1}) = g \sum (g^{-1}g_i)\phi(g_i^{-1}g)$$

but the $g^{-1}g_i$ are another set of coset representatives; the result follows. □

Corollary 4.25. *The corestriction map*

$$\mathrm{cores}_{k(P)/k} : H^2(k(P), \mathrm{Div}_{P_1}) \to H^2(k, \mathrm{Div}_P)$$

is an isomorphism.

Proof. This is essentially Shapiro's Lemma (see [27], Chapter II, Proposition 1.11). □

Corollary 4.26. *Suppose that the algebra* (4.11) *is Azumaya when lifted to* V*. Then the geometric components* P_i *of each* P *all lie below geometrically reducible fibres of* π*.*

Proof. Suppose without loss of generality that the fibre above P_1 is geometrically irreducible (and therefore so are those above the other P_i). Then Div_{P_1} is simply a copy of $\mathbb{Z}$, acted on trivially by $\mathrm{Gal}(\bar{k}/k(P))$; and $\pi^* P_1$ is 1 in this copy of $\mathbb{Z}$; so the cup-product map

$$c_P \mapsto \pi^* P_1 \cup dc_P$$

is an isomorphism. If the algebra maps to 0 in $H^2(k, \mathrm{Div}\, \bar{V})$, then it must map to 0 in each $H^2(k, \mathrm{Div}_P)$, hence in $H^2(k(P), \mathrm{Div}_{P_1})$ by Corollary 4.4.1. So by the isomorphism above, $c_P = 0$. □

Suppose now that the fibre over P_1 is geometrically reducible. It may already split, over $k(P)$, into several components which we will call D, D', D'' and so on. The geometrically irreducible components of D generate a subgroup Div_D of Div_{P_1}, as similarly do those of D', …; an element of $H^2(k(P), \mathrm{Div}_{P_1})$ is zero if and only if it gives zero in each of Div_D, $\mathrm{Div}_{D'}$, … since Div_{P_1} is the direct sum of these components. We now consider Div_D in more detail.

Lemma 4.27. *Let* D *be a divisor on* V*, defined over a field* l*; write* Div_D *for the subgroup of* $\mathrm{Div}\, \bar{V}$ *generated by the geometrically irreducible components of* D*. Let* $\bar{D}$ *be one of those geometrically irreducible components, and let* l' *be the least extension of* l *over which* D *splits completely into its irreducible* *components; that is, l' is the least field of definition of $\bar{D}$. Let c be an element of $H^1(l, \mathbb{Q}/\mathbb{Z})$. Then $D \cup dc$ is zero in $H^2(l, \mathrm{Div}_D)$ if and only if the restriction of c to $H^1(l', \mathbb{Q}/\mathbb{Z})$ is trivial.*

Proof. This is the same game as the one we played to show that we need only consider one of the P_i above. The Galois theory here is described in [19]: briefly, the group $\mathrm{Gal}(l'/l)$ acts faithfully and transitively on the geometrically irreducible components of D. This means that we can apply the same proof as in Lemma 4.24 to show that Div_D is isomorphic to the $\mathrm{Gal}(\bar{l}/l)$-module induced from the $\mathrm{Gal}(\bar{l}/l')$-module $\mathbb{Z}\bar{D}$. The corestriction map

$$\mathrm{cores}_{l'/l} : H^2(l', \mathbb{Z}\bar{D}) \to H^2(l, \mathrm{Div}_D)$$

is therefore an isomorphism (Shapiro's Lemma).

Now we can write D as $N_{l'/l}\bar{D}$, and then by standard properties of the cup-product

$$D \cup dc = \mathrm{cores}_{l'/l}(\bar{D} \cup d(\mathrm{res}_{l'/l}\, c))$$

which, since the corestriction map is an isomorphism on $H^2(l', \mathbb{Z}\bar{D})$, is zero if and only if $\mathrm{res}_{l'/l}\, c$ is trivial. □

We can now put all the results in this section together to get a useful description of the group B:

Proposition 4.28. *Let $\mathcal{A}$ be an element of $\mathrm{Br}\, k(t)$, written in the form shown in (4.11). For each point P, pick a closed point P_1, defined over $k(P)$, lying above P. For each P, the fibre $\pi^* P_1$ splits over $k(P)$ into components; let $\bar{D}$ run through one geometrically irreducible component of each of these components. Then the lift of $\mathcal{A}$ to V is Azumaya if and only if:*

1. *$\sum_P n_P \,\mathrm{cores}_{k(P)/k}\, c_P = 0$;*

2. *the restriction of c to the least field of definition of each $\bar{D}$ is trivial.*

Proof. Combine Lemmas 4.23 and 4.27. □

4.5 An example

The results of Sections 4.2 and 4.3 can be adapted to give corresponding results about the vertical Brauer group, the group B and its relation to $H^1(k, \mathrm{Pic}_{\mathrm{vert}})$. Rather than repeating the details of those results here, we instead illustrate their applications by working through the calculation of B given in Section 6 of [44]; we then compute the elements of $H^1(k, \mathrm{Pic}_{\mathrm{vert}})$ corresponding to the algebras exhibited there, and show that those algebras all lift to equivalent Azumaya algebras on V.

4.5.1 Definitions

We work on the diagonal quartic surface V, defined by the equation (1.1), where the product $a_0a_1a_2a_3$ of the four coefficients is a square. We also assume that no other relation holds between the coefficients; in other words, the surface falls into case A1 of the classification in Appendix A.

The fibration $\pi : V \to \mathbb{P}^1$ is given explicitly in [44]; the only piece of information we will need is the description of the reducible fibres of π. It turns out that the coordinates of the points of $\mathbb{P}^1$ lying below the six geometrically reducible fibres fall into conjugate pairs. We will call these coordinates t_1, t_1', t_2, t_2', t_3, t_3'. Writing $u_1 = \sqrt{-a_2a_3}$, $u_2 = \sqrt{-a_1a_3}$, $u_3 = \sqrt{-a_1a_2}$, we have each conjugate pair t_i, t_i' lying in $\mathbb{Q}(u_i)$. The fibres above each point all consist of straight lines, as follows:

Point	Fibre
t_1	$L_{11}^{123} + L_{15}^{123} + L_{51}^{123} + L_{55}^{123}$
t_1'	$L_{33}^{123} + L_{37}^{123} + L_{73}^{123} + L_{77}^{123}$
t_2	$L_{11}^{231} + L_{15}^{231} + L_{51}^{231} + L_{55}^{231}$
t_2'	$L_{33}^{231} + L_{37}^{231} + L_{73}^{231} + L_{77}^{231}$
t_3	$L_{11}^{312} + L_{15}^{312} + L_{51}^{312} + L_{55}^{312}$
t_3'	$L_{33}^{312} + L_{37}^{312} + L_{73}^{312} + L_{77}^{312}$

It is easily checked that each of these fibres is indeed defined over the appropriate $\mathbb{Q}(t_i) = \mathbb{Q}(u_i)$, and that the automorphism of $\mathbb{Q}(u_i)/\mathbb{Q}$ interchanges the fibres above t_i and t_i'.

We also need to know the field of definition of one, hence all, of the geometrically irreducible components of each fibre. As an illustration, L_{11}^{123} is defined by the equations

$$X_0 = \sqrt[4]{-a_1/a_0}X_1, \quad X_2 = \sqrt[4]{-a_3/a_2}X_3.$$

Now, as $a_0a_1a_2a_3$ is a rational square, we have

$$\mathbb{Q}(u_1) = \mathbb{Q}(\sqrt{-a_2a_3}) = \mathbb{Q}(\sqrt{-a_1/a_0}) = \mathbb{Q}(\sqrt{-a_3/a_2})$$

and so the field of definition of L_{11}^{123} is given by

$$K_1 = \mathbb{Q}(u_1, \sqrt[4]{-a_1/a_0}, \sqrt[4]{-a_3/a_2}) = \mathbb{Q}(u_1, \sqrt{-a_1u_1\theta}, \sqrt{a_2u_1})$$

where θ is the (rational) square root of $a_0a_1a_2a_3$. Thus K_1 is a biquadratic extension of $\mathbb{Q}(u_1)$. Being deliberately vague about the choice of roots here does not matter: it merely gives another component of the same fibre. Replacing u_1 with $-u_1$ takes us to the conjugate fibre, that over t_1'. Permuting the indices cyclically gives the definitions of K_2 and K_3, the least fields of definition for the geometrically irreducible components of the fibres above t_2 and t_3 respectively.

4.5.2 Computing B

The computation of the subgroup B of $\mathrm{Br}\,\mathbb{Q}(t)$ is carried out in detail in [44]; we reproduce it here to illustrate the use of Proposition 4.28. Knowing that, in the case under consideration, $H^1(\mathbb{Q}, \mathrm{Pic}\,\bar{V})$ is of order 2, we look first for quaternion algebras; it will turn out that these are sufficient to list all elements of B.

Suppose that an algebra of the form (4.11) lies in B. We suppose that each c_P is a quadratic character on $k(P) = \mathbb{Q}(u_i)$; let the corresponding elements of $\mathbb{Q}(u_i)^\times/(\mathbb{Q}(u_i)^\times)^2$ be called α_i. The first condition of Proposition 4.28

then says that the product

$$\prod N_{\mathbb{Q}(u_i)/\mathbb{Q}} \alpha_i^{n_i} \tag{4.13}$$

must be a square in $\mathbb{Q}$; and the second condition says that each α_i must be a square in K_i. Now $(K_i^\times)^2/(\mathbb{Q}(u_i)^\times)^2$ is a 4-group, whose non-trivial elements are $a_j u_i$, $-a_i u_i \theta$ and their product $a_i a_k \theta$, where i, j, k is a cyclic permutation of $1, 2, 3$. Choosing α_i from these possibilities, we find that the only solutions making (4.13) a square are

$$N_{\mathbb{Q}(u_i)/\mathbb{Q}} a_i a_k \theta = (a_i a_k \theta)^2 \in (\mathbb{Q}^\times)^2 \quad (i = 1, 2, 3)$$

and

$$\prod_{i=1}^{3} N_{\mathbb{Q}(u_i)/\mathbb{Q}}(-a_i u_i \theta) = \prod (a_i^2 \theta^2 a_j a_k) \in (\mathbb{Q}^\times)^2$$

and therefore B is of order 16, generated by the four elements

$$\operatorname{cores}_{\mathbb{Q}(u_i)/\mathbb{Q}}(a_i a_k \theta, t - t_i) \quad (i = 1, 2, 3) \tag{4.14}$$

and

$$\sum_{i=1}^{3} \operatorname{cores}_{\mathbb{Q}(u_i)/\mathbb{Q}}(-a_i u_i \theta, t - t_i). \tag{4.15}$$

4.5.3 The map to $H^1(\mathbb{Q}, \mathrm{Pic}_{\mathrm{vert}})$

The subgroup $\mathrm{Pic}_{\mathrm{vert}}$ of $\mathrm{Pic}\,\bar{V}$ is that generated by the irreducible components of the fibres of π. Now each reducible fibre has four irreducible components, each of which is a straight line; each fibre is linearly equivalent to every other fibre, and by general theory about fibrations there are no non-trivial linear equivalences. Thus $\mathrm{Pic}_{\mathrm{vert}}$ is of rank 19, generated by the class of a fibre together with the classes of three irreducible components of each reducible fibre. The Galois action is that induced from $\mathrm{Pic}\,\bar{V}$, and so we can use the methods of Section 3.6.1 to compute

$$\frac{H^0(G, \mathrm{Pic}_{\mathrm{vert}} \otimes \mathbb{Q}/\mathbb{Z})}{\operatorname{im} H^0(G, \mathrm{Pic}_{\mathrm{vert}} \otimes \mathbb{Q})} \cong H^1(\mathbb{Q}, \mathrm{Pic}_{\mathrm{vert}}) \tag{4.16}$$

where again G is the Galois group over $\mathbb{Q}$ of the least field of definition of the 48 lines. The calculation shows that the group on the left is indeed generated by four elements of order 2, which we may lift to obtain

$$\begin{aligned} &\frac{1}{2}(L_{11}^{123} + L_{33}^{123} + L_{55}^{123} + L_{77}^{123}), \\ &\frac{1}{2}(L_{11}^{231} + L_{33}^{231} + L_{55}^{231} + L_{77}^{231}), \\ &\frac{1}{2}(L_{11}^{312} + L_{33}^{312} + L_{55}^{312} + L_{77}^{312}) \end{aligned} \tag{4.17}$$

and

$$\begin{aligned} \frac{1}{2}(L_{11}^{123} + L_{15}^{123} + L_{33}^{123} + L_{37}^{123} & \\ + L_{11}^{231} + L_{15}^{231} + L_{33}^{231} + L_{37}^{231} & \\ + L_{11}^{312} + L_{15}^{312} + L_{33}^{312} + L_{37}^{312}). & \end{aligned} \tag{4.18}$$

Now we show how these generators could instead be obtained by the map in Proposition 4.21. Note that the map in (4.16) is defined in precisely the same way as usual if we use the form (4.4) of $H^1(\mathbb{Q}, \mathrm{Pic}_{\mathrm{vert}})$; so we may forget about the components at infinity of the algebras (4.14) and (4.15), as described in Corollary 4.13.

First consider the algebra (4.14) with $i = 1$. This algebra is easy because $a_1 a_3 \theta$ is already rational; so

$$\mathrm{cores}_{\mathbb{Q}(u_1)/\mathbb{Q}}(a_1 a_3 \theta, t - t_1) = (a_1 a_3 \theta, N_{\mathbb{Q}(u_1)/\mathbb{Q}}(t - t_1)).$$

By the appropriate variant of Corollary 4.20, we must write the fibres above t_1 and t_1' as norms from $\mathbb{Q}(\sqrt{a_1 a_3 \theta})$. A short calculation reveals that

$$\pi^* t_1 + \pi^* t_1' = N_{\mathbb{Q}(\sqrt{a_1 a_3 \theta})/\mathbb{Q}}(L_{11}^{123} + L_{33}^{123} + L_{55}^{123} + L_{77}^{123})$$

which by Corollary 4.20 and the isomorphism (4.16) corresponds to the first of the generators (4.17). Similarly the $i = 2$ and $i = 3$ cases of (4.14) give the other two generators of (4.17).

For the fourth generator (4.15) of B, we must write each divisor $\pi^* t_i$ as a norm from $\mathbb{Q}(u_i, \sqrt{-a_i u_i \theta})$ to $\mathbb{Q}(u_i)$. Again, calculation shows that the appropriate form is

$$\pi^* t_1 = N_{\mathbb{Q}(u_1, \sqrt{-a_1 u_1 \theta})/\mathbb{Q}(u_1)}(L_{11}^{123} + L_{15}^{123})$$

and similarly for the other two components. The map between B and $H^1(\mathbb{Q}, \mathrm{Pic}_{\mathrm{vert}})$ commutes with corestriction, as does the isomorphism (4.16), so the element we obtain from the algebra (4.15) is

$$N_{\mathbb{Q}(u_1)/\mathbb{Q}}(L_{11}^{123} + L_{15}^{123}) + N_{\mathbb{Q}(u_2)/\mathbb{Q}}(L_{11}^{231} + L_{15}^{231}) + N_{\mathbb{Q}(u_3)/\mathbb{Q}}(L_{11}^{312} + L_{15}^{312})$$

which does indeed give the fourth generator (4.18) as desired.

4.5.4 Lifting to $\mathrm{Br}\, V$

The calculations in the previous section agree with the results obtained in [44]: that B is generated by four elements of order 2. However, we now show that those four generators all map to the same element of $\mathrm{Br}\, V$. That is, these four distinct elements of $\mathrm{Br}\, \mathbb{Q}(t)$ give equivalent Azumaya algebras when lifted to V.

In light of Proposition 4.21, all we need to show is that the four generators of $H^1(\mathbb{Q}, \mathrm{Pic}_{\mathrm{vert}})$ given in (4.17) and (4.18) all map to the same non-trivial element of $H^1(\mathbb{Q}, \mathrm{Pic}\, \bar{V})$. This map is the same as the map

$$\frac{H^0(G, \mathrm{Pic}_{\mathrm{vert}} \otimes \mathbb{Q}/\mathbb{Z})}{\mathrm{im}\, H^0(G, \mathrm{Pic}_{\mathrm{vert}} \otimes \mathbb{Q})} \to \frac{H^0(G, \mathrm{Pic}\, \bar{V} \otimes \mathbb{Q}/\mathbb{Z})}{\mathrm{im}\, H^0(G, \mathrm{Pic}\, \bar{V} \otimes \mathbb{Q})}$$

whose kernel is the image, in the object on the left, of $H^0(G, \mathrm{Pic}\, \bar{V} \otimes \mathbb{Q})$. An easy computation shows that the differences of the four generators of $H^1(\mathbb{Q}, \mathrm{Pic}_{\mathrm{vert}})$ do indeed lie in this kernel.

4.5.5 Other examples

The computations carried out for this example are easy to repeat with other cases and other fibrations; for example, the fibrations of Section 2.3.3 all have $\mathrm{Pic}_{\mathrm{vert}}$ groups which are straightforward to compute. It is *not* always the case that the map $B \to \mathrm{Br}_1 V/\mathrm{Br}_0 V$ is surjective, as in the example above. For instance, in the case where each quotient a_i/a_j is a square (case A3 in the tables of Appendix A), the group $\mathrm{Br}_1 V/\mathrm{Br}_0 V$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^5$. The fibration used in the previous example is defined, and the associated group B this time is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^6$; but its image in $\mathrm{Br}_1 V/\mathrm{Br}_0 V$ is only isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$.

Chapter 5

Numerical methods and examples

The material in the previous chapters has been somewhat removed from the original aim of studying the Brauer–Manin obstruction on diagonal quartic surfaces. This chapter contains some concrete examples, which show how the methods developed can be used to look at the Brauer–Manin obstruction. First we explain the algorithms used for two important peripheral procedures: testing local solubility of the equations, and searching for small solutions. Together, these give us the ability to look for surfaces which might have an interesting obstruction.

The rest of this chapter contains examples of calculating the Brauer–Manin obstruction for some diagonal quartic surfaces.

Note that most of the cases listed in Appendix A contain both locally soluble and locally insoluble surfaces. Some cases are always insoluble at some place: for example, case A3, where all the coefficients are squares, is insoluble in $\mathbb{R}$; and certain other cases are always insoluble in $\mathbb{Q}_2$.

5.1 Local solubility

Testing whether an equation has solutions everywhere locally is the natural first step to determining whether there are any integer solutions. We will now show how this is accomplished. The main tool is Hensel's Lemma, which we state in the following form.

Lemma 5.1 (Hensel). *Let $f(X_0, \ldots, X_n)$ be a polynomial in $n+1$ variables with integer coefficients. Fix a prime p, and suppose that there exist integers (x_i) and $0 \leq j \leq n$ such that $0 \leq 2k < m$, where*

$$k = v_p\left(\frac{\partial f}{\partial X_j}(x_0, \ldots, x_n)\right)$$
$$m = v_p(f(x_0, \ldots, x_n)).$$

Then there exists $\alpha \in \mathbb{Q}_p$ such that, replacing x_j by α, we have

$$f(x_0, \ldots, \alpha, \ldots, x_n) = 0$$

and α is congruent to x_j modulo p^{m-k}.

Proof. See Serre [36, Chapter 2, 2.2, Theorem 1]. □

In particular, Hensel's Lemma shows this: let $\bar{f}$ be the polynomial over $\mathbb{F}_p$ obtained by reducing f modulo p; then each smooth point of the variety over $\mathbb{F}_p$ defined by $\bar{f}$ lifts to a point of the variety over $\mathbb{Q}_p$ defined by f.

To begin, we show that there are only finitely many primes at which local solubility of the diagonal quartic is not automatic.

Lemma 5.2. *Let p be a prime, not equal to 2 or 5 and not dividing $a_0a_1a_2a_3$. Then the equation (1.1) has solutions in $\mathbb{Q}_p$.*

Proof. It is enough to check solubility in $\mathbb{F}_p$: for the conditions on p imply that any solution in $\mathbb{F}_p$ must satisfy the conditions for Hensel's Lemma to be applied, and hence lifts to a solution in $\mathbb{Q}_p$.

It follows from the Weil conjectures (see [28, Chapter 26]) that the number N_p of points on our surface over $\mathbb{F}_p$ satisfies

$$|N_p - (p^2 + 1)| \leq 22p$$

where the 22 here is the second Betti number of the surface over $\mathbb{C}$. Therefore, for $p \geq 23$, the surface always has points.

Next, suppose that $p \equiv 3 \pmod 4$. Then squares in $\mathbb{F}_p$ are all fourth powers: for if a is a square, with square roots $\pm x$, then the fact that -1 is not a square means that either x or $-x$ must be a square, and hence a is a fourth power. Hence solving (1.1) is equivalent to solving the equation

$$a_0X_0^2 + a_1X_1^2 + a_2X_2^2 + a_3X_3^2 = 0$$

where the coefficients are all non-zero in $\mathbb{F}_p$; but this has solutions, by the Chevalley–Warning theorem (see [36, Chapter I, 2.2, Corollary 2]).

This leaves the primes 13 and 17. For each of these, a short computer search shows that all diagonal quartics with non-zero coefficients have a solution. □

Next, we show how to test local solubility at one given prime p, which may divide $a_0a_1a_2a_3$. Continuity shows that near every smooth point of $V(\mathbb{Q}_p)$ is an integer point which satisfies the hypothesis of Hensel's Lemma. A naïve approach to testing local solubility might work thus: search for all solutions to (1.1) in $\mathbb{F}_p$. If a solution is found which fulfils the conditions for applying Hensel's Lemma, we are done; otherwise search through the possible lifts of each solution to $\mathbb{Z}/p^2\mathbb{Z}$, and so on. This is essentially the approach we will use, though in a slightly different form. Our method is the same as that used by Pinch for his calculations [31].

We may assume that the coefficients a_i are coprime integers, and that no a_i is divisible by a fourth power. If we multiply each a_i by p and then remove any factors of p^4 which might have appeared, we obtain a new equation which clearly has rational solutions if and only if the original one has; but the new equation has a different reduction modulo p. Repeating this process gives four polynomials over $\mathbb{F}_p$ which are all "valid reductions modulo p" of the original variety. We call these polynomials $\bar{f}_j$, where j takes values from 0 to 3. They might be described thus:

$$\bar{f}_j(X_0, X_1, X_2, X_3) = b_{0j}X_0^4 + b_{1j}X_1^4 + b_{2j}X_2^4 + b_{3j}X_3^4$$

where

$$b_{ij} \equiv \begin{cases} p^{-v_p(a_i)} a_i & \text{if } v_p(a_i) \equiv j \pmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 5.3. *Let p be an odd prime. The equation* (1.1) *has a solution in $\mathbb{Q}_p$ if and only if there exists a smooth point on the variety over $\mathbb{F}_p$ defined by one of the polynomials $\bar{f}_j$.*

Proof. If there is such a smooth point, we can apply Hensel's Lemma to lift it to a point in $\mathbb{Q}_p$.

Conversely, suppose that there is a solution P in $\mathbb{P}^3(\mathbb{Q}_p)$. By continuity, we can find integers (x_0, x_1, x_2, x_3) such that

$$f(x_0, x_1, x_2, x_3) = a_0 x_0^4 + a_1 x_1^4 + a_2 x_2^4 + a_3 x_3^4$$

has arbitrarily high p-adic valuation. Now choose i_0 such that $v_p(4a_{i_0} x_{i_0}^3)$ is minimal; we may in addition ensure that $v_p(x_{i_0}) = 0$, as no a_i has valuation higher than 3 by our earlier assumptions. Write j for $v_p(a_{i_0})$. We now define new coefficients a_i' by

$$a_i' = \begin{cases} p^{-j} a_i & \text{if } v_p(a_i) \geq j \\ p^{4-j} a_i & \text{if } v_p(a_i) < j \end{cases}$$

and new values x_i' by

$$x_i' = \begin{cases} x_i & \text{if } v_p(a_i) \geq j \\ x_i/p & \text{if } v_p(a_i) < j \end{cases}$$

where the expression x_i/p is an integer, because otherwise we would have chosen i_0 differently. The polynomial

$$f'(X_0, X_1, X_2, X_3) = a_0' X_0^4 + a_1' X_1^4 + a_2' X_2^4 + a_3' X_3^4$$

reduces modulo p to $\bar{f}_j$. The new point (x_0', x_1', x_2', x_3') is a solution to $\bar{f}_j$ provided that we chose our original integer solution close enough to the p-

adic solution; and moreover $4a'_{i_0}x'_{i_0}$ is a unit in $\mathbb{F}_p$, so the point is smooth. □

For $p = 2$, small changes are needed. To apply Hensel's Lemma, we need a solution in the ring $\mathbb{Z}/32\mathbb{Z}$ with not all the $a_i x_i$ divisible by 2. The same argument works, though, and we obtain

Proposition 5.4. *The equation* (1.1) *has a solution in* $\mathbb{Q}_2$ *if and only if one of the polynomials* $\bar{f}_j$*, considered over the ring* $\mathbb{Z}/32\mathbb{Z}$*, has a solution* (x_0, x_1, x_2, x_3) *where some* $a_i x_i$ *is not divisible by* 2. □

5.2 Finding small solutions

Searching for small solutions of the equation (1.1), with given coefficients a_i, is not an entirely straightforward procedure and merits some discussion.

We will consider only those cases where two coefficients are positive and the other two negative; this does not appear to be a great restriction, as a wide variety of cases are still available for experimentation. Anyway, the modifications needed to deal with other cases are not substantial. The equation can then be written as

$$ax^4 + by^4 = cu^4 + dv^4 \tag{5.1}$$

where a, b, c and d are coprime positive integers, free of fourth powers; and we seek solutions with x, y, u and v coprime and positive.

The "small" here means that we seek points of height less than a given bound; the height used is the standard height on $\mathbb{P}^3(\mathbb{Q})$, so that

$$H(x : y : u : v) = \max\{x, y, u, v\}$$

where x, y, u, v are coprime integers.

There is a reasonably straightforward way to find solutions to (5.1) of height less than or equal to H, which works as follows.

1. For each pair (x, y) with $0 \leq x, y \leq H$, put the triple $(x, y, ax^4 + by^4)$ in a list.

2. For each pair (u, v) with $0 \leq u, v \leq H$, put the triple $(u, v, cu^4 + dv^4)$ in a second list.

3. Sort both lists on the third elements of the triples.

4. Merge the two lists: for each triple (x, y, A) from the first list and (u, v, B) from the second list such that $A = B$, print the solution (x, y, u, v).

This algorithm is moderately successful for small H, but rapidly runs out of space to store the lists. To work for $H = 10^4$, say, each of the two lists must contain 10^8 elements, each of size 10 bytes or so; that is already a gigabyte of storage. This may be written to a file, but the sorting either requires that the entire file fit in memory, or else is extremely slow. The sorting can be avoided by using some data structure which sorts the data as it is inserted; but storage space is still a serious constraint. A more sophisticated algorithm is needed.

The answer is found in a paper by Bernstein [4]. Here an algorithm is given for enumerating the values of $p(x) + q(y)$ in increasing order, where p and q are increasing functions of x and y respectively. The algorithm makes use of a *heap*, which is a data structure particularly suited to the operation needed, namely insertion of a new element whilst removing the smallest element. Briefly, the algorithm works roughly as follows. The heap contains triples $(x, y, p(x) + q(y))$, and there is always precisely one element in the heap for each value of y from 0 to H. On each iteration, the triple with the smallest value of $p(x) + q(y)$ is removed, and the new triple inserted into the heap is $(x + 1, y, p(x + 1) + q(y))$. When x reaches H, no new triple is inserted.

The storage required for this algorithm is only of the order of H, compared with H^2 for the previous naïve method. Applying it to diagonal quartic surfaces with small integral coefficients allows us to search for solutions of height up to about 10^4. A barrier is reached, though, when the quantities $ax^4 + by^4$ can no longer be stored in 64 bits: for that is the largest size of integer which most desktop computers can use in arithmetic operations.

There are several ways round this problem. One is to perform all operations modulo some prime which is slightly less than 2^{64}, and then find out which of these solutions come from integer solutions. Another is to work modulo two or more primes, whose product is greater than the largest number which will arise. Finally, one can use a multiple-precision integer arithmetic library: this is the solution used to produce the results in this chapter. The `sortedsums` package written by Bernstein was modified to use the PARI library. Using this algorithm on a Pentium III running at 800 MHz, it takes less than four seconds to list all solutions of height less than 1000 to a given diagonal quartic equation of the form (5.1). Solutions of height less than 10^4 can be listed in about ten minutes.

It would be possible to speed up this algorithm by a constant factor by using various local constraints. In particular, fourth powers can only be congruent to 0 or 1 modulo 16, so taking advantage of this would be an easy way to gain some speed. Similarly one can use the fact that fourth powers are 0 or 1 modulo 5.

Appendix B contains a list of all the diagonal quartic surfaces of the form (5.1), with integral coefficients between 1 and 15, which are everywhere locally soluble but have no points of height less than 10^4. This list was produced using the algorithms described above, and will be useful to provide examples for more detailed study.

5.3 Example with a fibration

In this example, we look at the Brauer–Manin obstruction on the particular surface V defined by

$$X_0^4 + X_1^4 = 6X_2^4 + 12X_3^4. \tag{5.2}$$

This surface appears in the list of Appendix B, so has no rational points of height less than 10^4. We will describe an element of the unique non-trivial class of the Brauer group of V, and show that the resulting Brauer–Manin obstruction is non-trivial. This proves that the equation (5.2) has no rational solutions.

The surface (5.2) falls into case A121 of the classification listed in Appendix A. Using the methods of Chapter 3, we determine that the Picard group over $\mathbb{Q}$ is of rank 2. There is an elliptic fibration on this surface defined over the rational numbers: two singular fibres of the fibration are

$$F = L_{11}^{123} + L_{15}^{123} + L_{31}^{123} + L_{35}^{123}$$
$$F' = L_{53}^{123} + L_{57}^{123} + L_{73}^{123} + L_{77}^{123}.$$

We can easily write down defining equations for F:

$$F : X_0^2 - \sqrt{-2}X_0X_1 - X_1^2 = 0, \quad X_2^2 - \sqrt{-2}X_3^2 = 0.$$

The equations for F' are the conjugates over $\mathbb{Q}$ of those for F. Note that, although the fibration is defined over $\mathbb{Q}$, these two singular fibres are not: they are defined over $K = \mathbb{Q}(\sqrt{-2})$. In fact, we do not at this stage know the equation for any rational fibre; neither do we have any explicit description of a map from V to $\mathbb{P}^1$ defined over $\mathbb{Q}$. What we can do is write down a function with a zero along F and a pole along F':

$$f(X_0, X_1, X_2, X_3) = \frac{X_0^2 - \sqrt{-2}X_0X_1 - X_1^2}{X_2^2 + \sqrt{-2}X_3^2}.$$

Here the numerator of the rational function is zero along F and on the remaining L_{1n}^{123} and L_{3n}^{123}. The denominator is zero on F' and also along those same straight lines; thus the divisor of f is as desired. The morphism $\pi = (1 : f)$ defines a map from V to $\mathbb{P}^1$, albeit only over K.

Proposition 4.28 states that we can write down elements of the Brauer group of the surface by using these singular fibres. The group $\operatorname{Br}_1 V / \operatorname{Br}_0 V$ has order 2, so any Azumaya algebra we can find which is not equivalent to a constant algebra lies in the non-trivial class. To use Proposition 4.28, though, the fibre at infinity must be non-singular and defined over $\mathbb{Q}$; our map π has fibre at infinity equal to F', which is neither. We must find a fibre of π which is defined over $\mathbb{Q}$, which after a change of coordinates on $\mathbb{P}^1$ will be our new fibre at infinity.

A fibre is defined over $\mathbb{Q}$ if and only if it is fixed by the Galois action on V. To find such a fibre, we write the equation for a general fibre

$$f(X_0, X_1, X_2, X_3) = c$$

and seek a value of c such that $\{f^\sigma = \sigma c\}$ defines the same variety as $\{f = c\}$, where σ is the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$. Now note that f^σ has divisor $F' - F$, and therefore $N_{K/\mathbb{Q}} f = f^\sigma f$ is a constant. In fact we have

$$f^\sigma f = \frac{X_0^4 + X_1^4}{X_2^4 + 2X_3^4} = 6.$$

Now, suppose that the two varieties $\{f = c\}$ and $\{f^\sigma = \sigma c\}$ are the same; then, multiplying the two equations, we have

$$N_{K/\mathbb{Q}} c = N_{K/\mathbb{Q}} f = 6$$

and, conversely, if $N_{K/\mathbb{Q}} c = N_{K/\mathbb{Q}} f$ then $f = c$ if and only if $f^\sigma = \sigma c$, that is, the fibre over c is fixed by the Galois action and is therefore defined over $\mathbb{Q}$.

A solution is

$$c = 2 - \sqrt{-2}.$$

The function $f/(f-c)$ therefore has a zero at the singular fibre F, and a pole at some fibre of π which is defined over the rationals. Therefore this function can play the rôle of the function $\pi^*(t - t_P)$ of Proposition 4.28.

Were we interested in having an equation for a map from V to $\mathbb{P}^1$ defined over $\mathbb{Q}$, we would note that by Hilbert's theorem 90 the general solution to $N_{K/\mathbb{Q}}(c) = 6$ is

$$c = \frac{(2 - \sqrt{-2})(u - \sqrt{-2}v)}{u + \sqrt{-2}v}.$$

Setting f equal to this expression, we can derive the desired equation. In this situation, though, all we need are defining equations for one rational fibre.

According to Proposition 4.28, the other piece of information needed to write down an Azumaya algebra on V is a character on $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ which becomes trivial when restricted to the least field of definition of one of the geometrically irreducible components of F. That field is

$$L = K(\sqrt{-1}, \sqrt[4]{-2})$$

which is a biquadratic extension of K. The characters which satisfy the above requirement are the quadratic characters associated to -1 and $\pm\sqrt{-2}$. To satisfy the first condition of Proposition 4.28 as well, we choose the character associated to -1. We now have a non-trivial Azumaya algebra of V: it is the algebra $\mathcal{A} = (-1, G)$, where

$$\begin{aligned} G &= N_{K/\mathbb{Q}}\left(\frac{f}{f-c}\right) \\ &= \frac{Nf}{(f-c)(f-c)^\sigma} \\ &= \frac{Nf}{Nf + Nc - fc^\sigma - f^\sigma c} \\ &= \frac{6}{12 - \mathrm{Tr}(fc^\sigma)}. \end{aligned}$$

Using the identity $\mathrm{Tr}(a/b) = \mathrm{Tr}(ab^\sigma)/Nb$, we get

$$\begin{aligned} \mathrm{Tr}(fc^\sigma) &= \frac{\mathrm{Tr}\left((X_0^2 - \sqrt{-2}X_0X_1 - X_1^2)(2+\sqrt{-2})(X_2^2 - \sqrt{-2}X_3^2)\right)}{X_2^4 + 2X_3^4} \\ &= \frac{4X_0^2X_2^2 + 4X_0^2X_3^2 - 8X_0X_1X_3^2 + 4X_0X_1X_2^2 - 4X_1^2X_2^2 - 4X_1^2X_3^2}{X_2^4 + 2X_3^4} \\ &= \frac{4\left((X_2^2 + X_3^2)(X_0^2 - X_1^2) + (X_2^2 - 2X_3^2)X_0X_1\right)}{X_2^4 + 2X_3^4} \end{aligned}$$

and, substituting into the above expression for G,

$$\begin{aligned} G &= \frac{6(X_2^4 + 2X_3^4)}{12(X_2^4 + 2X_3^4) - 4(X_2^2 + X_3^2)(X_0^2 - X_1^2) - 4(X_2^2 - 2X_3^2)X_0X_1} \\ &= \frac{X_0^4 + X_1^4}{2(X_0^4 + X_1^4) - (4X_2^2 + 4X_3^2)(X_0^2 - X_1^2) - 4(X_2^2 - 2X_3^2)X_0X_1}. \end{aligned}$$

We now calculate the Brauer–Manin obstruction associated to $\mathcal{A}$. For each place v of $\mathbb{Q}$, including the real place, $\mathrm{Br}(\mathbb{Q}_v)[2]$ is cyclic of order 2; the invariant inv_v is directly related [35, Chapter XIV] to the Hilbert symbol $(\quad,\quad)_v$. For each adèlic point (x_v) of V, we must evaluate

$$(-1)^{2\sum_v \mathrm{inv}_v \mathcal{A}(x_v)} = \prod_v (-1, G(x_v))_v.$$

At each place, the function $(-1, G(x_v))_v$ is continuous, hence locally constant, on $V(\mathbb{Q}_v)$. If we were to find a place where this function were not constant, there could be no Brauer–Manin obstruction: for by changing our adèlic point at that place, we could always make the sum of the invariants equal zero.

We note (see [10, Lemma 3.1.2]) that the complement of any union of divisors on V is dense in V, not only in the Zariski topology but also in the real or p-adic topology on each $V(\mathbb{Q}_v)$. Therefore we need not check the Brauer–Manin condition on the support of (G).

For primes p not equal to 2 or 3, both the surface V and the algebra $\mathcal{A}$ have good reduction. It follows (see [25, Chapter VI, §44]) that $\mathrm{inv}_p \mathcal{A}(x_p)$ is zero on all of $V(\mathbb{Q}_p)$.

At $p = 3$, we note that -2 is a square in $\mathbb{Q}_3$. The algebra $\mathcal{A}$ splits over $K = \mathbb{Q}(\sqrt{-2})$, hence over $\mathbb{Q}_3$ which contains a copy of K. Thus the local invariant is constantly zero on $V(\mathbb{Q}_3)$.

At $p = 2$, looking at the equation (5.2) modulo 16 shows that any primitive solution must have all four X_i odd. To evaluate the obstruction, it turns out that we must look at the X_i modulo 32. Now, if X_i is known modulo 2^5, then X_i^4 is known modulo 2^7. This means that the value of

$$P = X_0^4 + X_1^4 - 6X_2^4 - 12X_3^4$$

is known modulo 2^7. Suppose that we know a solution to

$$P(X_0, X_1, X_2, X_3) \equiv 0 \pmod{2^7}. \tag{5.3}$$

We apply Hensel's Lemma, considering P as a polynomial in the one variable X_0. The derivative is $P' = 4X_0^3$, which has 2-adic valuation 2 since X_0 is odd. The conclusion of Hensel's Lemma states that our solution lifts to one in $\mathbb{Q}_2$ which is unique modulo

$$2^{v_2(P(X_0,X_1,X_2,X_3))-v_2(P'(X_0,X_1,X_2,X_3))} = 2^5$$

and therefore the primitive solutions to (5.3) are, modulo 2^5, equivalent to all primitive solutions to P in $\mathbb{Q}_2$.

Using a computer, we list all the solutions modulo 32 to (5.3). Now, up to squares, G is equivalent to

$$(X_0^4+X_1^4)(2(X_0^4+X_1^4)-4(X_2^2+X_3^2)(X_0^2-X_1^2)-4(X_2^2-2X_3^2)X_0X_1) \quad (5.4)$$

and knowing the X_i modulo 32 gives the value of (5.4) modulo 2^8. We evaluate the expression (5.4) for each solution found, and discover that the value is always congruent to either 96 or 176 modulo 2^8. In either case, by the description of the Hilbert symbol in [36, Chapter III, 1.2, Theorem 1], we can evaluate $(-1, G(x_2))_2 = -1$ for all points x_v of $V(\mathbb{Q}_2)$.

Over $\mathbb{R}$, we note that the function G has no zeros in $V(\mathbb{R})$: if so, we would have

$$X_0^4 + X_1^4 = 6X_2^4 + 12X_3^4 = 0$$

and hence all the X_i equal to zero. The one pole of G lies on the curve of genus 1 which is the fibre defined by $f = c$, and is a double pole; so in a neighbourhood of any simple point of this curve, G takes either only positive or only negative values. We deduce that G is either everywhere positive or everywhere negative. Evaluation at the point $(2:2:1:\sqrt[4]{13/6})$ reveals that G is everywhere positive. Hence $(-1, G)_{\mathbb{R}}$ is everywhere equal to $+1$.

Combining these results, we obtain

$$\sum_v \operatorname{inv}_v \mathcal{A}(x_v) = \frac{1}{2}$$

for all adèlic points (x_v) of $V(\mathbb{A}_{\mathbb{Q}})$. Thus the equation (5.2) has no rational solutions.

5.4 Example with no fibration

Our second example is a surface which falls into the most general class, that is, case A222 in the table of Appendix A. From the list of Appendix B we choose the surface $(2, 6, 7, 15)$, which we rearrange as

$$7X_0^4 + 15X_1^4 = 2X_2^4 + 6X_3^4. \tag{5.5}$$

This surface has Picard group of rank 1, generated by the class Π of a plane section. The group $\operatorname{Br}_1 V / \operatorname{Br}_0 V$ is again of order 2, so any non-trivial Azumaya algebra will give the same obstruction.

Although the surface clearly has no elliptic fibration, we can still use the fibrations studied earlier to construct an Azumaya algebra. We will use Proposition 4.17. For this we must find a cyclic extension $L/\mathbb{Q}$, a non-principal divisor D defined over L, and a function $f \in k(V)$ such that $(f) = N_{L/\mathbb{Q}} D$.

The case studied in detail in [44] shows that if we take $L = \mathbb{Q}(\sqrt{a_0 a_1 a_2 a_3})$, then the surface V defined by (5.5) has a pencil of curves of genus 1 defined over L. Explicit descriptions are given in [44] of equations defining this fibration. Let F be one fibre, defined over L; then we will construct a function f defined over $\mathbb{Q}$ such that

$$(f) = F + \sigma F - 2\Pi = N_{L/\mathbb{Q}}(F - \Pi) \tag{5.6}$$

to satisfy Proposition 4.17.

The surface (5.5) has $a_0 a_1 a_2 a_3 = 6^2 \times 35$, and so we take $L = \mathbb{Q}(\sqrt{35})$. To write down equations for the fibration, the recipe given in [44] requires that we solve the equation

$$15r_1^2 - 2r_2^2 - 6r_3^2 = 0 \tag{5.7}$$

over L. If instead we were to use the approach of the previous example, we would take a singular fibre consisting of straight lines but not defined over L; we would use that to produce an equation for the fibration, not defined over L; and we would then try to turn that equation into one defined over L. In the previous example, that last step involved solving a simple norm equation. If we try that approach in this example, we must again solve a norm equation; that turns out to be equivalent to solving (5.7). We therefore stick to the recipe given in [44].

Solving the conic equation (5.7) is not entirely straightforward; a good discussion of how to approach such an equation is given in Simon's thesis [40]. We first apply Legendre's technique of descent to reduce the equation to

$$x^2 - \omega y^2 = 3z^2$$

where $\omega = 6 + \sqrt{35}$ is a fundamental unit in L. Then a computer search reveals a solution, which gives

$$(r_1, r_2, r_3) = (20 + 2\sqrt{35}, 15, 20 + 5\sqrt{35}).$$

Putting these into Swinnerton–Dyer's recipe and removing some spare factors gives polynomials

$$\begin{aligned} A &= 3(\sqrt{35}X_0^2 - (20 + 5\sqrt{35})X_1^2 + (20 + 2\sqrt{35})X_3^2) \\ B &= (35 + 4\sqrt{35})X_0^2 + 15X_1^2 + (20 + 2\sqrt{35})X_2^2 \\ C &= (-35 - 4\sqrt{35})X_0^2 - 15X_1^2 + (20 + 2\sqrt{35})X_2^2 \\ D &= \sqrt{35}X_0^2 - (20 + 5\sqrt{35})X_1^2 - (20 + 2\sqrt{35})X_3^2 \end{aligned}$$

such that $AD = BC$ gives the equation (5.5) of the original surface. The two fibrations $\pi_i : V \to \mathbb{P}^1$ are defined by

$$\begin{aligned} \pi_1 &= (A : B) = (C : D) \\ \pi_2 &= (A : C) = (B : D) \end{aligned}$$

and the classes in $\operatorname{Pic} V_L$ of these two fibrations are conjugates over $\mathbb{Q}$. If we write (A) for the divisor of zeros of the polynomial A, and so on, then

$$(A) = F_1 + F_2 \qquad (B) = F_1' + F_2$$
$$(C) = F_1 + F_2' \qquad (D) = F_1' + F_2'$$

where F_1 and F_1' are two fibres of π_1, each defined over L, and similarly F_2 and F_2' are two fibres of π_2.

The goal now is to find a function f satisfying (5.6), where we take $F = F_1$. This requires that we know some more about σF_1. It is a fibre, defined over L, of π_2, and therefore defined by an equation of the form $B/D = c$ for some constant $c \in L$. To find c, it suffices to evaluate B/D at any point of σF_1. We first find a $\bar{\mathbb{Q}}$-valued point on F_1: such a point is a common zero of A and C. Rearranging the equation $A = 0$ gives us X_3^2 in terms of X_0 and X_1; similarly $C = 0$ yields an expression for X_2^2. Setting $X_0 = 0$ and $X_1 = 1$ gives

$$X_2^2 = \frac{r_2}{r_1} \qquad X_3^2 = \frac{r_3}{r_1}$$

and, taking conjugates and substituting into B/D, we obtain

$$\frac{B}{D}(\sigma F_1) = -6$$

We can now use this to write down a suitable function f:

$$\frac{C}{X_0^2}\left(\frac{B}{D} + 6\right) = \frac{A + 6C}{X_0^2}$$

which after removing a constant factor gives

$$f(X_0, X_1, X_2, X_3) = \frac{7X_0^2 + 5X_1^2 - 4X_2^2 - 2X_3^2}{X_0^2}.$$

To evaluate the obstruction, we may ignore the X_0^2 in the denominator of f. At each place v of $\mathbb{Q}$, we look at $(35, g)_v$ where $g = 7X_0^2 + 5X_1^2 - 4X_2^2 - 2X_3^2$.

At $p = 2$, looking at the equation (5.5) modulo 16 shows that X_2 must be even and the other X_i all odd. Evaluating g at each possible solution modulo 16 always gives a result congruent to 6 or 14 modulo 16, and hence

$(35, g)_2 = -1$ everywhere.

At $p = 3$, we list the solutions modulo 27 and find that the value of g at each point is either 6, 15 or 24 modulo 27; hence $(35, g)_3 = -1$.

At $p = 5$, the situation is quite different. Using the formula in [36, Chapter III, 1.2, Theorem 1], we have

$$(35, b)_5 = \left(\frac{7}{5}\right)^{\beta} \left(\frac{v}{5}\right) = (-1)^{\beta} \left(\frac{v}{5}\right)$$

where $b = 5^{\beta} v$ with v a 5-adic unit. Listing the solutions modulo 25 shows that the value of g is always a unit, but is sometimes a quadratic residue modulo 5 and sometimes not. For example, the point $(2 : 1 : 1 : 5)$ satisfies Hensel's Lemma, so lifts to a point of $V(\mathbb{Q}_5)$, and we have

$$g(2, 1, 1, 5) \equiv 4 \pmod{25}.$$

Now any element of $\mathbb{Q}_5$ congruent to 4 modulo 25 is a square, and so at that point $(35, g)_5 = 1$. However, the point $(2 : 2 : 7 : 5)$ also lifts to a point of $V(\mathbb{Q}_5)$; but there, we have

$$g(2, 2, 7, 5) \equiv 2 \pmod{25}$$

which cannot be a square in $\mathbb{Q}_5$, so $(35, g)_5 = -1$ there.

At $p = 7$, a similar phenomenon occurs: $(35, g)_7$ takes both values ± 1 on $V(\mathbb{Q}_7)$. Therefore there is no arithmetic Brauer–Manin obstruction to the existence of rational points on the surface (5.5).

Given the number of surfaces we have found in this category with no small rational points, it seems reasonable to conjecture that the Brauer–Manin obstruction is not the only obstruction to the Hasse principle for diagonal quartic surfaces, at least when no elliptic fibration is defined.

5.5 Trivial Brauer group

The calculations leading to the tables of Appendix A reveal certain families of diagonal quartic surfaces with Brauer group as small as possible: that is, $\mathrm{Br}_1 V / \mathrm{Br}_0 V$ is trivial. For these surfaces, no Brauer–Manin obstruction can possibly come from the arithmetic part of the Brauer group; and so studying such a family of surfaces is an apparently attractive way of investigating whether there can be surfaces with trivial Brauer–Manin obstruction but no rational points.

One such class is case A127 of the table, where the equation of the surface looks like

$$X_0^4 + aX_1^4 = 4(aX_2^4 + 2b^2X_3^4) \tag{5.8}$$

for suitably general constants a and b. It is straightforward to produce a list of surfaces like this, to test local solubility and to search for solutions. Appendix C contains a list of such surfaces with no point of height less than 10^4.

Unfortunately, it is not possible to draw many conclusions from these results. For the coefficients of the surfaces quickly become moderately large (or at least not small). It seems reasonable to believe that a diagonal quartic surface with large coefficients might also have large solutions; therefore the non-existence of a point of height less that 10^4 on a surface with even slightly large coefficients should not be taken as an indication that the surface is unlikely to have any points at all.

This rather vague idea is borne out by some numerical experimentation: surfaces with coefficients of the order of 15 appear far less likely to have a point of height less that 10^4 than surfaces with coefficients all less that 4, say. This effect occurs partly because surfaces with small coefficients are more likely to fall into a narrow case of our classification and so have rational curves. However, even if we exclude points on the 48 lines, which account for much of that phenomenon, then surfaces with small coefficients still appear in general to have more small points than surfaces with large coefficients. We conclude that, if meaningful results were to be obtained when searching for points on surfaces such as those in Appendix C, then it would be necessary to search to a higher height than we have been able to.

Appendix A

Tables of cases

This appendix contains tables listing the 546 different cases into which the Galois action of $\mathrm{Gal}(\bar{k}/k)$ on $\mathrm{Pic}\,\bar{V}$ may fall. The cases are split first by the base field k: each of the five tables corresponds to one of the possible fields $k \cap \mathbb{Q}(\epsilon)$. Within each table, the cases are split according to whether the product $a_0a_1a_2a_3$ is a square, minus a square, twice a square, minus twice a square, or none of these. Where k contains square roots of -1 or 2, some of these cases merge.

The first column in each table contains the index number of the case: this has no meaning and comes simply from the order in which the cases were originally listed. The second column shows a generic example of the coefficients (a_0, a_1, a_2, a_3) for this case, as described in Section 3.5.2. The third column contains the rank of the group $H^0(k, \mathrm{Pic}\,\bar{V})$. The fourth column shows the structure, as a product of cyclic groups, of the group $\mathrm{Br}_1\,V/\,\mathrm{Br}_0\,V$ in each case. This is isomorphic to $H^1(k, \mathrm{Pic}\,\bar{V})$. The final column list all those immediate subcases of each case which appear in the same table.

A.1 $k \cap \mathbb{Q}(\epsilon) = \mathbb{Q}$

Number	Example	ρ	Br_1	Subcases
		$a_0a_1a_2a_3$ square		
A1	$[1, c_1, c_2, c_3^2c_2^3c_1^3]$	2	$[2]$	A2, A4, A6, A8, A36, A37, A56, A84
A2	$[1, c_1^2, c_2, c_3^2c_2^3]$	2	$[2,2,2]$	A3, A5, A7, A9, A11, A13, A15, A25, A38, A50, A57, A87
A3	$[1, c_1^2, c_2^2, c_3^2]$	2	$[2,2,2,2,2]$	A16, A26, A60, A96
A4	$[1, -4c_1^2, c_2, -4c_3^2c_2^3]$	2	$[2]$	A5, A10, A12, A14, A21, A31, A43, A53, A65, A99
A5	$[1, c_1^2, -4c_2^2, -4c_3^2]$	2	$[2,2,2]$	A17, A22, A27, A32, A68, A105
A6	$[1, 2c_1^2, c_2, 2c_3^2c_2^3]$	2	$[2]$	A7, A10, A48, A76, A85
A7	$[1, c_1^2, 2c_2^2, 2c_3^2]$	2	$[2,2,2]$	A18, A28, A77, A90
A8	$[1, -8c_1^2, c_2, -8c_3^2c_2^3]$	2	$[2]$	A9, A10, A49, A79, A86
A9	$[1, c_1^2, -8c_2^2, -8c_3^2]$	2	$[2,2,2]$	A19, A29, A80, A93
A10	$[1, -4c_1^2, 2c_2^2, -8c_3^2]$	2	$[2]$	A23, A33, A82, A102
A11	$[1, c_1, c_2^2c_1^3, c_1^2]$	2	$[2,2,2]$	A16, A17, A28, A29, A41, A52, A58, A89
A12	$[1, c_1, -4c_2^2c_1^3, -4c_1^2]$	2	$[2]$	A22, A33, A46, A55, A66, A101
A13	$[1, c_1, c_2^2c_1^3, 4c_1^2]$	2	$[2,2,2]$	A18, A19, A26, A27, A42, A52, A59, A88
A14	$[1, c_1, -4c_2^2c_1^3, -c_1^2]$	2	$[2,2]$	A23, A32, A47, A55, A67, A100

Number	Example	ρ	Br_1	Subcases
A15	$[1, c_1^2, c_2, c_2]$	2	$[2, 2, 2]$	A16, A17, A18, A19, A39, A51, A58, A88
A16	$[1, c_1^2, c_2^2, 1]$	2	$[2, 2, 2, 2, 2]$	A20, A30, A61, A97
A17	$[1, -4c_1^2, -4c_2^2, 1]$	2	$[2, 2, 2, 2]$	A24, A34, A69, A106
A18	$[1, 2c_1^2, 2c_2^2, 1]$	2	$[2, 2, 2]$	A78, A91
A19	$[1, -8c_1^2, -8c_2^2, 1]$	2	$[2, 2, 2]$	A81, A94
A20	$[1, c_1^2, 1, 1]$	2	$[2, 2, 2, 2, 2]$	A62, A98
A21	$[1, -4c_1^2, c_2, -4c_2]$	2	$[2]$	A22, A23, A44, A54, A66, A100
A22	$[1, c_1^2, -4c_2^2, -4]$	2	$[2, 2, 2]$	A24, A35, A70, A107
A23	$[1, 2c_1^2, -8c_2^2, -4]$	2	$[2, 2]$	A83, A103
A24	$[1, c_1^2, -4, -4]$	2	$[4, 2, 2, 2]$	A71, A108
A25	$[1, c_1^2, c_2, 4c_2]$	3	$[2, 2]$	A26, A27, A28, A29, A40, A51, A59, A89
A26	$[1, c_1^2, c_2^2, 4]$	3	$[2, 2, 2, 2]$	A30, A63, A97
A27	$[1, -4c_1^2, -4c_2^2, 4]$	3	$[2, 2]$	A35, A72, A106
A28	$[1, 2c_1^2, 2c_2^2, 4]$	3	$[2, 2]$	A78, A92
A29	$[1, -8c_1^2, -8c_2^2, 4]$	3	$[2, 2]$	A81, A95
A30	$[1, c_1^2, 1, 4]$	4	$[2, 2, 2]$	A64, A98
A31	$[1, -4c_1^2, c_2, -c_2]$	3	$[2]$	A32, A33, A45, A54, A67, A101
A32	$[1, c_1^2, -4c_2^2, -1]$	3	$[2, 2, 2]$	A34, A35, A73, A107
A33	$[1, 2c_1^2, -8c_2^2, -1]$	3	$[2]$	A83, A104
A34	$[1, -4c_1^2, 1, -1]$	4	$[2, 2, 2]$	A74, A108
A35	$[1, c_1^2, -4, -1]$	4	$[2, 2]$	A75, A108
A36	$[1, c_1, c_2, c_2^3c_1]$	3	$[]$	A38, A43, A48, A49, A57, A65, A85, A86
A37	$[1, c_1, c_2, 4c_2^3c_1]$	2	$[2]$	A48, A49, A50, A53, A76, A79, A87, A99

Number	Example	ρ	Br_1	Subcases
A38	$[1, c_1, c_2^2c_1^3, c_2^2c_1^2]$	4	$[2]$	A39, A40, A41, A42, A60, A68, A90, A93
A39	$[1, 1, c_2, c_2]$	4	$[2]$	A61, A69, A91, A94
A40	$[1, 4, c_2, 4c_2]$	6	$[]$	A63, A72, A92, A95
A41	$[1, c_1^2, c_2^2c_1^3, c_2^2c_1]$	4	$[2]$	A61, A69, A92, A95
A42	$[1, c_1^2, 2c_2^2c_1^3, 2c_2^2c_1]$	4	$[2, 2]$	A63, A72, A91, A94
A43	$[1, c_1, -4c_2^2c_1^3, -4c_2^2c_1^2]$	4	$[]$	A44, A45, A46, A47, A68, A102
A44	$[1, -4, c_2, -4c_2]$	4	$[]$	A70, A103
A45	$[1, -1, c_2, -c_2]$	6	$[]$	A73, A104
A46	$[1, -4c_1^2, c_2^2c_1^3, -4c_2^2c_1]$	4	$[]$	A70, A104
A47	$[1, -4c_1^2, 2c_2^2c_1^3, -8c_2^2c_1]$	4	$[2]$	A73, A103
A48	$[1, c_1, 2c_2^2c_1^3, 8c_2^2c_1^2]$	3	$[]$	A77, A82, A90, A102
A49	$[1, c_1, -8c_2^2c_1^3, -2c_2^2c_1^2]$	3	$[]$	A80, A82, A93, A102
A50	$[1, c_1, c_2^2c_1^3, 4c_2^2c_1^2]$	2	$[2, 2, 2]$	A51, A52, A77, A80, A96, A105
A51	$[1, 1, c_2, 4c_2]$	3	$[2, 2]$	A78, A81, A97, A106
A52	$[1, c_1^2, c_2^2c_1^3, 4c_2^2c_1]$	2	$[2, 2, 2]$	A78, A81, A97, A106
A53	$[1, c_1, -4c_2^2c_1^3, -c_2^2c_1^2]$	2	$[2]$	A54, A55, A82, A105
A54	$[1, -4, c_2, -c_2]$	3	$[2]$	A83, A107
A55	$[1, -4c_1^2, c_2^2c_1^3, -c_2^2c_1]$	2	$[2, 2]$	A83, A107
A56	$[1, c_1, c_2, c_2^3c_1^3]$	2	$[4]$	A57, A65, A76, A79
A57	$[1, c_1^2, c_2, c_2^3c_1^2]$	3	$[2, 2]$	A58, A59, A60, A68, A77, A80
A58	$[1, 1, c_2, c_2^3]$	3	$[2, 2]$	A61, A69, A78, A81
A59	$[1, 4, c_2, 4c_2^3]$	4	$[2]$	A63, A72, A78, A81
A60	$[1, c_1^2, c_2^2, c_2^2c_1^2]$	5	$[2, 2]$	A61, A63

Number	Example	ρ	Br_1	Subcases
A61	$[1, 1, c_2^2, c_2^2]$	5	$[2, 2, 2]$	A62, A64
A62	$[1, 1, 1, 1]$	5	$[2, 2, 2, 2]$	
A63	$[1, 4, c_2^2, 4c_2^2]$	7	$[2]$	A64
A64	$[1, 1, 4, 4]$	9	$[]$	
A65	$[1, -4c_1^2, c_2, -4c_2^3c_1^2]$	3	$[2]$	A66, A67, A68, A82
A66	$[1, -4, c_2, -4c_2^3]$	3	$[2]$	A70, A83
A67	$[1, -1, c_2, -c_2^3]$	4	$[2]$	A73, A83
A68	$[1, c_1^2, -4c_2^2, -4c_2^2c_1^2]$	5	$[2]$	A69, A70, A72, A73
A69	$[1, 1, -4c_2^2, -4c_2^2]$	5	$[2, 2]$	A71, A74
A70	$[1, -4, c_2^2, -4c_2^2]$	5	$[2]$	A71, A75
A71	$[1, 1, -4, -4]$	5	$[4, 2]$	
A72	$[1, 4, -4c_2^2, -c_2^2]$	7	$[]$	A75
A73	$[1, -1, c_2^2, -c_2^2]$	7	$[2]$	A74, A75
A74	$[1, 1, -1, -1]$	9	$[2]$	
A75	$[1, -4, 4, -1]$	9	$[]$	
A76	$[1, 2c_1^2, c_2, 8c_2^3c_1^2]$	2	$[8]$	A77, A82
A77	$[1, c_1^2, 2c_2^2, 8c_2^2c_1^2]$	3	$[4, 2]$	A78
A78	$[1, 1, 2c_2^2, 8c_2^2]$	4	$[4]$	
A79	$[1, -8c_1^2, c_2, -2c_2^3c_1^2]$	2	$[8]$	A80, A82
A80	$[1, c_1^2, -8c_2^2, -2c_2^2c_1^2]$	3	$[4, 2]$	A81
A81	$[1, 1, -8c_2^2, -2c_2^2]$	4	$[4]$	
A82	$[1, -4c_1^2, 2c_2^2, -2c_2^2c_1^2]$	3	$[4]$	A83
A83	$[1, -4, 2c_2^2, -2c_2^2]$	4	$[4]$	
A84	$[1, c_1, c_2, 4c_2^3c_1^3]$	2	$[2]$	A85, A86, A87, A99
A85	$[1, 2c_1^2, c_2, 2c_2^3c_1^2]$	3	$[]$	A90, A102
A86	$[1, -8c_1^2, c_2, -8c_2^3c_1^2]$	3	$[]$	A93, A102
A87	$[1, c_1^2, c_2, 4c_2^3c_1^2]$	2	$[2, 2, 2]$	A88, A89, A90, A93, A96, A105
A88	$[1, 1, c_2, 4c_2^3]$	2	$[2, 2, 2]$	A91, A94, A97, A106
A89	$[1, 4, c_2, c_2^3]$	3	$[2, 2]$	A92, A95, A97, A106

Number	Example	ρ	Br_1	Subcases
A90	$[1, c_1^2, 2c_2^2, 2c_2^2c_1^2]$	4	$[2]$	A91, A92
A91	$[1, 1, 2c_2^2, 2c_2^2]$	4	$[2, 2]$	
A92	$[1, 4, 2c_2^2, 8c_2^2]$	6	$[]$	
A93	$[1, c_1^2, -8c_2^2, -8c_2^2c_1^2]$	4	$[2]$	A94, A95
A94	$[1, 1, -8c_2^2, -8c_2^2]$	4	$[2, 2]$	
A95	$[1, 4, -8c_2^2, -2c_2^2]$	6	$[]$	
A96	$[1, c_1^2, c_2^2, 4c_2^2c_1^2]$	2	$[2, 2, 2, 2, 2]$	A97
A97	$[1, 1, c_2^2, 4c_2^2]$	3	$[2, 2, 2, 2]$	A98
A98	$[1, 1, 1, 4]$	5	$[2, 2]$	
A99	$[1, -4c_1^2, c_2, -c_2^3c_1^2]$	2	$[2]$	A100, A101, A102, A105
A100	$[1, -4, c_2, -c_2^3]$	2	$[2, 2]$	A103, A107
A101	$[1, -1, c_2, -4c_2^3]$	3	$[2]$	A104, A107
A102	$[1, -4c_1^2, 2c_2^2, -8c_2^2c_1^2]$	4	$[]$	A103, A104
A103	$[1, -4, 2c_2^2, -8c_2^2]$	4	$[2]$	
A104	$[1, -1, 2c_2^2, -2c_2^2]$	6	$[]$	
A105	$[1, c_1^2, -4c_2^2, -c_2^2c_1^2]$	2	$[2, 2, 2]$	A106, A107
A106	$[1, 1, -4c_2^2, -c_2^2]$	3	$[4, 2, 2]$	A108
A107	$[1, -4, c_2^2, -c_2^2]$	3	$[2, 2, 2]$	A108
A108	$[1, 1, -4, -1]$	5	$[4, 2]$	
	$2a_0a_1a_2a_3$ square			
A109	$[1, c_1, c_2, 2c_3^2c_2^3c_1^3]$	1	$[2]$	A110, A112
A110	$[1, c_1^2, c_2, 2c_3^2c_2^3]$	1	$[2, 2]$	A111, A113, A114, A116, A121
A111	$[1, c_1^2, c_2^2, 2c_3^2]$	1	$[2, 2, 2]$	A117, A122
A112	$[1, -4c_1^2, c_2, -8c_3^2c_2^3]$	1	$[2]$	A113, A115, A119, A127
A113	$[1, c_1^2, -4c_2^2, -8c_3^2]$	1	$[2, 2]$	A118, A120, A123, A128
A114	$[1, 2c_1^2, c_2, 4c_2]$	1	$[4, 2]$	A117, A118
A115	$[1, -8c_1^2, c_2, -c_2]$	1	$[4]$	A120

Number	Example	ρ	Br_1	Subcases
A116	$[1, c_1, 2c_2^2c_1^3, c_1^2]$	1	$[2, 2]$	A117, A118, A122, A123
A117	$[1, c_1^2, 2c_2^2, 4]$	1	$[4, 2, 2]$	A124
A118	$[1, -4c_1^2, -8c_2^2, 4]$	1	$[4, 2, 2]$	A129
A119	$[1, c_1, -8c_2^2c_1^3, -4c_1^2]$	1	$[4]$	A120, A128
A120	$[1, c_1^2, -8c_2^2, -1]$	1	$[4, 2]$	A125, A129
A121	$[1, 2c_1^2, c_2, c_2]$	2	$[2]$	A122, A123
A122	$[1, c_1^2, 2c_2^2, 1]$	2	$[2, 2]$	A124, A126
A123	$[1, -4c_1^2, -8c_2^2, 1]$	2	$[2, 2]$	A125, A130
A124	$[1, 2c_1^2, 1, 4]$	2	$[4, 4]$	
A125	$[1, -8c_1^2, 1, -1]$	2	$[4, 4]$	
A126	$[1, 2c_1^2, 1, 1]$	4	$[]$	
A127	$[1, -8c_1^2, c_2, -4c_2]$	2	$[]$	A128
A128	$[1, c_1^2, -8c_2^2, -4]$	2	$[2]$	A129, A130
A129	$[1, 2c_1^2, -4, -1]$	2	$[4, 2]$	
A130	$[1, 2c_1^2, -4, -4]$	4	$[]$	
		$-a_0a_1a_2a_3$ square		
A131	$[1, c_1, c_2, -4c_3^2c_2^3c_1^3]$	1	$[2]$	A132, A134, A157, A158, A170, A185
A132	$[1, c_1^2, c_2, -4c_3^2c_2^3]$	1	$[2, 2]$	A133, A135, A136, A137, A138, A139, A140, A144, A148, A152, A159, A165, A171, A187
A133	$[1, c_1^2, c_2^2, -4c_3^2]$	1	$[2, 2, 2]$	A141, A145, A149, A153, A176, A195
A134	$[1, 2c_1^2, c_2, -8c_3^2c_2^3]$	1	$[2]$	A135, A164, A181, A186
A135	$[1, c_1^2, 2c_2^2, -8c_3^2]$	1	$[2, 2]$	A142, A146, A150, A154, A182, A192

Number	Example	ρ	Br_1	Subcases
A136	$[1, c_1, c_2^2 c_1^3, -4c_1^2]$	1	$[2, 2]$	A145, A154, A162, A169, A172, A190
A137	$[1, c_1, -4c_2^2 c_1^3, c_1^2]$	1	$[2, 2]$	A141, A150, A162, A168, A173, A191
A138	$[1, c_1, c_2^2 c_1^3, -c_1^2]$	1	$[4, 2]$	A146, A153, A163, A168, A174, A188
A139	$[1, c_1, -4c_2^2 c_1^3, 4c_1^2]$	1	$[2, 2, 2]$	A142, A149, A163, A169, A175, A189
A140	$[1, -4c_1^2, c_2, c_2]$	1	$[2, 2]$	A141, A142, A160, A166, A172, A188
A141	$[1, c_1^2, -4c_2^2, 1]$	1	$[2, 2, 2, 2]$	A143, A147, A151, A155, A177, A196
A142	$[1, 2c_1^2, -8c_2^2, 1]$	1	$[2, 2, 2]$	A183, A193
A143	$[1, -4c_1^2, 1, 1]$	1	$[2, 2, 2, 2, 2]$	A178, A197
A144	$[1, c_1^2, c_2, -4c_2]$	1	$[2, 2]$	A145, A146, A160, A167, A173, A189
A145	$[1, c_1^2, c_2^2, -4]$	1	$[4, 2, 2]$	A147, A156, A177, A198
A146	$[1, 2c_1^2, 2c_2^2, -4]$	1	$[4, 2]$	A184, A193
A147	$[1, c_1^2, 1, -4]$	1	$[4, 2, 2, 2]$	A178, A199
A148	$[1, -4c_1^2, c_2, 4c_2]$	2	$[2, 2]$	A149, A150, A161, A167, A174, A190
A149	$[1, c_1^2, -4c_2^2, 4]$	2	$[2, 2, 2]$	A151, A156, A179, A198
A150	$[1, 2c_1^2, -8c_2^2, 4]$	2	$[2, 2]$	A184, A194
A151	$[1, -4c_1^2, 1, 4]$	3	$[2, 2, 2]$	A180, A199
A152	$[1, c_1^2, c_2, -c_2]$	2	$[2]$	A153, A154, A161, A166, A175, A191
A153	$[1, c_1^2, c_2^2, -1]$	2	$[2, 2]$	A155, A156, A179, A196
A154	$[1, 2c_1^2, 2c_2^2, -1]$	2	$[2]$	A183, A194
A155	$[1, c_1^2, 1, -1]$	3	$[2, 2, 2]$	A180, A197

Number	Example	ρ	Br_1	Subcases
A156	$[1, c_1^2, -4, 4]$	3	$[2, 2]$	A180, A199
A157	$[1, c_1, c_2, -4c_2^3c_1]$	2	$[]$	A159, A164, A171, A186
A158	$[1, c_1, c_2, -c_2^3c_1]$	1	$[2]$	A164, A165, A181, A187
A159	$[1, c_1, c_2^2c_1^3, -4c_2^2c_1^2]$	3	$[]$	A160, A161, A162, A163, A176, A192
A160	$[1, 1, c_2, -4c_2]$	3	$[]$	A177, A193
A161	$[1, 4, c_2, -c_2]$	5	$[]$	A179, A194
A162	$[1, c_1^2, -4c_2^2c_1^3, c_2^2c_1]$	3	$[]$	A177, A194
A163	$[1, c_1^2, -8c_2^2c_1^3, 2c_2^2c_1]$	3	$[2]$	A179, A193
A164	$[1, c_1, 2c_2^2c_1^3, -2c_2^2c_1^2]$	2	$[]$	A182, A192
A165	$[1, c_1, c_2^2c_1^3, -c_2^2c_1^2]$	1	$[2, 2]$	A166, A167, A168, A169, A182, A195
A166	$[1, 1, c_2, -c_2]$	2	$[2]$	A183, A196
A167	$[1, -4, c_2, 4c_2]$	2	$[2, 2]$	A184, A198
A168	$[1, c_1^2, -4c_2^2c_1^3, 4c_2^2c_1]$	1	$[4, 2]$	A184, A196
A169	$[1, -4c_1^2, -4c_2^2c_1^3, -c_2^2c_1]$	1	$[2, 2, 2]$	A183, A198
A170	$[1, c_1, c_2, -4c_2^3c_1^3]$	1	$[4]$	A171, A181
A171	$[1, c_1^2, c_2, -4c_2^3c_1^2]$	2	$[2]$	A172, A173, A174, A175, A176, A182
A172	$[1, 1, c_2, -4c_2^3]$	2	$[4]$	A177, A183
A173	$[1, -4, c_2, c_2^3]$	2	$[4]$	A177, A184
A174	$[1, 4, c_2, -c_2^3]$	3	$[2]$	A179, A184
A175	$[1, -1, c_2, 4c_2^3]$	3	$[2]$	A179, A183
A176	$[1, c_1^2, c_2^2, -4c_2^2c_1^2]$	4	$[]$	A177, A179
A177	$[1, 1, c_2^2, -4c_2^2]$	4	$[2]$	A178, A180
A178	$[1, 1, 1, -4]$	4	$[2, 2]$	
A179	$[1, 4, c_2^2, -c_2^2]$	6	$[]$	A180
A180	$[1, 1, 4, -1]$	8	$[]$	
A181	$[1, 2c_1^2, c_2, -2c_2^3c_1^2]$	1	$[8]$	A182
A182	$[1, c_1^2, 2c_2^2, -2c_2^2c_1^2]$	2	$[4]$	A183, A184

Number	Example	ρ	Br_1	Subcases
A183	$[1, 1, 2c_2^2, -2c_2^2]$	3	$[4]$	
A184	$[1, -4, 2c_2^2, 8c_2^2]$	3	$[2, 2]$	
A185	$[1, c_1, c_2, -c_2^3c_1^3]$	1	$[2]$	A186, A187
A186	$[1, 2c_1^2, c_2, -8c_2^3c_1^2]$	2	$[]$	A192
A187	$[1, c_1^2, c_2, -c_2^3c_1^2]$	1	$[2, 2]$	A188, A189, A190, A191, A192, A195
A188	$[1, 1, c_2, -c_2^3]$	1	$[4, 2]$	A193, A196
A189	$[1, -4, c_2, 4c_2^3]$	1	$[2, 2, 2]$	A193, A198
A190	$[1, 4, c_2, -4c_2^3]$	2	$[2, 2]$	A194, A198
A191	$[1, -1, c_2, c_2^3]$	2	$[2]$	A194, A196
A192	$[1, c_1^2, 2c_2^2, -8c_2^2c_1^2]$	3	$[]$	A193, A194
A193	$[1, 1, 2c_2^2, -8c_2^2]$	3	$[2]$	
A194	$[1, 4, 2c_2^2, -2c_2^2]$	5	$[]$	
A195	$[1, c_1^2, c_2^2, -c_2^2c_1^2]$	1	$[4, 2, 2]$	A196, A198
A196	$[1, 1, c_2^2, -c_2^2]$	2	$[2, 2, 2]$	A197, A199
A197	$[1, 1, 1, -1]$	4	$[2, 2, 2, 2]$	
A198	$[1, -4, c_2^2, 4c_2^2]$	2	$[4, 2, 2]$	A199
A199	$[1, 1, -4, 4]$	4	$[2, 2]$	

$-2a_0a_1a_2a_3$ square

A200	$[1, c_1, c_2, -8c_3^2c_2^3c_1^3]$	1	$[2]$	A201, A203
A201	$[1, c_1^2, c_2, -8c_3^2c_2^3]$	1	$[2, 2]$	A202, A204, A206, A209, A212
A202	$[1, c_1^2, c_2^2, -8c_3^2]$	1	$[2, 2, 2]$	A210, A213
A203	$[1, -4c_1^2, c_2, 2c_3^2c_2^3]$	1	$[2]$	A204, A205, A207, A218
A204	$[1, c_1^2, -4c_2^2, 2c_3^2]$	1	$[2, 2]$	A208, A211, A214, A219
A205	$[1, 2c_1^2, c_2, -c_2]$	1	$[4]$	A208
A206	$[1, -8c_1^2, c_2, 4c_2]$	1	$[4, 2]$	A210, A211
A207	$[1, c_1, 2c_2^2c_1^3, -4c_1^2]$	1	$[4]$	A208, A219
A208	$[1, c_1^2, 2c_2^2, -1]$	1	$[4, 2]$	A216, A220

Number	Example	ρ	Br_1	Subcases
A209	$[1, c_1, -8c_2^2c_1^3, c_1^2]$	1	$[2, 2]$	A210, A211, A213, A214
A210	$[1, c_1^2, -8c_2^2, 4]$	1	$[4, 2, 2]$	A215
A211	$[1, -4c_1^2, 2c_2^2, 4]$	1	$[4, 2, 2]$	A220
A212	$[1, -8c_1^2, c_2, c_2]$	2	$[2]$	A213, A214
A213	$[1, c_1^2, -8c_2^2, 1]$	2	$[2, 2]$	A215, A217
A214	$[1, -4c_1^2, 2c_2^2, 1]$	2	$[2, 2]$	A216, A221
A215	$[1, -8c_1^2, 1, 4]$	2	$[4, 2, 2]$	
A216	$[1, 2c_1^2, 1, -1]$	2	$[4, 4]$	
A217	$[1, -8c_1^2, 1, 1]$	4	$[2]$	
A218	$[1, 2c_1^2, c_2, -4c_2]$	2	$[]$	A219
A219	$[1, c_1^2, 2c_2^2, -4]$	2	$[2]$	A220, A221
A220	$[1, 2c_1^2, -4, 4]$	2	$[4, 2]$	
A221	$[1, 2c_1^2, 1, -4]$	4	$[]$	
		Other cases		
A222	$[1, c_1, c_2, c_3]$	1	$[2]$	A1, A109, A131, A200, A223, A224, A225, A226
A223	$[1, c_1, c_2, c_3^2]$	1	$[2, 2]$	A2, A110, A132, A201, A227, A229, A231, A232, A233, A234, A236, A244, A257, A268
A224	$[1, c_1, c_2, -4c_3^2]$	1	$[2]$	A4, A112, A132, A203, A228, A230, A232, A235, A241, A249, A263, A276
A225	$[1, c_1, c_2, 2c_3^2]$	1	$[2]$	A6, A110, A134, A203, A233, A235
A226	$[1, c_1, c_2, -8c_3^2]$	1	$[2]$	A8, A112, A134, A201, A234, A235

Number	Example	ρ	Br_1	Subcases
A227	$[1, c_1, c_2, 1]$	1	$[2, 2]$	A15, A121, A140, A212, A237, A238, A247, A248
A228	$[1, c_1, c_2, -4]$	1	$[2]$	A21, A127, A144, A218, A242, A251
A229	$[1, c_1, c_2, 4]$	1	$[4, 2]$	A25, A114, A148, A206, A239, A240, A245, A246
A230	$[1, c_1, c_2, -1]$	1	$[4]$	A31, A115, A152, A205, A243, A250
A231	$[1, c_1, c_2^2, c_3^2]$	1	$[2, 2, 2]$	A3, A111, A133, A202, A237, A245, A258, A269
A232	$[1, c_1, c_2^2, -4c_3^2]$	1	$[2, 2]$	A5, A113, A133, A204, A238, A242, A246, A250, A259, A264, A270, A277
A233	$[1, c_1, c_2^2, 2c_3^2]$	1	$[2, 2]$	A7, A111, A135, A204, A239, A247, A260, A271
A234	$[1, c_1, c_2^2, -8c_3^2]$	1	$[2, 2]$	A9, A113, A135, A202, A240, A248, A261, A272
A235	$[1, c_1, -4c_2^2, 2c_3^2]$	1	$[2]$	A10, A113, A135, A204, A243, A251, A265, A278
A236	$[1, c_1, c_2, c_2^2]$	1	$[2, 2]$	A11, A116, A137, A209, A237, A238, A239, A240, A258, A259, A271, A272

Number	Example	ρ	Br_1	Subcases
A237	$[1, c_1, c_2^2, 1]$	1	$[2, 2, 2]$	A16, A122, A141, A213, A252, A254, A262, A275
A238	$[1, c_1, -4c_2^2, 1]$	1	$[2, 2, 2]$	A17, A123, A141, A214, A253, A255, A266, A281
A239	$[1, c_1, 2c_2^2, 4]$	1	$[4, 2]$	A28, A117, A150, A211
A240	$[1, c_1, -8c_2^2, 4]$	1	$[4, 2]$	A29, A118, A150, A210
A241	$[1, c_1, c_2, -4c_2^2]$	1	$[2]$	A12, A119, A136, A207, A242, A243, A264, A278
A242	$[1, c_1, c_2^2, -4]$	1	$[2, 2]$	A22, A128, A145, A219, A253, A256, A267, A282
A243	$[1, c_1, 2c_2^2, -1]$	1	$[4]$	A33, A120, A154, A208
A244	$[1, c_1, c_2, 4c_2^2]$	1	$[2, 2]$	A13, A116, A139, A209, A245, A246, A247, A248, A260, A261, A269, A270
A245	$[1, c_1, c_2^2, 4]$	1	$[4, 2, 2]$	A26, A117, A149, A210, A254, A273
A246	$[1, c_1, -4c_2^2, 4]$	1	$[4, 2]$	A27, A118, A149, A211, A256, A279
A247	$[1, c_1, 2c_2^2, 1]$	1	$[2, 2]$	A18, A122, A142, A214
A248	$[1, c_1, -8c_2^2, 1]$	1	$[2, 2]$	A19, A123, A142, A213

Number	Example	ρ	Br_1	Subcases
A249	$[1, c_1, c_2, -c_2^2]$	1	$[4]$	A14, A119, A138, A207, A250, A251, A265, A277
A250	$[1, c_1, c_2^2, -1]$	1	$[4, 2]$	A32, A120, A153, A208, A255, A256, A274, A280
A251	$[1, c_1, 2c_2^2, -4]$	1	$[4]$	A23, A128, A146, A219
A252	$[1, c_1, 1, 1]$	1	$[2, 2, 2]$	A20, A126, A143, A217
A253	$[1, c_1, 1, -4]$	1	$[2, 2, 2]$	A24, A130, A147, A221
A254	$[1, c_1, 1, 4]$	1	$[4, 4, 2]$	A30, A124, A151, A215
A255	$[1, c_1, 1, -1]$	1	$[4, 2, 2]$	A34, A125, A155, A216
A256	$[1, c_1, -4, 4]$	1	$[4, 4]$	A35, A129, A156, A220
A257	$[1, c_1, c_2, c_2^2 c_1^2]$	1	$[2, 2]$	A15, A114, A140, A206, A258, A259, A260, A261
A258	$[1, c_1^2, c_2, c_2^2]$	1	$[2, 2, 2]$	A16, A117, A141, A210, A262, A273
A259	$[1, -4c_1^2, c_2, c_2^2]$	1	$[2, 2, 2]$	A17, A118, A141, A211, A267, A280
A260	$[1, 2c_1^2, c_2, 4c_2^2]$	1	$[2, 2]$	A18, A117, A142, A211
A261	$[1, -8c_1^2, c_2, 4c_2^2]$	1	$[2, 2]$	A19, A118, A142, A210
A262	$[1, c_1, 1, c_1^2]$	1	$[2, 2, 2]$	A20, A124, A143, A215

Number	Example	ρ	Br_1	Subcases
A263	$[1, c_1, c_2, -4c_2^2c_1^2]$	1	$[2]$	A21, A115, A144, A205, A264, A265
A264	$[1, c_1^2, c_2, -4c_2^2]$	1	$[2, 2]$	A22, A120, A145, A208, A266, A267, A274, A279
A265	$[1, 2c_1^2, c_2, -c_2^2]$	1	$[4]$	A23, A120, A146, A208
A266	$[1, c_1, 1, -4c_1^2]$	1	$[2, 2, 2]$	A24, A125, A147, A216
A267	$[1, c_1, -4, c_1^2]$	1	$[2, 2, 2]$	A24, A129, A147, A220
A268	$[1, c_1, c_2, 4c_2^2c_1^2]$	2	$[2]$	A25, A121, A148, A212, A269, A270, A271, A272
A269	$[1, c_1^2, c_2, 4c_2^2]$	2	$[2, 2]$	A26, A122, A149, A213, A273, A275
A270	$[1, -4c_1^2, c_2, 4c_2^2]$	2	$[2]$	A27, A123, A149, A214, A274, A282
A271	$[1, 2c_1^2, c_2, c_2^2]$	2	$[2]$	A28, A122, A150, A214
A272	$[1, -8c_1^2, c_2, c_2^2]$	2	$[2]$	A29, A123, A150, A213
A273	$[1, c_1, 4, c_1^2]$	2	$[4, 2]$	A30, A124, A151, A215
A274	$[1, c_1, -1, -4c_1^2]$	2	$[4]$	A35, A125, A156, A216
A275	$[1, c_1, 1, 4c_1^2]$	3	$[2]$	A30, A126, A151, A217
A276	$[1, c_1, c_2, -c_2^2c_1^2]$	2	$[]$	A31, A127, A152, A218, A277, A278

Number	Example	ρ	Br_1	Subcases
A277	$[1, c_1^2, c_2, -c_2^2]$	2	$[2]$	A32, A128, A153, A219, A279, A280, A281, A282
A278	$[1, 2c_1^2, c_2, -4c_2^2]$	2	$[]$	A33, A128, A154, A219
A279	$[1, c_1, 4, -4c_1^2]$	2	$[4]$	A35, A129, A156, A220
A280	$[1, c_1, -1, c_1^2]$	2	$[2, 2]$	A34, A129, A155, A220
A281	$[1, c_1, 1, -c_1^2]$	3	$[2]$	A34, A130, A155, A221
A282	$[1, c_1, -4, 4c_1^2]$	3	$[]$	A35, A130, A156, A221

A.2 $k \cap \mathbb{Q}(\epsilon) = \mathbb{Q}(i)$

Number	Example	ρ	Br_1	Subcases
		$a_0a_1a_2a_3$ square		
B1	$[1, c_1, c_2, c_3^2c_2^3c_1^3]$	2	$[2]$	B2, B4, B16, B17, B27, B39
B2	$[1, c_1^2, c_2, c_3^2c_2^3]$	2	$[2, 2, 2]$	B3, B5, B6, B7, B8, B12, B18, B24, B28, B41
B3	$[1, c_1^2, c_2^2, c_3^2]$	2	$[2, 2, 2, 2, 2]$	B9, B13, B31, B47
B4	$[1, 2c_1^2, c_2, 2c_3^2c_2^3]$	2	$[2]$	B5, B23, B36, B40
B5	$[1, c_1^2, 2c_2^2, 2c_3^2]$	2	$[2, 2, 2]$	B10, B14, B37, B44
B6	$[1, c_1, c_2^2c_1^3, c_1^2]$	2	$[2, 2, 2]$	B9, B14, B21, B26, B29, B43
B7	$[1, c_1, c_2^2c_1^3, 4c_1^2]$	2	$[2, 2, 2, 2]$	B10, B13, B22, B26, B30, B42

Number	Example	ρ	Br_1	Subcases
B8	$[1, c_1^2, c_2, c_2]$	2	$[2, 2, 2]$	B9, B10, B19, B25, B29, B42
B9	$[1, c_1^2, c_2^2, 1]$	2	$[4, 2, 2, 2, 2, 2]$	B11, B15, B32, B48
B10	$[1, 2c_1^2, 2c_2^2, 1]$	2	$[2, 2, 2, 2]$	B38, B45
B11	$[1, c_1^2, 1, 1]$	2	$[4, 4, 2, 2, 2, 2, 2]$	B33, B49
B12	$[1, c_1^2, c_2, 4c_2]$	4	$[2, 2]$	B13, B14, B20, B25, B30, B43
B13	$[1, c_1^2, c_2^2, 4]$	4	$[2, 2, 2, 2]$	B15, B34, B48
B14	$[1, 2c_1^2, 2c_2^2, 4]$	4	$[2, 2]$	B38, B46
B15	$[1, c_1^2, 1, 4]$	6	$[2, 2, 2, 2]$	B35, B49
B16	$[1, c_1, c_2, c_2^3c_1]$	4	$[]$	B18, B23, B28, B40
B17	$[1, c_1, c_2, 4c_2^3c_1]$	2	$[2]$	B23, B24, B36, B41
B18	$[1, c_1, c_2^2c_1^3, c_2^2c_1^2]$	6	$[]$	B19, B20, B21, B22, B31, B44
B19	$[1, 1, c_2, c_2]$	6	$[]$	B32, B45
B20	$[1, 4, c_2, 4c_2]$	10	$[]$	B34, B46
B21	$[1, c_1^2, c_2^2c_1^3, c_2^2c_1]$	6	$[]$	B32, B46
B22	$[1, c_1^2, 2c_2^2c_1^3, 2c_2^2c_1]$	6	$[2, 2]$	B34, B45
B23	$[1, c_1, 2c_2^2c_1^3, 8c_2^2c_1^2]$	4	$[]$	B37, B44
B24	$[1, c_1, c_2^2c_1^3, 4c_2^2c_1^2]$	2	$[2, 2, 2]$	B25, B26, B37, B47
B25	$[1, 1, c_2, 4c_2]$	4	$[2, 2]$	B38, B48
B26	$[1, c_1^2, c_2^2c_1^3, 4c_2^2c_1]$	2	$[2, 2, 2, 2]$	B38, B48
B27	$[1, c_1, c_2, c_2^3c_1^3]$	2	$[4, 2]$	B28, B36
B28	$[1, c_1^2, c_2, c_2^3c_1^2]$	4	$[2, 2]$	B29, B30, B31, B37
B29	$[1, 1, c_2, c_2^3]$	4	$[4, 2]$	B32, B38
B30	$[1, 4, c_2, 4c_2^3]$	6	$[2]$	B34, B38
B31	$[1, c_1^2, c_2^2, c_2^2c_1^2]$	8	$[]$	B32, B34
B32	$[1, 1, c_2^2, c_2^2]$	8	$[2, 2]$	B33, B35
B33	$[1, 1, 1, 1]$	8	$[2, 2, 2, 2]$	
B34	$[1, 4, c_2^2, 4c_2^2]$	12	$[]$	B35
B35	$[1, 1, 4, 4]$	16	$[]$	
B36	$[1, 2c_1^2, c_2, 8c_2^3c_1^2]$	2	$[8, 4]$	B37

Number	Example	ρ	Br_1	Subcases
B37	$[1, c_1^2, 2c_2^2, 8c_2^2c_1^2]$	4	$[4, 4]$	B38
B38	$[1, 1, 2c_2^2, 8c_2^2]$	6	$[4, 2]$	
B39	$[1, c_1, c_2, 4c_2^3c_1^3]$	2	$[2]$	B40, B41
B40	$[1, 2c_1^2, c_2, 2c_2^3c_1^2]$	4	$[]$	B44
B41	$[1, c_1^2, c_2, 4c_2^3c_1^2]$	2	$[2, 2, 2]$	B42, B43, B44, B47
B42	$[1, 1, c_2, 4c_2^3]$	2	$[2, 2, 2, 2]$	B45, B48
B43	$[1, 4, c_2, c_2^3]$	4	$[2, 2]$	B46, B48
B44	$[1, c_1^2, 2c_2^2, 2c_2^2c_1^2]$	6	$[]$	B45, B46
B45	$[1, 1, 2c_2^2, 2c_2^2]$	6	$[2, 2]$	
B46	$[1, 4, 2c_2^2, 8c_2^2]$	10	$[]$	
B47	$[1, c_1^2, c_2^2, 4c_2^2c_1^2]$	2	$[2, 2, 2, 2, 2, 2]$	B48
B48	$[1, 1, c_2^2, 4c_2^2]$	4	$[4, 2, 2, 2, 2]$	B49
B49	$[1, 1, 1, 4]$	8	$[2, 2, 2, 2]$	
		$2a_0a_1a_2a_3$ square		
B50	$[1, c_1, c_2, 2c_3^2c_2^3c_1^3]$	1	$[2]$	B51
B51	$[1, c_1^2, c_2, 2c_3^2c_2^3]$	1	$[2, 2]$	B52, B53, B54, B56
B52	$[1, c_1^2, c_2^2, 2c_3^2]$	1	$[4, 2, 2]$	B55, B57
B53	$[1, 2c_1^2, c_2, 4c_2]$	1	$[4, 4]$	B55
B54	$[1, c_1, 2c_2^2c_1^3, c_1^2]$	1	$[4, 2]$	B55, B57
B55	$[1, c_1^2, 2c_2^2, 4]$	1	$[4, 4, 2, 2]$	B58
B56	$[1, 2c_1^2, c_2, c_2]$	3	$[]$	B57
B57	$[1, c_1^2, 2c_2^2, 1]$	3	$[2, 2]$	B58, B59
B58	$[1, 2c_1^2, 1, 4]$	3	$[4, 4, 2, 2]$	
B59	$[1, 2c_1^2, 1, 1]$	7	$[]$	
		Other cases		
B60	$[1, c_1, c_2, c_3]$	1	$[2]$	B1, B50, B61, B62
B61	$[1, c_1, c_2, c_3^2]$	1	$[2, 2]$	B2, B51, B63, B64, B65, B66, B67, B70, B75, B79
B62	$[1, c_1, c_2, 2c_3^2]$	1	$[2]$	B4, B51, B66

Number	Example	ρ	Br_1	Subcases
B63	$[1, c_1, c_2, 1]$	1	$[2, 2]$	B8, B56, B68, B72
B64	$[1, c_1, c_2, 4]$	1	$[4, 4]$	B12, B53, B69, B71
B65	$[1, c_1, c_2^2, c_3^2]$	1	$[2, 2, 2]$	B3, B52, B68, B71, B76, B80
B66	$[1, c_1, c_2^2, 2c_3^2]$	1	$[2, 2]$	B5, B52, B69, B72, B77, B81
B67	$[1, c_1, c_2, c_2^2]$	1	$[2, 2]$	B6, B54, B68, B69, B76, B81
B68	$[1, c_1, c_2^2, 1]$	1	$[2, 2, 2, 2]$	B9, B57, B73, B74, B78, B83
B69	$[1, c_1, 2c_2^2, 4]$	1	$[4, 4]$	B14, B55
B70	$[1, c_1, c_2, 4c_2^2]$	1	$[4, 2]$	B7, B54, B71, B72, B77, B80
B71	$[1, c_1, c_2^2, 4]$	1	$[4, 4, 2]$	B13, B55, B74, B82
B72	$[1, c_1, 2c_2^2, 1]$	1	$[4, 2]$	B10, B57
B73	$[1, c_1, 1, 1]$	1	$[2, 2, 2, 2, 2]$	B11, B59
B74	$[1, c_1, 1, 4]$	1	$[4, 4, 4, 4]$	B15, B58
B75	$[1, c_1, c_2, c_2^2c_1^2]$	1	$[2, 2]$	B8, B53, B76, B77
B76	$[1, c_1^2, c_2, c_2^2]$	1	$[2, 2, 2, 2]$	B9, B55, B78, B82
B77	$[1, 2c_1^2, c_2, 4c_2^2]$	1	$[4, 2]$	B10, B55
B78	$[1, c_1, 1, c_1^2]$	1	$[2, 2, 2, 2, 2]$	B11, B58
B79	$[1, c_1, c_2, 4c_2^2c_1^2]$	3	$[]$	B12, B56, B80, B81
B80	$[1, c_1^2, c_2, 4c_2^2]$	3	$[2]$	B13, B57, B82, B83
B81	$[1, 2c_1^2, c_2, c_2^2]$	3	$[]$	B14, B57
B82	$[1, c_1, 4, c_1^2]$	3	$[4, 2]$	B15, B58
B83	$[1, c_1, 1, 4c_1^2]$	5	$[]$	B15, B59

A.3 $k \cap \mathbb{Q}(\epsilon) = \mathbb{Q}(\sqrt{2})$

Number	Example	ρ	Br_1	Subcases
		$a_0a_1a_2a_3$ square		

Number	Example	ρ	Br_1	Subcases
C1	$[1, c_1, c_2, c_3^2c_2^3c_1^3]$	2	$[2]$	C2, C4, C15, C22
C2	$[1, c_1^2, c_2, c_3^2c_2^3]$	2	$[2, 2, 2]$	C3, C5, C6, C8, C16, C23
C3	$[1, c_1^2, c_2^2, c_3^2]$	2	$[2, 2, 2, 2, 2]$	C9, C25
C4	$[1, -4c_1^2, c_2, -4c_3^2c_2^3]$	2	$[2]$	C5, C7, C12, C19, C28
C5	$[1, c_1^2, -4c_2^2, -4c_3^2]$	2	$[2, 2, 2]$	C10, C13, C30
C6	$[1, c_1, c_2^2c_1^3, c_1^2]$	2	$[2, 2, 2]$	C9, C10, C18, C24
C7	$[1, c_1, -4c_2^2c_1^3, -4c_1^2]$	2	$[2, 2]$	C13, C21, C29
C8	$[1, c_1^2, c_2, c_2]$	3	$[2, 2]$	C9, C10, C17, C24
C9	$[1, c_1^2, c_2^2, 1]$	3	$[2, 2, 2, 2]$	C11, C26
C10	$[1, -4c_1^2, -4c_2^2, 1]$	3	$[2, 2, 2, 2]$	C14, C31
C11	$[1, c_1^2, 1, 1]$	5	$[2, 2, 2]$	C27
C12	$[1, -4c_1^2, c_2, -4c_2]$	3	$[2]$	C13, C20, C29
C13	$[1, c_1^2, -4c_2^2, -4]$	3	$[2, 2, 2]$	C14, C32
C14	$[1, c_1^2, -4, -4]$	5	$[2, 2, 2]$	C33
C15	$[1, c_1, c_2, c_2^3c_1]$	3	$[]$	C16, C19, C23, C28
C16	$[1, c_1, c_2^2c_1^3, c_2^2c_1^2]$	4	$[2]$	C17, C18, C25, C30
C17	$[1, 1, c_2, c_2]$	6	$[]$	C26, C31
C18	$[1, c_1^2, c_2^2c_1^3, c_2^2c_1]$	4	$[2, 2]$	C26, C31
C19	$[1, c_1, -4c_2^2c_1^3, -4c_2^2c_1^2]$	4	$[]$	C20, C21, C30
C20	$[1, -4, c_2, -4c_2]$	6	$[]$	C32
C21	$[1, -4c_1^2, c_2^2c_1^3, -4c_2^2c_1]$	4	$[2]$	C32
C22	$[1, c_1, c_2, c_2^3c_1^3]$	2	$[8]$	C23, C28
C23	$[1, c_1^2, c_2, c_2^3c_1^2]$	3	$[4, 2]$	C24, C25, C30
C24	$[1, 1, c_2, c_2^3]$	4	$[4]$	C26, C31
C25	$[1, c_1^2, c_2^2, c_2^2c_1^2]$	5	$[2, 2, 2]$	C26
C26	$[1, 1, c_2^2, c_2^2]$	7	$[2, 2]$	C27
C27	$[1, 1, 1, 1]$	11	$[]$	
C28	$[1, -4c_1^2, c_2, -4c_2^3c_1^2]$	3	$[4]$	C29, C30
C29	$[1, -4, c_2, -4c_2^3]$	4	$[4]$	C32
C30	$[1, c_1^2, -4c_2^2, -4c_2^2c_1^2]$	5	$[4]$	C31, C32

Number	Example	ρ	Br_1	Subcases
C31	$[1,1,-4c_2^2,-4c_2^2]$	7	$[2,2]$	C33
C32	$[1,-4,c_2^2,-4c_2^2]$	7	$[4]$	C33
C33	$[1,1,-4,-4]$	11	$[2]$	
		$-a_0a_1a_2a_3$ square		
C34	$[1,c_1,c_2,-4c_3^2c_2^3c_1^3]$	1	$[2]$	C35, C45, C49
C35	$[1,c_1^2,c_2,-4c_3^2c_2^3]$	1	$[2,2]$	C36, C37, C38, C39, C42, C46, C50
C36	$[1,c_1^2,c_2^2,-4c_3^2]$	1	$[2,2,2,2]$	C40, C43, C53
C37	$[1,c_1,c_2^2c_1^3,-4c_1^2]$	1	$[4,2]$	C43, C48, C51
C38	$[1,c_1,-4c_2^2c_1^3,c_1^2]$	1	$[2,2,2]$	C40, C48, C52
C39	$[1,-4c_1^2,c_2,c_2]$	2	$[2,2]$	C40, C47, C51
C40	$[1,c_1^2,-4c_2^2,1]$	2	$[2,2,2,2]$	C41, C44, C54
C41	$[1,-4c_1^2,1,1]$	4	$[2,2,2,2]$	C55
C42	$[1,c_1^2,c_2,-4c_2]$	2	$[2]$	C43, C47, C52
C43	$[1,c_1^2,c_2^2,-4]$	2	$[2,2,2]$	C44, C54
C44	$[1,c_1^2,1,-4]$	4	$[2,2,2]$	C55
C45	$[1,c_1,c_2,-4c_2^3c_1]$	2	$[]$	C46, C50
C46	$[1,c_1,c_2^2c_1^3,-4c_2^2c_1^2]$	3	$[]$	C47, C48, C53
C47	$[1,1,c_2,-4c_2]$	5	$[]$	C54
C48	$[1,c_1^2,-4c_2^2c_1^3,c_2^2c_1]$	3	$[2]$	C54
C49	$[1,c_1,c_2,-4c_2^3c_1^3]$	1	$[8]$	C50
C50	$[1,c_1^2,c_2,-4c_2^3c_1^2]$	2	$[4]$	C51, C52, C53
C51	$[1,1,c_2,-4c_2^3]$	3	$[2,2]$	C54
C52	$[1,-4,c_2,c_2^3]$	3	$[4]$	C54
C53	$[1,c_1^2,c_2^2,-4c_2^2c_1^2]$	4	$[2]$	C54
C54	$[1,1,c_2^2,-4c_2^2]$	6	$[2]$	C55
C55	$[1,1,1,-4]$	10	$[]$	
		Other cases		
C56	$[1,c_1,c_2,c_3]$	1	$[2]$	C1, C34, C57, C58

Number	Example	ρ	Br_1	Subcases
C57	$[1, c_1, c_2, c_3^2]$	1	$[2, 2]$	C2, C35, C59, C61, C62, C63, C70
C58	$[1, c_1, c_2, -4c_3^2]$	1	$[2]$	C4, C35, C60, C62, C66, C74
C59	$[1, c_1, c_2, 1]$	1	$[4, 2]$	C8, C39, C64, C65
C60	$[1, c_1, c_2, -4]$	1	$[4]$	C12, C42, C67
C61	$[1, c_1, c_2^2, c_3^2]$	1	$[2, 2, 2]$	C3, C36, C64, C71
C62	$[1, c_1, c_2^2, -4c_3^2]$	1	$[2, 2]$	C5, C36, C65, C67, C72, C75
C63	$[1, c_1, c_2, c_2^2]$	1	$[2, 2]$	C6, C38, C64, C65, C71, C72
C64	$[1, c_1, c_2^2, 1]$	1	$[4, 2, 2]$	C9, C40, C68, C73
C65	$[1, c_1, -4c_2^2, 1]$	1	$[4, 2, 2]$	C10, C40, C69, C76
C66	$[1, c_1, c_2, -4c_2^2]$	1	$[4]$	C7, C37, C67, C75
C67	$[1, c_1, c_2^2, -4]$	1	$[4, 2]$	C13, C43, C69, C77
C68	$[1, c_1, 1, 1]$	1	$[4, 4, 2, 2]$	C11, C41
C69	$[1, c_1, 1, -4]$	1	$[4, 4, 4]$	C14, C44
C70	$[1, c_1, c_2, c_2^2c_1^2]$	2	$[2]$	C8, C39, C71, C72
C71	$[1, c_1^2, c_2, c_2^2]$	2	$[2, 2]$	C9, C40, C73
C72	$[1, -4c_1^2, c_2, c_2^2]$	2	$[2, 2]$	C10, C40, C77
C73	$[1, c_1, 1, c_1^2]$	3	$[2, 2]$	C11, C41
C74	$[1, c_1, c_2, -4c_2^2c_1^2]$	2	$[]$	C12, C42, C75
C75	$[1, c_1^2, c_2, -4c_2^2]$	2	$[2]$	C13, C43, C76, C77
C76	$[1, c_1, 1, -4c_1^2]$	3	$[4]$	C14, C44
C77	$[1, c_1, -4, c_1^2]$	3	$[2]$	C14, C44

A.4 $k \cap \mathbb{Q}(\epsilon) = \mathbb{Q}(\sqrt{-2})$

Number	Example	ρ	Br_1	Subcases
		$a_0a_1a_2a_3$ square		
D1	$[1, c_1, c_2, c_3^2c_2^3c_1^3]$	2	$[2]$	D2, D4, D15, D22

Number	Example	ρ	Br_1	Subcases
D2	$[1, c_1^2, c_2, c_3^2c_2^3]$	2	$[2, 2, 2]$	D3, D5, D6, D8, D16, D23
D3	$[1, c_1^2, c_2^2, c_3^2]$	2	$[2, 2, 2, 2, 2]$	D9, D25
D4	$[1, -4c_1^2, c_2, -4c_3^2c_2^3]$	2	$[2]$	D5, D7, D12, D19, D28
D5	$[1, c_1^2, -4c_2^2, -4c_3^2]$	2	$[2, 2, 2]$	D10, D13, D30
D6	$[1, c_1, c_2^2c_1^3, c_1^2]$	2	$[2, 2, 2]$	D9, D10, D18, D24
D7	$[1, c_1, -4c_2^2c_1^3, -4c_1^2]$	2	$[2, 2]$	D13, D21, D29
D8	$[1, c_1^2, c_2, c_2]$	3	$[2, 2]$	D9, D10, D17, D24
D9	$[1, c_1^2, c_2^2, 1]$	3	$[2, 2, 2, 2]$	D11, D26
D10	$[1, -4c_1^2, -4c_2^2, 1]$	3	$[2, 2, 2, 2]$	D14, D31
D11	$[1, c_1^2, 1, 1]$	5	$[2, 2, 2]$	D27
D12	$[1, -4c_1^2, c_2, -4c_2]$	3	$[2]$	D13, D20, D29
D13	$[1, c_1^2, -4c_2^2, -4]$	3	$[2, 2, 2]$	D14, D32
D14	$[1, c_1^2, -4, -4]$	5	$[2, 2, 2]$	D33
D15	$[1, c_1, c_2, c_2^3c_1]$	3	$[]$	D16, D19, D23, D28
D16	$[1, c_1, c_2^2c_1^3, c_2^2c_1^2]$	4	$[2]$	D17, D18, D25, D30
D17	$[1, 1, c_2, c_2]$	6	$[]$	D26, D31
D18	$[1, c_1^2, c_2^2c_1^3, c_2^2c_1]$	4	$[2, 2]$	D26, D31
D19	$[1, c_1, -4c_2^2c_1^3, -4c_2^2c_1^2]$	4	$[]$	D20, D21, D30
D20	$[1, -4, c_2, -4c_2]$	6	$[]$	D32
D21	$[1, -4c_1^2, c_2^2c_1^3, -4c_2^2c_1]$	4	$[2]$	D32
D22	$[1, c_1, c_2, c_2^3c_1^3]$	2	$[8]$	D23, D28
D23	$[1, c_1^2, c_2, c_2^3c_1^2]$	3	$[4, 2]$	D24, D25, D30
D24	$[1, 1, c_2, c_2^3]$	4	$[4]$	D26, D31
D25	$[1, c_1^2, c_2^2, c_2^2c_1^2]$	5	$[2, 2, 2]$	D26
D26	$[1, 1, c_2^2, c_2^2]$	7	$[2, 2]$	D27
D27	$[1, 1, 1, 1]$	11	$[]$	
D28	$[1, -4c_1^2, c_2, -4c_2^3c_1^2]$	3	$[4]$	D29, D30
D29	$[1, -4, c_2, -4c_2^3]$	4	$[4]$	D32
D30	$[1, c_1^2, -4c_2^2, -4c_2^2c_1^2]$	5	$[4]$	D31, D32
D31	$[1, 1, -4c_2^2, -4c_2^2]$	7	$[2, 2]$	D33

Number	Example	ρ	Br_1	Subcases
D32	$[1, -4, c_2^2, -4c_2^2]$	7	$[4]$	D33
D33	$[1, 1, -4, -4]$	11	$[2]$	
		$-a_0a_1a_2a_3$ square		
D34	$[1, c_1, c_2, -4c_3^2c_2^3c_1^3]$	1	$[2]$	D35, D45, D49
D35	$[1, c_1^2, c_2, -4c_3^2c_2^3]$	1	$[2, 2]$	D36, D37, D38, D39, D42, D46, D50
D36	$[1, c_1^2, c_2^2, -4c_3^2]$	1	$[2, 2, 2, 2]$	D40, D43, D53
D37	$[1, c_1, c_2^2c_1^3, -4c_1^2]$	1	$[4, 2]$	D43, D48, D51
D38	$[1, c_1, -4c_2^2c_1^3, c_1^2]$	1	$[2, 2, 2]$	D40, D48, D52
D39	$[1, -4c_1^2, c_2, c_2]$	2	$[2, 2]$	D40, D47, D51
D40	$[1, c_1^2, -4c_2^2, 1]$	2	$[2, 2, 2, 2]$	D41, D44, D54
D41	$[1, -4c_1^2, 1, 1]$	4	$[2, 2, 2]$	D55
D42	$[1, c_1^2, c_2, -4c_2]$	2	$[2]$	D43, D47, D52
D43	$[1, c_1^2, c_2^2, -4]$	2	$[2, 2, 2]$	D44, D54
D44	$[1, c_1^2, 1, -4]$	4	$[2, 2, 2]$	D55
D45	$[1, c_1, c_2, -4c_2^3c_1]$	2	$[]$	D46, D50
D46	$[1, c_1, c_2^2c_1^3, -4c_2^2c_1^2]$	3	$[]$	D47, D48, D53
D47	$[1, 1, c_2, -4c_2]$	5	$[]$	D54
D48	$[1, c_1^2, -4c_2^2c_1^3, c_2^2c_1]$	3	$[2]$	D54
D49	$[1, c_1, c_2, -4c_2^3c_1^3]$	1	$[8]$	D50
D50	$[1, c_1^2, c_2, -4c_2^3c_1^2]$	2	$[4]$	D51, D52, D53
D51	$[1, 1, c_2, -4c_2^3]$	3	$[2, 2]$	D54
D52	$[1, -4, c_2, c_2^3]$	3	$[4]$	D54
D53	$[1, c_1^2, c_2^2, -4c_2^2c_1^2]$	4	$[2]$	D54
D54	$[1, 1, c_2^2, -4c_2^2]$	6	$[2]$	D55
D55	$[1, 1, 1, -4]$	10	$[]$	
		Other cases		
D56	$[1, c_1, c_2, c_3]$	1	$[2]$	D1, D34, D57, D58
D57	$[1, c_1, c_2, -4c_3^2]$	1	$[2]$	D4, D35, D60, D62, D66, D74

Number	Example	ρ	Br_1	Subcases
D58	$[1, c_1, c_2, c_3^2]$	1	$[2, 2]$	D2, D35, D59, D61, D62, D63, D70
D59	$[1, c_1, c_2, 1]$	1	$[4, 2]$	D8, D39, D64, D65
D60	$[1, c_1, c_2, -4]$	1	$[4]$	D12, D42, D67
D61	$[1, c_1, c_2^2, c_3^2]$	1	$[2, 2, 2]$	D3, D36, D64, D71
D62	$[1, c_1, c_2^2, -4c_3^2]$	1	$[2, 2]$	D5, D36, D65, D67, D72, D75
D63	$[1, c_1, c_2, c_2^2]$	1	$[2, 2]$	D6, D38, D64, D65, D71, D72
D64	$[1, c_1, c_2^2, 1]$	1	$[4, 2, 2]$	D9, D40, D68, D73
D65	$[1, c_1, -4c_2^2, 1]$	1	$[4, 2, 2]$	D10, D40, D69, D76
D66	$[1, c_1, c_2, -4c_2^2]$	1	$[4]$	D7, D37, D67, D75
D67	$[1, c_1, c_2^2, -4]$	1	$[4, 2]$	D13, D43, D69, D77
D68	$[1, c_1, 1, 1]$	1	$[4, 4, 4]$	D11, D41
D69	$[1, c_1, 1, -4]$	1	$[4, 4, 4]$	D14, D44
D70	$[1, c_1, c_2, c_2^2c_1^2]$	2	$[2]$	D8, D39, D71, D72
D71	$[1, c_1^2, c_2, c_2^2]$	2	$[2, 2]$	D9, D40, D73
D72	$[1, -4c_1^2, c_2, c_2^2]$	2	$[2, 2]$	D10, D40, D77
D73	$[1, c_1, 1, c_1^2]$	3	$[4]$	D11, D41
D74	$[1, c_1, c_2, -4c_2^2c_1^2]$	2	$[]$	D12, D42, D75
D75	$[1, c_1^2, c_2, -4c_2^2]$	2	$[2]$	D13, D43, D76, D77
D76	$[1, c_1, 1, -4c_1^2]$	3	$[4]$	D14, D44
D77	$[1, c_1, -4, c_1^2]$	3	$[2]$	D14, D44

A.5 $k \cap \mathbb{Q}(\epsilon) = \mathbb{Q}(\epsilon)$

Number	Example	ρ	Br_1	Subcases
		$a_0a_1a_2a_3$ square		
E1	$[1, c_1, c_2, c_3^2c_2^3c_1^3]$	2	$[2]$	E2, E8, E12
E2	$[1, c_1^2, c_2, c_3^2c_2^3]$	2	$[2, 2, 2]$	E3, E4, E5, E9, E13
E3	$[1, c_1^2, c_2^2, c_3^2]$	2	$[2, 2, 2, 2, 2, 2]$	E6, E15

Number	Example	ρ	Br_1	Subcases
E4	$[1, c_1, c_2^2c_1^3, c_1^2]$	2	$[2, 2, 2, 2]$	E6, E11, E14
E5	$[1, c_1^2, c_2, c_2]$	4	$[2, 2]$	E6, E10, E14
E6	$[1, c_1^2, c_2^2, 1]$	4	$[2, 2, 2, 2, 2, 2]$	E7, E16
E7	$[1, c_1^2, 1, 1]$	8	$[2, 2, 2, 2, 2]$	E17
E8	$[1, c_1, c_2, c_2^3c_1]$	4	$[]$	E9, E13
E9	$[1, c_1, c_2^2c_1^3, c_2^2c_1^2]$	6	$[]$	E10, E11, E15
E10	$[1, 1, c_2, c_2]$	10	$[]$	E16
E11	$[1, c_1^2, c_2^2c_1^3, c_2^2c_1]$	6	$[2, 2]$	E16
E12	$[1, c_1, c_2, c_2^3c_1^3]$	2	$[8, 4]$	E13
E13	$[1, c_1^2, c_2, c_2^3c_1^2]$	4	$[4, 4]$	E14, E15
E14	$[1, 1, c_2, c_2^3]$	6	$[4, 2]$	E16
E15	$[1, c_1^2, c_2^2, c_2^2c_1^2]$	8	$[2, 2]$	E16
E16	$[1, 1, c_2^2, c_2^2]$	12	$[2, 2]$	E17
E17	$[1, 1, 1, 1]$	20	$[]$	
		Other cases		
E18	$[1, c_1, c_2, c_3]$	1	$[2]$	E1, E19
E19	$[1, c_1, c_2, c_3^2]$	1	$[2, 2]$	E2, E20, E21, E22, E25
E20	$[1, c_1, c_2, 1]$	1	$[4, 4]$	E5, E23
E21	$[1, c_1, c_2^2, c_3^2]$	1	$[4, 2, 2]$	E3, E23, E26
E22	$[1, c_1, c_2, c_2^2]$	1	$[4, 2]$	E4, E23, E26
E23	$[1, c_1, c_2^2, 1]$	1	$[4, 4, 2, 2]$	E6, E24, E27
E24	$[1, c_1, 1, 1]$	1	$[4, 4, 4, 4, 4, 2]$	E7
E25	$[1, c_1, c_2, c_2^2c_1^2]$	3	$[]$	E5, E26
E26	$[1, c_1^2, c_2, c_2^2]$	3	$[2, 2]$	E6, E27
E27	$[1, c_1, 1, c_1^2]$	5	$[2, 2]$	E7

Appendix B

Locally soluble surfaces with no small solutions

This appendix lists the surfaces of the form

$$ax^4 + by^4 = cu^4 + dv^4$$

where a, b, c and d are no greater than 15, the equation is locally soluble, but no integer solution of height less than 10^4 exists. These data are substantially the same as those obtained by Pinch [31]; the only difference is that there only solutions of height up to 300 were sought, or 1000 in some specific cases.

The surfaces are listed as (a, b, c, d) and are grouped according to their case, as classified in the tables in Appendix A. Before each case, we give the structure of $\mathrm{Br}_1 / \mathrm{Br}_0$ for that case.

Case A8 $[2]$

(7, 8, 9, 14)

Case A19 $[2, 2, 2]$

(4, 9, 8, 8)

Case A76 $[8]$

(2, 9, 6, 12)

Case A109 [2]

(4, 12, 10, 15)

Case A112 [2]

(4, 14, 7, 9) (4, 7, 9, 14)

Case A118 $[4, 2, 2]$

(1, 4, 8, 9)

Case A121 [2]

(1, 1, 6, 12)	(2, 4, 11, 11)	(3, 6, 11, 11)	(3, 6, 8, 8)
(6, 12, 11, 11)			

Case A123 $[2, 2]$

(2, 4, 9, 9)

Case A127 []

(3, 14, 7, 12) (3, 7, 12, 14)

Case A222 [2]

(1, 14, 6, 11)	(1, 15, 10, 11)	(1, 15, 11, 13)	(1, 15, 11, 14)
(1, 15, 7, 11)	(1, 7, 5, 12)	(1, 7, 6, 11)	(11, 14, 12, 15)
(2, 10, 7, 11)	(2, 11, 12, 15)	(2, 11, 3, 15)	(2, 11, 6, 10)
(2, 12, 7, 11)	(2, 13, 5, 11)	(2, 13, 6, 10)	(2, 14, 10, 15)
(2, 14, 5, 12)	(2, 14, 6, 13)	(2, 15, 7, 11)	(2, 3, 7, 11)
(2, 6, 5, 11)	(2, 6, 5, 13)	(2, 6, 7, 11)	(2, 6, 7, 15)
(2, 7, 10, 15)	(2, 7, 11, 12)	(3, 13, 10, 15)	(3, 13, 7, 8)
(3, 13, 8, 14)	(3, 7, 4, 15)	(3, 7, 8, 11)	(3, 8, 13, 14)
(4, 11, 7, 13)	(4, 12, 11, 13)	(4, 12, 11, 14)	(4, 12, 5, 14)
(4, 12, 7, 10)	(4, 15, 6, 14)	(4, 5, 11, 14)	(4, 5, 12, 13)
(4, 5, 6, 14)	(4, 6, 11, 15)	(4, 7, 6, 10)	(5, 11, 6, 7)
(5, 11, 6, 8)	(5, 11, 7, 13)	(6, 10, 7, 11)	(7, 10, 11, 12)

(7, 13, 8, 15)	(7, 8, 11, 13)	(7, 9, 10, 15)	(7, 9, 11, 13)
(7, 9, 12, 13)	(7, 9, 12, 15)	(8, 12, 11, 13)	(8, 15, 11, 13)
(9, 10, 11, 14)	(9, 10, 12, 13)	(9, 11, 12, 15)	(9, 11, 13, 14)
(9, 13, 10, 15)			

Case A223 $[2, 2]$

(4, 9, 11, 14)

Case A224 $[2]$

(4, 13, 7, 9)	(4, 13, 9, 11)	(4, 15, 7, 9)

Case A225 $[2]$

(1, 2, 5, 12)	(1, 2, 7, 10)	(1, 8, 10, 15)	(1, 8, 11, 14)
(1, 8, 6, 11)	(2, 14, 3, 6)	(2, 5, 6, 12)	(2, 7, 6, 12)
(2, 9, 12, 15)	(2, 9, 13, 14)	(3, 6, 11, 14)	(3, 6, 8, 14)
(4, 8, 11, 13)	(4, 8, 13, 15)	(4, 8, 7, 13)	(6, 12, 7, 15)
(7, 14, 11, 12)	(8, 9, 10, 14)	(8, 9, 11, 13)	(8, 9, 11, 14)

Case A226 $[2]$

(1, 14, 7, 10)	(1, 15, 2, 11)	(1, 15, 8, 11)	(1, 7, 3, 14)
(2, 10, 7, 9)	(2, 11, 4, 12)	(2, 11, 7, 9)	(2, 14, 3, 7)
(2, 14, 5, 7)	(2, 14, 6, 7)	(2, 14, 7, 10)	(2, 14, 7, 12)
(2, 14, 7, 13)	(2, 14, 9, 10)	(2, 14, 9, 13)	(2, 7, 11, 14)
(3, 13, 4, 6)	(3, 4, 8, 11)	(4, 12, 6, 7)	(4, 14, 7, 13)
(4, 7, 6, 14)	(5, 14, 7, 9)	(6, 10, 12, 13)	(6, 14, 7, 15)
(6, 7, 8, 14)	(7, 11, 13, 14)	(7, 13, 14, 15)	(7, 8, 10, 14)
(7, 9, 10, 14)	(7, 9, 13, 14)	(7, 9, 8, 11)	

Case A227 $[2, 2]$

(2, 2, 7, 11)	(4, 11, 10, 10)	(4, 4, 11, 13)	(4, 4, 7, 13)
(4, 6, 11, 11)	(7, 7, 11, 12)	(8, 8, 10, 15)	(8, 8, 11, 14)

Case A228 $[2]$

(1, 12, 3, 14)	(1, 14, 4, 13)	(2, 3, 8, 11)	(3, 13, 12, 14)
(3, 14, 4, 12)	(3, 4, 11, 12)	(3, 7, 11, 12)	

Case A229 $[4, 2]$

(1, 4, 3, 14)	(1, 4, 6, 11)	(2, 8, 11, 13)	(2, 8, 11, 15)
(2, 8, 3, 15)	(2, 8, 5, 11)	(2, 8, 5, 13)	(2, 8, 7, 11)

Case A234 $[2, 2]$

(2, 14, 4, 9)

Case A235 $[2]$

(1, 14, 8, 9)	(2, 9, 4, 14)	(4, 8, 7, 9)	(4, 8, 9, 11)
(4, 8, 9, 15)			

Case A238 $[2, 2, 2]$

(4, 4, 7, 9) (4, 4, 9, 11)

Case A240 $[4, 2]$

(1, 4, 8, 13)	(2, 8, 7, 9)	(3, 12, 6, 10)	(3, 12, 6, 13)

Case A241 $[2]$

(4, 12, 9, 10)

Case A248 $[2, 2]$

(2, 2, 7, 9)	(2, 2, 9, 11)	(7, 12, 14, 14)	(7, 9, 14, 14)
(8, 8, 9, 11)	(8, 8, 9, 13)		

Case A249 $[4]$

(4, 6, 9, 13)

Case A251 $[4]$

(1, 8, 4, 13) (2, 14, 8, 9)

Case A257 $[2, 2]$

(4, 9, 10, 15)

Appendix C

Surfaces with trivial Brauer group and no small solutions

This appendix lists surfaces belonging to case A127 of the table in Appendix A. Such surfaces have no Brauer–Manin obstruction arising from the arithmetic part of the Brauer group. Those listed here are everywhere locally soluble and have no rational point of height less than 10^4.

The table lists (a, b, c, d), where the surface is of the form

$$ax^4 + by^4 = cu^4 + dv^4.$$

$(7, 54, 28, 27)$	$(3, 7, 12, 14)$	$(3, 14, 12, 7)$	$(21, 2, 84, 1)$
$(11, 1, 44, 2)$	$(11, 24, 44, 3)$	$(11, 9, 44, 72)$	$(11, 27, 44, 54)$
$(11, 54, 44, 27)$	$(11, 216, 44, 27)$	$(3, 88, 12, 11)$	$(33, 1, 132, 2)$
$(33, 2, 132, 1)$	$(33, 8, 132, 1)$	$(11, 56, 44, 7)$	$(7, 88, 28, 11)$
$(11, 21, 44, 42)$	$(11, 42, 44, 21)$	$(11, 21, 44, 168)$	$(7, 33, 28, 264)$
$(33, 7, 132, 56)$	$(21, 22, 84, 11)$	$(17, 1, 68, 2)$	$(17, 8, 68, 1)$
$(17, 3, 68, 6)$	$(17, 6, 68, 3)$	$(17, 3, 68, 24)$	$(17, 72, 68, 9)$
$(17, 27, 68, 216)$	$(3, 17, 12, 136)$	$(9, 136, 36, 17)$	$(17, 7, 68, 56)$
$(17, 168, 68, 21)$	$(21, 34, 84, 17)$	$(17, 11, 68, 88)$	$(11, 17, 44, 34)$
$(11, 34, 44, 17)$	$(11, 17, 44, 136)$	$(17, 33, 68, 66)$	$(33, 17, 132, 34)$
$(33, 34, 132, 17)$	$(33, 136, 132, 17)$	$(1, 19, 4, 38)$	$(19, 1, 76, 8)$

$(19, 24, 76, 3)$	$(19, 9, 76, 18)$	$(19, 18, 76, 9)$	$(19, 9, 76, 72)$
$(19, 216, 76, 27)$	$(3, 19, 12, 38)$	$(3, 152, 12, 19)$	$(19, 7, 76, 14)$
$(19, 14, 76, 7)$	$(19, 56, 76, 7)$	$(19, 21, 76, 168)$	$(21, 19, 84, 152)$
$(19, 88, 76, 11)$	$(11, 152, 44, 19)$	$(19, 33, 76, 264)$	$(33, 19, 132, 38)$
$(33, 38, 132, 19)$	$(33, 19, 132, 152)$	$(17, 19, 68, 38)$	$(17, 38, 68, 19)$
$(17, 19, 68, 152)$	$(1, 23, 4, 184)$	$(23, 27, 92, 54)$	$(23, 54, 92, 27)$
$(23, 216, 92, 27)$	$(9, 23, 36, 46)$	$(9, 23, 36, 184)$	$(23, 7, 92, 14)$
$(7, 23, 28, 46)$	$(7, 184, 28, 23)$	$(23, 42, 92, 21)$	$(23, 22, 92, 11)$
$(11, 184, 44, 23)$	$(33, 23, 132, 184)$	$(17, 23, 68, 184)$	$(23, 152, 92, 19)$
$(19, 23, 76, 46)$	$(19, 46, 76, 23)$	$(19, 184, 76, 23)$	$(1, 62, 4, 31)$
$(31, 2, 124, 1)$	$(31, 24, 124, 3)$	$(31, 9, 124, 72)$	$(3, 248, 12, 31)$
$(9, 31, 36, 248)$	$(31, 56, 124, 7)$	$(7, 248, 28, 31)$	$(31, 21, 124, 168)$
$(21, 31, 84, 62)$	$(21, 62, 84, 31)$	$(21, 31, 84, 248)$	$(31, 88, 124, 11)$
$(11, 31, 44, 62)$	$(11, 62, 44, 31)$	$(11, 248, 44, 31)$	$(33, 31, 132, 62)$
$(33, 62, 132, 31)$	$(33, 31, 132, 248)$	$(31, 17, 124, 136)$	$(17, 31, 68, 62)$
$(17, 31, 68, 248)$	$(31, 19, 124, 38)$	$(19, 248, 76, 31)$	$(31, 184, 124, 23)$

Appendix D

Implementation of algorithms

This appendix contains the implementations, in GP, of the algorithms described in the text.

D.1 Subgroups of Γ

A subgroup H of Γ is represented by a 2-element row vector. The first element is a 4×4 matrix whose columns generate $H \cap \Gamma'$; the second element is either the empty vector, or else a column vector representing an element g of Γ' such that τg is the fifth generator for H.

D.1.1 Algorithm 3.9

```
\\ Given a subgroup H in HNF and an element h, reduce h to a
\\ canonical coset representative by subtracting elements of H
coset_reduce(H,h) = forstep(i = 4, 1, -1,
  h -= (h[i] \ H[i,i]) * H[,i]~); h;

\\ Put a subgroup into a canonical form
subgroup_reduce(H) =
{
  for(i = 1, 3, H[1][i,] %= 4; if(H[2] != [], H[2][i] %= 4));
  H[1][4,] %= 2; if(H[2] != [], H[2][4] %= 2);
```

```
  H[1] = mathnf(concat(H[1],matdiagonal([4,4,4,2])));
  if(H[2] != [], H[2] = coset_reduce(H[1],H[2]));
  H;
}
```

D.1.2 Algorithm 3.10

```
\\ Return a canonical representative of the conjugacy class
\\ of H
conj_reduce(H) =
{
  for(i = 1, 3, H[1][i,] %= 4; if(H[2] != [], H[2][i] %= 4));
  H[1][4,] %= 2; if(H[2] != [], H[2][4] %= 2);
  H[1] = mathnf(concat(H[1],matdiagonal([4,4,4,2])));
  if(H[2] != [],
    H[2] = coset_reduce(mathnf(concat(H[1],2*matid(4))),H[2]));
  H;
}
```

D.1.3 Finding canonical subgroups

```
\\ Swap two rows of the subgroup
swap_rows(H,i,j) =
{
  local(t);
  t = H[1][i,]; H[1][i,] = H[1][j,]; H[1][j,] = t;
  if(H[2] != [], t=H[2][i]; H[2][i] = H[2][j]; H[2][j] = t);
  H;
}

\\ Return the element of t which comes first in the lex
\\ ordering
lexmin(t) =
{
```

```
  local(n, j);
  n = matsize(t)[2];
  j = 1;
  for(i = 2, n, if(lex(t[i], t[j]) == -1, j = i));
  t[j];
}

\\ Return a canonical subgroup equivalent to H by
\\ conjugation and permutation of the first three rows.
make_unique1(H) =
{
  local(t);
  t = vector(6);
  t[1] = conj_reduce(H);
  t[2] = conj_reduce(swap_rows(t[1],1,2));
  t[3] = conj_reduce(swap_rows(t[2],2,3));
  t[4] = conj_reduce(swap_rows(t[3],1,2));
  t[5] = conj_reduce(swap_rows(t[4],2,3));
  t[6] = conj_reduce(swap_rows(t[5],1,2));
  lexmin(t);
}

\\ Return a canonical subgroup equivalent to H by conjugation
\\ and projective permutation of variables
make_unique(H) =
{
  local(A, B, C, t);
  A = [-1,0,0,0;-1,1,0,0;-1,0,1,0;0,0,0,1];
  B = [1,-1,0,0;0,-1,0,0;0,-1,1,0;0,0,0,1];
  C = [1,0,-1,0;0,1,-1,0;0,0,-1,0;0,0,0,1];
  t = vector(4);
  t[1] = make_unique1(H);
  if(H[2] == [],
```

```
    t[2] = make_unique1([A*H[1], []]);
    t[3] = make_unique1([B*H[1], []]);
    t[4] = make_unique1([C*H[1], []]);
  ,
    t[2] = make_unique1([A*H[1], (A*H[2]~)~]);
    t[3] = make_unique1([B*H[1], (B*H[2]~)~]);
    t[4] = make_unique1([C*H[1], (C*H[2]~)~]);
  );
  lexmin(t);
}
```

D.2 Relating surfaces to subgroups

D.2.1 Algorithm 3.11

```
find_group(a0, a1, a2, a3) =
{
  local(f1, f2, f3, S, n, Q, Qe, K1, K2, K3,
    v1, v2, v3, M, v, w1, w2, w3);
  f1 = factor(a1/a0);
  f2 = factor(a2/a0);
  f3 = factor(a3/a0);

  \\ First find out which primes interest us
  S = Set([-1, 2]);
  S = setunion(S, Set(f1[,1]));
  S = setunion(S, Set(f2[,1]));
  S = setunion(S, Set(f3[,1]));
  n = matsize(S)[2];
  for(i = 1, n, S[i] = eval(S[i]));
  S = vecsort(S);

  \\ Now find the subgroups of Q* containing fourth
```

```
\\ powers of the various fields
Q = 4 * matid(n); Q[1,1] = 2;
Qe = Q; Qe[1,2] = 1; Qe[2,2] = 2; Qe[2,1] = 2;
v3 = factor2basis(f3, S); K3 = concat(v3, Qe);
v2 = factor2basis(f2, S); K2 = concat(v2, K3);
v1 = factor2basis(f1, S); K1 = concat(v1, K2);

\\ Work out the degrees of the relevant extensions
M = matrix(4,4); v = vector(4);
v[1] = matdet(mathnf(K1));
v[2] = matdet(mathnf(K2));
v[3] = matdet(mathnf(K3));
v[4] = matdet(Qe);
M[1,1] = 4 * v[1] / v[2];
M[2,2] = 4 * v[2] / v[3];
M[3,3] = 4 * v[3] / v[4];
M[4,4] = 1;

\\ Find out how the various extensions are related to
\\ each other
w1 = matsolvemod(K2, 4, (4 / M[1,1]) * v1);
w2 = matsolvemod(K3, 4, (4 / M[2,2]) * v2);
w3 = matsolvemod(Qe, 4, (4 / M[3,3]) * v3);

\\ Work out the Galois group
M[1,2] = M[2,2] * w1[1] * M[1,1] / 4;
M[2,3] = M[3,3] * w2[1] * M[2,2] / 4;
M[1,3] = (M[2,3] * w1[1] + M[3,3] * w1[2]) * M[1,1] / 4;
M[3,4] = 2 * w3[1] * M[3,3] / 4;
M[2,4] = (M[3,4] * w2[1] + 2 * w2[2]) * M[2,2] / 4;
M[1,4] = (M[2,4] * w1[1] + M[3,4] * w1[2] + 2 * w1[3])
  * M[1,1] / 4;
v[1] = v1[1] % 2;
```

```
  v[2] = v2[1] % 2;
  v[3] = v3[1] % 2;
  v[4] = 0;

  [mathnf(M), v];
}
```

D.2.2 Finding the constant field

```
\\ Return a code for the constant field fixed by H:
\\   1  Q
\\   2  Q(i)
\\   3  Q(\sqrt(2))
\\   4  Q(\sqrt(-2))
\\   5  Q(i,\sqrt(2))
constant_field(H) =
{
  if(H[2] == [], \\ is i fixed?
    if((H[1][4,] % 2) == [0,0,0,0], 5, 2),
    if((H[1][4,] % 2) == [0,0,0,0],
      if((H[2][4] % 2) == 0, 3, 4),
      1
    )
  )
}
```

D.2.3 Algorithm 3.17

```
X4 = [[1,1,1,1],[1,I,-1,-I],[1,-1,1,-1],[1,-I,-1,I],[1,1,1,1]];
X2 = [[1,1],[1,-1],[1,1]];

\\ Return a 128-element vector which contains the effect of
\\ applying the group element x to each of the 128 basis
\\ vectors
```

```
doelt(x) =
{
  local(A,B,C,D);
  A = X4[x[1]+1];
  B = X4[x[2]+1];
  C = X4[x[3]+1];
  D = X2[x[4]+1];
  tensor(A, tensor(B, tensor(C, D)))[1,];
}

\\ Return a matrix which gives a set of generators for
\\ the subring of B fixed by H, on the (multiplicative) basis
\\ ((1+i), \sqrt(2), t_1, t_2, t_3)
fixed_field(H) =
{
  local(M, n, b, c, N);
  \\ First find a basis for the fixed part as a module
  n = matsize(H[1])[2];
  M = matrix(n, 128);
  \\ Do the generators which fix i first
  for(i = 1, n, M[i,] = doelt(H[1][,i]));
  \\ Find out which basis elements were fixed by all of these
  b = vector(128);
  for(j = 1, 128,
    b[j] = 1;
    for(i = 1, n, if(M[i,j] != 1, b[j] = 0; break));
  );
  \\ Now see what happens when we apply the generator which
  \\ takes i to -i
  if(H[2] != [],
    c = doelt(H[2]);
    for(j = 1, 128,
      if(b[j] == 1,
```

```
        if(c[j] == I, b[j] = 1-I,
          if(c[j] == -1, b[j] = I,
            if(c[j] == -I, b[j] = 1+I)
          )
        )
      )
    )
  );

  \\ Next express our basis elements multiplicatively in terms
  \\ of (1+i), \sqrt(2), t_1, t_2, t_3
  N = matrix(5,129);
  for(i = 1, 128,
    if(b[i] != 0,
      N[3,i] = (i - 1) % 4;
      N[4,i] = ((i - 1) \ 4) % 4;
      N[5,i] = ((i - 1) \ 16) % 4;
      N[2,i] = (i - 1) \ 64;
      if(b[i] == 1+I, N[1,i] = 1,
        if(b[i] == I, N[1,i] = 2,
          if(b[i] == 1-I, N[1,i] = 3)
        )
      )
    )
  );
  \\ If i is fixed, stick that in too
  if(H[2] == [], N[1,129] = 2);
  \\ Now find a set of multiplicative generators
  N = mathnf(concat(N, matdiagonal([4,2,4,4,4])));
}
```

D.2.4 Algorithm 3.18

```
\\ Take powers of 4 out of an integer
remove4s(n) =
{
  local(f);
  f = factor(n); f[,2] %= 4; factorback(f);
}

\\ Give general expressions for surface (1, a_1, a_2, a_3) to
\\ give subgroup H
example(H) =
{
  local(N, v, n, c);

  N = concat([0,0,0;0,0,0;1,0,0;0,1,0;0,0,1],fixed_field(H)~)~;
  for(i=3,5,
    N[,i] *= (4 / N[i+3,i]);
    for(j=3, i-1, N[,i] -= (N[j+3,i]/N[j+3,j])*N[,j]);
  );
  v = vector(4);
  v[1] = 1;
  for(i=3, 5,
    v[i-1] = 'c1^(N[1,i] % 4) * 'c2^(N[2,i] % 4)
      * 'c3^(N[3,i] % 4);
    n = (1+I)^N[4,i] * ('r2^N[5,i] % ('r2^2-2));
    c = gcd(real(content(n)), imag(content(n)));
    n /= (c / remove4s(c));
    v[i-1] *= n;
  );
  v;
}
```

D.3 Computing with G-modules

D.3.1 Algorithm 3.19

```
\\ Find H^0(G, M)
H0(M) =
{
  local(n,r,U);
  n = matsize(M)[2];
  r = matsize(M[1])[1];
  U = matker(M[1] - matid(r));
  for(i=2,n,
    U = matintersect(U, matker(M[i] - matid(r)));
  );
  matrixqz(U,-2);
}
```

D.3.2 Working modulo m

```
\\ Find H^0(G, M \otimes Z/mZ)
H0torsion(M, m) =
{
  local(n,r,U);
  n = matsize(M)[2];
  r = matsize(M[1])[1];
  U = kermod(M[1] - matid(r), m);
  for(i=2,n,
    U = latticeintersect(U, kermod(M[i] - matid(r), m));
  );
  U;
}
```

D.3.3 Algorithm 3.20

```
\\ Find a set of generators for H^1(G, M)[m], given as elements
\\ of M \otimes Q/Z
H1torsion(M, m) =
{
  local(V,W,A,d,U);
  W = H0torsion(G,m);
  V = mathnf(concat(H0(G),
    matdiagonal(vector(matsize(M)[1],i,m))));
  \\ Find the quotient group and put it into Smith normal form
  A = matsnf(M^-1*N,1);
  d = matsnf(A[3],4);
  \\ Extract the generators
  if(d == [], U = [;],
    U = vecextract(M*A[1]^-1, Str("1.." matsize(d)[2])));
  [d, U/m];
}
```

D.3.4 Algorithm 3.22

```
\\ Represent the element g on the basis
\\   { \epsilon^n t_j/t_i | n=1,3,5,7 }
small_rep(g,i,j) =
{
  local(b);
  b = 2*g[4];
  if(j > 0, b += g[j]);
  if(i > 0, b -= g[i]);
  b %= 4;
  if(b == 0, matid(4),
    if(b == 1, [0,0,0,1;1,0,0,0;0,1,0,0;0,0,1,0],
      if(b == 2, [0,0,1,0;0,0,0,1;1,0,0,0;0,1,0,0],
        [0,1,0,0;0,0,1,0;0,0,0,1;1,0,0,0]
```

```
      )
    )
  );
}

small_rep_conj(g,i,j) \
  = [0,0,0,1;0,0,1,0;0,1,0,0;1,0,0,0] * small_rep(g,i,j);

\\ Represent the element g on the basis
\\  { L^{pqr}_{mn} | m,n=1,3,5,7 }
big_rep(g,p) = tensor(small_rep(g,(p%3)+1,((p+1)%3)+1), \
                      small_rep(g,0,p));

big_rep_conj(g,p) = tensor(\
  small_rep_conj(g,(p%3)+1,((p+1)%3)+1), \
  small_rep_conj(g,0,p));

\\ Put three 16-row matrices together into a 48-row one
concat48(M1,M2,M3) =
{
  M1 = concat(M1~,matrix(matsize(M1)[2],32))~;
  M2 = concat(matrix(matsize(M2)[2],16),
    concat(M2~,matrix(matsize(M2)[2],16)))~;
  M3 = concat(matrix(matsize(M3)[2],32),M3~)~;
  concat(M1,concat(M2,M3));
}

rep48(g) = concat48(big_rep(g,1), big_rep(g,2), big_rep(g,3));
rep48_conj(g) = concat48(big_rep_conj(g,1), \
  big_rep_conj(g,2), big_rep_conj(g,3));
```

D.3.5 Calculating a basis for $\operatorname{Pic}\bar{V}$

```
intersect(a,m,n,b,i,j) =
{
  if(a == b,
    if((m == i) && (n == j),
      -2,
      if((m == i) || (n == j), 1, 0)
    ),
    if(Mod(b,3) == Mod(a+1,3),
      if(Mod(m-n,8) == Mod(i+j,8),1,0),
      if(Mod(i-j,8) == Mod(m+n,8),1,0)
    )
  )
}
Q = matrix(48,48);
{
  for(a=0,2,
    for(m=0,3,
      for(n=0,3,
        for(b=0,2,
          for(i=0,3,
            for(j=0,3,
              Q[1+a*16+m*4+n,1+b*16+i*4+j] =
        intersect(a,2*m+1,2*n+1,b,2*i+1,2*j+1)
            )
          )
        )
      )
    )
  )
}
\\ A0 = Z-basis for kernel of Q
```

```
A0 = matrixqz(matker(Q),-2);
\\ P = plane section ( = Z-basis for positive definite part)
P = [1,1,1,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\
      0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]~;
\\ B = Q-basis for negative definite part
B = matintersect(vecextract(matsupplement(A0),"29..48"),\
                 matker(Mat(P~*Q)));
\\ C = matrix which projects onto the subspace we want
C1 = concat(P,concat(B,A0));
C2 = matdiagonal([1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,\
   0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0]);
C = C1*C2*C1^-1;
\\ Find a Z-basis for the lattice generated by the
\\ columns of C; this is a basis for NS(V)
D = mathnf(C);
\\ E = projection onto NS(V) (a left inverse for D)
E = matleftinverse(D) * C;
```

Bibliography

[1] M. Artin. On isolated rational singularities of surfaces. *Amer. J. Math.*, 88:129–136, 1966.

[2] W. Barth, C. Peters, and A. Van de Ven. *Compact Complex Surfaces*, volume 3.4 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, 1984.

[3] A. Beauville. *Complex Algebraic Surfaces*. Number 68 in London Mathematical Society Lecture Note Series. Cambridge University Press, 1983.

[4] D. J. Bernstein. Enumerating solutions to $p(a) + q(b) = r(c) + s(d)$. *Math. Comp.*, 70(233):389–394, 2001.

[5] N. Bourbaki. *Commutative Algebra*. Elements of Mathematics. Hermann, Paris, 1972. Translated from the French.

[6] J. W. S. Cassels and M. J. T. Guy. On the Hasse principle for cubic surfaces. *Mathematika*, 13:111–120, 1966.

[7] F. Châtelet. Variations sur un thème de H. Poincaré. *Ann. Sci. École Norm. Sup. (3)*, 61:249–300, 1944.

[8] H. Cohen. *A Course in Computational Algebraic Number Theory*. Number 138 in Graduate Texts in Mathematics. Springer-Verlag, second edition, 1995.

[9] J.-L. Colliot-Thélène. L'arithmétique des variétés rationnelles. *Ann. Fac. Sci. Toulouse Math. (6)*, 1(3):295–336, 1992.

[10] J.-L. Colliot-Thélène, D. Coray, and J.-J. Sansuc. Descente et principe de Hasse pour certaines variétés rationelles. *J. Reine Angew. Math.*, 320:150–191, 1980.

[11] J.-L. Colliot-Thélène, A. N. Skorobogatov, and Sir Peter Swinnerton-Dyer. Hasse principle for pencils of curves of genus one whose jacobians have rational 2-division points. *Inventiones Mathematicae*, 134:579–650, 1998.

[12] J.-L. Colliot-Thélène, A. N. Skorobogatov, and Sir Peter Swinnerton-Dyer. Rational points and zero-cycles on fibred varieties: Schinzel's hypothesis and Salberger's device. *J. Reine Angew. Math.*, 495:1–28, 1998.

[13] J.-L. Colliot-Thélène and Sir Peter Swinnerton-Dyer. Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties. *J. Reine Angew. Math.*, 453:49–112, 1994.

[14] P. Deligne, editor. *Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$: Cohomologie Étale.* Number 569 in Lecture Notes in Mathematics. Springer-Verlag, 1977.

[15] M. Deuring. *Algebren*, volume 4.1 of *Ergebnisse der Mathematik*. Springer, 1935.

[16] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.*, 44(170):463–471, 1985.

[17] P. Griffiths and J. Harris. *Principles of algebraic geometry*. Wiley-Interscience [John Wiley & Sons], New York, 1978. Pure and Applied Mathematics.

[18] A. Grothendieck. Le groupe de Brauer I, II, III. In J. Giraud et al., editors, *Dix Exposés sur la Cohomologie des Schémas*, volume 3 of *Advanced studies in mathematics*. North-Holland, Amsterdam, 1968.

[19] A. Grothendieck. Le groupe fondamental: Généralités. In *Séminaire de Géometrie Algébrique du Bois-Marie SGA 1: Revêtements Étales et Groupe Fondamental*, number 224 in Lecture Notes in Mathematics, chapter V. Springer-Verlag, 1971.

[20] D. Harari. Obstructions de Manin transcendantes. In *Number theory (Paris, 1993–1994)*, pages 75–87. Cambridge Univ. Press, Cambridge, 1996.

[21] R. Hartshorne. *Algebraic Geometry.* Number 52 in Graduate Texts in Mathematics. Springer-Verlag, 1977.

[22] V. A. Iskovskikh and I. R. Shafarevich. Algebraic surfaces. In I. R. Shafarevich, editor, *Algebraic Geometry II*, volume 35 of *Encyclopaedia of Mathematical Sciences*, chapter II. Springer-Verlag, 1996.

[23] S. Lang. *Survey of Diophantine Geometry.* Springer, 1997.

[24] Yu. I. Manin. Le groupe de Brauer-Grothendieck en géométrie diophantienne. In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*, pages 401–411. Gauthier-Villars, Paris, 1971.

[25] Yu. I. Manin. *Cubic forms: algebra, geometry, arithmetic.* North-Holland Publishing Co., Amsterdam, 1974. Translated from Russian by M. Hazewinkel, North-Holland Mathematical Library, Vol. 4.

[26] Yu. I. Manin and M. A. Tsfasman. Rational varieties: algebra, geometry, arithmetic. *Uspekhi Mat. Nauk*, 41(2(248)):43–94, 1986.

[27] J. S. Milne. Class field theory. Online notes, available on the author's web site at `http://www.jmilne.org/math`.

[28] J. S. Milne. Lectures on etale cohomology. Online notes, available on the author's web site at `http://www.jmilne.org/math`.

[29] J. S. Milne. *Etale Cohomology.* Number 33 in Princeton mathematical series. Princeton University Press, 1980.

[30] L. J. Mordell. On the conjecture for the rational points on a cubic surface. *J. London Math. Soc.*, 40:149–158, 1965.

[31] R. G. E. Pinch. Various calculations on diagonal quartic surfaces. Unpublished, 1987.

[32] R. G. E. Pinch and H. P. F. Swinnerton-Dyer. Arithmetic of diagonal quartic surfaces. I. In *L-functions and arithmetic (Durham, 1989)*, pages 317–338. Cambridge Univ. Press, Cambridge, 1991.

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

[34] E. S. Selmer. The Diophantine equation $ax^3+by^3+cz^3 = 0$. *Acta Math.*, 85:203–362 (1 plate), 1951.

[35] J.-P. Serre. *Corps Locaux*, volume VIII of *Publications de l'Institut de Mathématique de l'Université de Nancago*. Hermann, Paris, 1968.

[36] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[37] T. Shioda. On elliptic modular surfaces. *J. Math. Soc. Japan*, 24:20–59, 1972.

[38] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[39] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Number 151 in Graduate Texts in Mathematics. Springer-Verlag, 1994.

[40] D. Simon. *Équations dans les Corps de Nombres et Discriminants Minimaux*. PhD thesis, Université Bordeaux I, 1998.

[41] A. N. Skorobogatov. Beyond the Manin obstruction. *Invent. Math.*, 135(2):399–424, 1999.

[42] H. P. F. Swinnerton-Dyer. Two special cubic surfaces. *Mathematika*, 9:54–56, 1962.

[43] Sir Peter Swinnerton-Dyer. The Brauer group of cubic surfaces. *Math. Proc. Camb. Phil. Soc.*, 113:449–460, May 1993.

[44] Sir Peter Swinnerton-Dyer. Arithmetic of diagonal quartic surfaces, II. *Proc. London Math. Soc.*, 80:513–544, 2000.

[45] G. Tamme. *Introduction to Étale Cohomology*. Springer-Verlag, 1994.

[46] J. T. Tate. Global class field theory. In J. W. S. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*. London Mathematical Society, Academic Press, 1967.