

**Aspects of the arithmetic of uniquely trigonal  
genus four curves:  
arithmetic invariant theory and class groups of  
cubic number fields**

by

**Avinash Kulkarni**

M.Sc., Simon Fraser University, 2014

B.Math. (Hons), University of Waterloo, 2012

Thesis Submitted in Partial Fulfillment of the  
Requirements for the Degree of  
Doctor of Philosophy

in the  
Department of Mathematics  
Faculty of Science

© Avinash Kulkarni 2018  
**SIMON FRASER UNIVERSITY**  
**Fall 2018**

Copyright in this work rests with the author. Please ensure that any reproduction or re-use  
is done in accordance with the relevant national copyright legislation.

# Approval

**Name:** Avinash Kulkarni

**Degree:** Doctor of Philosophy (Mathematics)

**Title:** Aspects of the arithmetic of uniquely trigonal genus four curves:  
arithmetic invariant theory and class groups of cubic number fields

**Examining Committee:**

**Chair:** Ben Adcock  
Associate Professor

**Nils Bruin**  
Senior Supervisor  
Professor

**Nathan Ilten-Gee**  
Supervisor  
Assistant Professor

**Imin Chen**  
Internal Examiner  
Associate Professor  
Simon Fraser University

**Bianca Viray**  
External Examiner  
Associate Professor  
Department of Mathematics  
University of Washington

**Date Defended:** November 1, 2018

# Abstract

In this thesis, we study the family of uniquely trigonal genus 4 curves via their connection to del Pezzo surfaces of degree 1. We consider two different aspects of these curves. First, we show how to construct any uniquely trigonal genus 4 curve whose Jacobian variety has fully rational 2-torsion and whose trigonal morphism has a prescribed totally ramified fibre. Using this construction, we find an infinite family of cubic number fields whose class group has 2-rank at least 8. We also consider genus 4 curves that are superelliptic of degree 3, and prove sharp results on the size of the 2-torsion subgroup of their Jacobian varieties over the rationals.

Our second result is a contribution to arithmetic invariant theory. We consider the moduli space of uniquely trigonal genus 4 curves whose trigonal morphism has a marked ramification point, originally studied by Coble, from a modern perspective. We then show under a technical hypothesis how to construct an assignment from the rational points on the Jacobian variety of such a curve to a fixed orbit space that is independent of the curve. The assignment is compatible with base extensions of the field, and over an algebraically closed field our assignment reduces to the assignment of a marked (in the aforementioned sense) uniquely trigonal genus 4 curve to its moduli point. The orbit space is constructed from the split algebraic group of type E8.

**Keywords:** trigonal curve; genus 4; del Pezzo surface; arithmetic invariant theory; E8;

# Acknowledgements

I am undoubtedly one of the lucky ones for all of the wonderful people in my life.

I am indebted to Colin Weir for his friendship in the early years, and especially for the honest conversations on mathematics and about the academic life. I am grateful to my local colleagues: Brett Nasserden, Myrto Makvraki, Khoa Nguyen, and others, for the many collaborations, discussions, and friendships. I would like to thank the community at UBC for welcoming me into their seminars and courses. I am glad for the friends I have made on the west coast, and for their support over all these years. I am particularly thankful to have lived with my roommates Karin Arikushi, Dan Hepler, and Theraesa Coyle. I am thankful for the joy that you have given me, Julie Wray. I am glad for the encouragement from my family. I am thankful for the financial support from NSERC and Simon Fraser University during this degree.

Finally, I would like to thank Nils. So much of what I have done in the last six years would have been impossible without his unwavering help and support. I am sincerely appreciative for his commentary on the drafts of my preprints, which helped me to develop my writing and my ideas, as well as for our discussions about new ideas. Nils continues to be an inspiration; it has been an honor and a pleasure knowing him.

# Table of Contents

<b>Approval</b>	<b>ii</b>
<b>Abstract</b>	<b>iii</b>
<b>Acknowledgements</b>	<b>iv</b>
<b>Table of Contents</b>	<b>v</b>
<b>List of Figures</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Class groups of cubic number fields . . . . .	1
1.2 Arithmetic invariant theory . . . . .	2
1.3 Structure of the thesis . . . . .	3
<b>2 Background</b>	<b>5</b>
2.1 General background . . . . .	5
2.1.1 Notation and conventions . . . . .	5
2.2 Surfaces . . . . .	6
2.2.1 Blow-ups: generalities . . . . .	7
2.2.2 Blow-ups of surfaces . . . . .	8
2.2.3 Elliptic surfaces . . . . .	9
2.3 Places, unramified extensions, and class groups . . . . .	12
2.4 The Chevalley-Weil theorem . . . . .	16
2.4.1 Chevalley-Weil for Jacobian varieties . . . . .	16
2.5 Affine algebraic groups and categorical quotients . . . . .	19
2.6 Lie groups and Lie algebras . . . . .	22
2.6.1 Lie algebras . . . . .	23
2.6.2 Simple lie algebras . . . . .	24
2.6.3 Affine algebraic groups and Lie algebras . . . . .	28
2.6.4 Classification . . . . .	30
2.6.5 The split Lie algebra of type $E_8$ . . . . .	31
2.6.6 The split (adjoint simple) group of type $E_8$ over $k$ . . . . .	32

2.6.7	Connected components of centralizers . . . . .	32
2.6.8	Background regarding groups of type $A, D, E$ . . . . .	34
2.6.9	A representation of dimension 16 . . . . .	37
2.6.10	The refined construction of Lurie . . . . .	38
2.7	Theta groups of curves . . . . .	39
2.8	Uniquely trigonal genus 4 curves, del Pezzo surfaces of degree 1, and $E_8$ . . . . .	41
2.8.1	Del Pezzo surfaces . . . . .	41
2.8.2	Uniquely trigonal genus 4 curves . . . . .	44
<b>3</b>	<b>Class groups of cubic fields</b>	<b>47</b>
3.1	Introduction . . . . .	47
3.2	Del Pezzo surfaces, elliptic surfaces, and curves of genus 4: Applications . . . . .	47
3.3	Recovering large class groups from curves with large rational 2-torsion . . . . .	51
3.4	Families of Galois cubic fields from genus 4 curves . . . . .	56
<b>4</b>	<b>On the arithmetic of uniquely trigonal genus 4 curves and stable involutions of <math>E_8</math></b>	<b>60</b>
4.1	Introduction . . . . .	60
4.1.1	Notation and conventions . . . . .	61
4.1.2	Statement of our main results . . . . .	61
4.2	A summary of Thorne’s construction of orbits . . . . .	63
4.3	Points on maximal tori in $E_8$ . . . . .	65
4.4	Construction of orbits for the $E_8$ case . . . . .	69
4.4.1	Proof of Theorem 4.1.3 . . . . .	69
4.4.2	Proof of Theorem 4.1.4 . . . . .	71
4.5	Future directions . . . . .	73
	<b>Bibliography</b>	<b>74</b>
	<b>Appendix A Some results on theta groups</b>	<b>83</b>
A.1	Part (a): $k$ -isomorphism classes of theta groups . . . . .	84
A.2	Part (b): Representations of theta groups . . . . .	85

# List of Figures

Figure 4.1	Diagram of functors. . . . .	65
------------	------------------------------	----

# Chapter 1

## Introduction

In this thesis, we study the family of uniquely trigonal genus 4 curves from two different perspectives via their connection to del Pezzo surfaces of degree 1. Loosely, a uniquely trigonal curve is a smooth curve that has an essentially unique, branched covering map of degree 3 of the projective line  $\mathbb{P}^1$  (for the precise definition, see Section 2.8). Our first result is an application of the classical theory. We construct an infinite family of cubic number fields whose class group has a subgroup isomorphic to  $(\mathbb{Z}/2)^8$  from a particular uniquely trigonal genus 4 curve. More specifically, we show how to construct a uniquely trigonal genus 4 curve that has two technical properties required to apply a specialization technique; the technique in question is originally due to Mestre [Mes83] and a more general form is due to Bilu and Gillibert [BG18]. We follow the ideas of [BG18] while keeping track of explicit details in our calculations to obtain our result. Our second result is a contribution to arithmetic invariant theory. We show how to construct an assignment from the rational points of the Jacobian varieties of certain uniquely trigonal genus 4 curves to an orbit space constructed from the split algebraic group of type  $E_8$ . This thesis is based on the articles [Kul18a] and [Kul17], with the nexus between the family of uniquely trigonal genus 4 curves, del Pezzo surfaces of degree 1, and the algebraic group of type  $E_8$  as the unifying theme.

We describe our results in separate sections below, since they fit into two substantially different directions of research. To focus on context, we provide simplified statements of our results in the introduction.

### 1.1 Class groups of cubic number fields

The task of finding number fields with exotic class groups is an old problem. The origins of the problem go back to *Disquisitiones Arithmeticae*, where Gauss developed the subject of genus theory and showed that the class group of a quadratic number field can be arbitrarily large [Gau66]. In 1922, Nagell proved that there are infinitely many quadratic number fields whose class groups have a subgroup isomorphic to  $(\mathbb{Z}/n)$  [Nag22]. The special case of class groups of quadratic number fields has been an active research topic since then [AC55, Hon68, Yam70, Wei73]. Class groups for non-quadratic number fields have also been considered [Nak86], including a construction for cubic

number fields whose class groups have 2-rank at least 6 [Nak86]. A modern trend is to establish quantitative estimates for the number of number fields of a fixed degree and bounded discriminant whose class group has a special subgroup [Mur99, BL05]. Number fields of degree indivisible by  $p$  whose class group has a subgroup isomorphic to  $(\mathbb{Z}/p)^r$  for  $r > 2$  are difficult to exhibit in practice; even though it is conjectured by Cohen and Lenstra that these number fields have positive asymptotic density (when ordered by discriminant) [CL84].

The Jacobian variety of an algebraic curve serves as a geometric analogue of the class group of a number field. A relatively recent idea to construct infinite families of number fields of degree  $d$  whose class group contains a large subgroup of exponent  $p$  is to construct an algebraic  $d$ -gonal curve whose Jacobian variety has either  $\mu_p^r$  or  $(\mathbb{Z}/p)^r$  as a subgroup (depending on the method) and then to choose fibres over points satisfying certain local conditions. See for example [Mes83, GL12]. So far, the examples with the best yield of class group  $p$ -rank from Jacobian variety  $p$ -rank have been from curves fibred over  $\mathbb{P}_{\mathbb{Q}}^1$  with a totally ramified fibre. We construct a uniquely trigonal curve of genus 4 where the trigonal morphism has a totally ramified fibre and whose Jacobian has a fully rational 2-torsion subgroup over  $\mathbb{Q}$ . In fact, any such curve arises from our construction. We prove Theorem 3.3.9, a simplified version of which is:

**Theorem A.** *There are infinitely many cubic number fields whose class group contains  $(\mathbb{Z}/2)^8$ .*

## 1.2 Arithmetic invariant theory

A common theme in arithmetic invariant theory is to study a representation of an algebraic group, and in particular, study the arithmetic of the varieties parameterized by the invariants of the algebraic group action. Since the beginnings of arithmetic invariant theory in the early 2000's, there have been several results regarding the average number of  $k$ -rational points on certain curves and abelian varieties [BG13, BGW17, BS15, BS17, RS17, RT17, Wan13]. A landmark result in this subject regards the method of 2-decent applied to hyperelliptic curves. Given a smooth projective curve  $C$  over a field  $k$ , the method of 2-descent allows us to compute the 2-Selmer group  $\text{Sel}^{(2)}(J_C/k)$  of  $J_C$ . The 2-Selmer group of  $J_C$  contains the group  $J_C(k)/2J_C(k)$ , so in particular, the method of 2-descent allows us to compute an explicit bound for the rank of  $J_C(k)$  [HS00]. If  $C$  has a  $k$ -rational point, then the Abel-Jacobi map  $j$  embeds  $C$  into  $J_C$ . In this situation, we may use the method of two-cover descent, described in [BS09], to identify a subset of the 2-Selmer group of  $J_C$  which contains those classes in the image of  $C(k) \xrightarrow{j} J_C(k) \xrightarrow{\delta} H^1(k, J_C[2])$ .

For a hyperelliptic curve  $C/k$  with a marked rational Weierstrass point, whose model is given by

$$C: y^2 = x^{2n+1} + a_{2n-1}x^{2n-1} + \dots + a_1x + a_0$$

it was shown by Bhargava and Gross in [BG13] that there is a natural inclusion of the Selmer group of its Jacobian variety into an orbit space

$$\text{Sel}^{(2)}(J_C/k) \hookrightarrow \text{SO}_{2n+1}(q)(k) \backslash \{A \in \mathfrak{sl}_{2n+1}(k) : A = r(A)\}$$

where the special orthogonal group  $\mathrm{SO}_{2n+1}(q)(k)$  acts on  $\mathfrak{sl}_{2n+1}(k)$  on the left by conjugation,  $r$  is the reflection in the anti-diagonal, and  $q$  is the quadratic form defined by the matrix whose non-zero entries are ones on the anti-diagonal [BG13], [Tho13, Section 2.2, Example]. This result was a key step in [BG13] for calculating the average rank of the Jacobian variety of a hyperelliptic curve of genus  $g$  with a marked Weierstrass point.

The construction in [BG13] extends to a connection between the adjoint representations of groups of type  $A, D, E$  and specifically identified families of curves [Tho13, RT17] which are constructed from the invariants of these representations. In this thesis, we show how to construct a similar assignment for certain uniquely trigonal genus 4 curves. A simplified description of our main result in this direction, Theorem 4.1.4, is described as follows. We say that a uniquely trigonal genus 4 curve  $C/k$  is of *split type* if there is a morphism  $\phi: C \rightarrow \mathbb{P}^2$  defined over  $k$  such that the image of  $C$  is a curve with exactly eight singularities, each of order 3, and the degree 3 divisor of  $C$  defined by any singularity is an odd theta characteristic of  $C$ . We prove:

**Theorem B.** *Let  $q$  be the quadratic form on  $k^{16}$  defined by the symmetric matrix whose only non-zero entries are 1's on the anti-diagonal. There is an action of  $\mathrm{SO}(q)$  on an explicitly determined variety  $X$  of dimension 128 such that for every number field  $k$  and every uniquely trigonal genus 4 curve of split type  $C/k$  with a  $k$ -rational simply ramified point of the trigonal morphism, there is an inclusion*

$$\frac{J_C(k)}{2J_C(k)} \hookrightarrow \mathrm{SO}(q)(k) \backslash X(k).$$

*There is a similar assignment for the uniquely trigonal genus 4 curves of split type  $C/k$  with a  $k$ -rational totally ramified point of the trigonal morphism; in this case, there is an inclusion*

$$\frac{J_C(k)}{2J_C(k)} \hookrightarrow \mathrm{SO}(q)(k) \backslash V(k)$$

where  $V$  is a projective space of dimension 127.

The varieties  $X, V$  and the action by  $\mathrm{SO}(q)$  arise out of a construction using a particular algebraic group of type  $E_8$ . In Section 4.1, we will comment on the new features of our results.

### 1.3 Structure of the thesis

We now discuss the outline of our thesis, and in particular where the full technical statements of the results appear.

In Chapter 2 we review some background content required to prove our results in the later chapters. The aim of the chapter is to provide a helpful reference for a reader familiar with the content of Hartshorne's book [Har77] and the basics of Galois cohomology – which can be found in Serre's book [Ser02]. We believe this is useful for the reader as the proofs of our results draw on a broad range of subjects. Each section of Chapter 2 is devoted to a different subject, where we give a terse overview of the concepts and results that we need. At the end of Chapter 2, in Section 2.8,

we give the definition of a uniquely trigonal genus 4 curve and discuss the connections to del Pezzo surfaces of degree 1 and the root system of type  $E_8$ .

In Chapter 3 we prove our results regarding class groups of cubic number fields by constructing a particular uniquely trigonal genus 4 curve. The main result of this chapter is Theorem 3.3.9. We also discuss some limitations of applying this method to construct infinite families of cubic number fields of the form  $\mathbb{Q}(\sqrt[3]{n})$  whose class group contains a large subgroup of exponent 2.

In Chapter 4 we prove our results in arithmetic invariant theory. We first show how the moduli space of uniquely trigonal genus 4 curves with some additional technical data can be described in terms of Vinberg theory [Vin76]. Following that, we apply a general strategy introduced by Thorne in [Tho16] to prove our main result, Theorem 4.1.4. Chapter 4 can be read independently of Chapter 3.

Our thesis contains a single appendix. Appendix A contains a detailed proof of one of the results regarding theta groups. We chose to move these details to an appendix since the result is well-known (though we could not find the statement in the literature), the proof is somewhat technical, and the proof does not contain ideas which are important to the rest of the thesis.

# Chapter 2

## Background

### 2.1 General background

#### 2.1.1 Notation and conventions

We denote by  $k$  a subfield of the complex numbers. We denote a separable closure by  $k^{\text{sep}}$ . Since  $k$  has characteristic 0, we may identify<sup>1</sup>  $k^{\text{sep}}$  with an algebraic closure  $k^{\text{al}}$ . We denote the absolute Galois group of  $k^{\text{sep}}/k$  by  $\text{Gal}(k^{\text{sep}}/k)$ . If  $K/k$  is a finite Galois extension, then we denote the Galois group of this extension by  $\text{Gal}(K/k)$ . If  $k$  is a number field, we denote the ring of integers of  $k$  by  $O_k$ . If  $S$  is a finite set of primes in  $O_k$ , then we denote by  $O_{k,S}$  the ring of  $S$ -integers.

For a discussion of Galois cohomology we refer the reader to [Ser02]. If  $G$  is a  $\text{Gal}(k^{\text{sep}}/k)$ -module (resp.  $\text{Gal}(k^{\text{sep}}/k)$ -set), then we denote the first cohomology group (resp. pointed cohomology set) of  $\text{Gal}(k^{\text{sep}}/k)$  with coefficients in  $G$  by  $H^1(k, G)$ . We assume the terminology of [Har77] and [HS00] regarding algebraic geometry and cohomology of sheaves. We use the notation  $X/k$  to indicate that  $X$  is a scheme defined over  $k$ , and we let  $X_{k^{\text{sep}}} := X \times_k k^{\text{sep}}$ . If  $R$  is a  $k$ -algebra, we denote the set of  $R$ -points of  $X/k$  by  $X(R)$ . We mean  $k$ -rational whenever the term rational is used.

We let  $\mathbf{Set}$  be the category of sets and let  $\mathbf{k}\text{-alg}$  be the category of  $k$ -algebras. For a description of functors to  $\mathbf{Set}$  representable by a scheme, see [SP, Tag 01JF]. If  $f_1, \dots, f_m \in k[x_1, \dots, x_n]$  are (weighted homogeneous) polynomials, we denote the subscheme of  $\mathbb{A}_k^n$  (resp.  $\text{Proj } k[x_1, \dots, x_n]$ ) that is the common zero-locus of  $f_1, \dots, f_m$  by  $Z(f_1, \dots, f_m)$ . For a discussion of moduli problems, moduli functors, and moduli spaces, we refer the reader to [HM98, Chapter 1A].

For a finitely generated abelian group  $M$ , we denote the free rank as a  $\mathbb{Z}$ -module by  $\text{rk } M$ . Additionally, we denote the 2-torsion of  $M$  by  $M[2]$  and denote  $\text{rk}_2 M[2]$  to be the rank of  $M[2]$  as a  $(\mathbb{Z}/2)$ -module.

In general, we allow a variety to be reducible, though we assume curves and surfaces are irreducible. If  $X$  is a smooth variety defined over a field  $k$  then we denote the class of the canonical

<sup>1</sup>We make an effort to distinguish  $k^{\text{sep}}$  and  $k^{\text{al}}$  in our exposition anyway. It is potentially interesting to consider if the results of this thesis can be adapted to when  $k = \mathbb{F}_q(t)$ .

divisor by  $\kappa_X$  and call  $-\kappa_X$  the *anti-canonical* class. By abuse of notation we often denote a canonical divisor of  $X$  by  $\kappa_X$  as well.

If  $C/k$  is a smooth algebraic curve, then we denote by  $\text{Div}(C/k)$  the group of divisors of  $C$  defined over  $k$  and we denote the subgroup of divisors of degree 0 defined over  $k$  by  $\text{Div}^0(C/k)$ . We denote the Picard variety of  $C/k$  by  $\text{Pic}^0(C)$  and the group of  $k$ -rational points of the Picard variety is denoted by  $\text{Pic}^0(C)(k)$ . Since we insist that  $\text{Pic}^0(C)$  has the structure of a variety over  $k$ , there is generally only an inclusion  $\text{Div}^0(C/k)/\text{Princ}(C/k) \hookrightarrow \text{Pic}^0(C)(k)$  rather than an isomorphism [Mil86b, Remark 1.6]. Our main results concern curves over  $k$  which have a  $k$ -rational point, so the aforementioned technicality does not play a significant role in this thesis. For simplicity, we identify the Jacobian variety of  $C$  and the Picard variety of  $C$ . We denote the Jacobian variety of  $C$  by  $J_C$ .

By a  $k$ -group, we mean a group variety  $G/k$ . If  $G/k$  is an abelian  $k$ -group, then the group  $G(k^{\text{sep}})$  has the structure of a Galois module. In general,  $G(k^{\text{sep}})$  has the structure of a pointed  $\text{Gal}(k^{\text{sep}}/k)$ -set. If  $G/k$  is a finite abelian  $k$ -group then we abbreviate  $H^1(k, G(k^{\text{sep}}))$  to  $H^1(k, G)$ . If  $G/k$  is a group variety acting on a scheme  $X/k$  on the left, we denote the set of  $G(k)$ -orbits of  $X(k)$  by  $G(k)\backslash X(k)$ . It will be clear from context that we do not mean a set difference.

## 2.2 Surfaces

**Definition 2.2.1.** A *surface* over  $k$  is an irreducible projective  $k$ -variety of dimension 2.

Note that we allow singular surfaces for the purposes of giving a more standard treatment of elliptic surfaces. However, we focus our exposition on smooth surfaces since these are what our arguments in Chapter 3 and Chapter 4 require.

**Theorem 2.2.2.** *Let  $X/k$  be a smooth projective surface. There is a unique bilinear pairing*

$$\langle C, D \rangle: \text{Div}(X) \times \text{Div}(X) \rightarrow \mathbb{Z}$$

such that the following hold:

- If  $C, D$  are smooth curves on  $X$  meeting transversally, then  $\langle C, D \rangle = \#(C \cap D)(k^{\text{al}})$ .
- For all  $C, D \in \text{Div}(X)$ , we have  $\langle C, D \rangle = \langle D, C \rangle$ .
- If  $C_1$  is linearly equivalent to  $C_2$ , then  $\langle C_1, D \rangle = \langle C_2, D \rangle$ .

Moreover, the pairing  $\langle \cdot, \cdot \rangle$  descends to a well-defined symmetric bilinear pairing  $\langle \cdot, \cdot \rangle: \text{Pic}(X) \times \text{Pic}(X) \rightarrow \mathbb{Z}$ .

*Proof.* See [Har77, Theorem V.1.1]. □

**Definition 2.2.3.** For a smooth projective surface  $X$ , we call the unique pairing identified in Theorem 2.2.2, on either  $\text{Div}(X)$  or  $\text{Pic}(X)$ , the *intersection pairing*.

In light of Definition 2.2.3, we say that a set of (possibly reducible) curves  $\{C_1, \dots, C_n\}$  on a smooth surface  $X$  are *pairwise orthogonal* if they are pairwise orthogonal with respect to the intersection pairing.

**Definition 2.2.4.** Let  $X/k$  be a smooth surface and let  $e \subseteq X$  be an irreducible curve on  $X$  such that  $\langle e, e \rangle = -1$ . Then we call  $e$  an *exceptional curve* of  $X$ .

The exceptional curves of a smooth surface  $X$  are related to certain birational morphisms with domain  $X$ . In the following sections, we describe this connection more precisely as it is critical in Chapter 3.

### 2.2.1 Blow-ups: generalities

**Theorem 2.2.5.** Let  $X$  be a variety over  $k$ , let  $Y \subseteq X$  be a zero-dimensional subscheme, and let  $\mathcal{I}_Y$  be the ideal sheaf associated to  $Y$  as a closed subscheme of  $X$ . There exists a scheme  $\text{Bl}_Y X$  and a proper morphism  $\pi: \text{Bl}_Y X \rightarrow X$  such that  $\pi^{-1}\mathcal{I}_Y \cdot \mathcal{O}_{\text{Bl}_Y X}$  is invertible and such that  $\text{Bl}_Y X$  satisfies the following universal property:

For any morphism  $f: Z \rightarrow X$  such that  $f^{-1}\mathcal{I}_Y \cdot \mathcal{O}_Z$  is an invertible sheaf, there exists a morphism  $g$  such that the diagram

$$\begin{array}{ccc} Z & \xrightarrow{g} & \text{Bl}_Y X \\ & \searrow f & \downarrow \pi \\ & & X \end{array}$$

commutes. By the universal property,  $\text{Bl}_Y X$  is unique up to isomorphism.

*Proof.* See [Har77, Proposition II.7.14]. Note that [Har77] generally assumes an algebraically closed base field, but the proof for general  $k$  is identical.  $\square$

**Definition 2.2.6.** With the notation of Theorem 2.2.6, we define  $\text{Bl}_Y X$  to be the *blow-up* of  $X$  at  $Y$ , and we call  $\pi$  the *blow-down* morphism. The invertible sheaf  $\pi^{-1}\mathcal{I}_Y \cdot \mathcal{O}_{\text{Bl}_Y X}$  viewed as a Cartier divisor, or as a Weil divisor, is called the *exceptional divisor* of the blow-up.

Note that Definition 2.2.6 can be made in a more general setting. A particularly important example of Definition 2.2.6 is when  $Y$  is a single reduced point  $p$ . In our specific setting, we enjoy the following properties.

**Proposition 2.2.7.** Let  $X/k$  be a variety and let  $Y \subseteq X$  be a zero-dimensional subscheme. Then:

- (a)  $\text{Bl}_Y X$  is a variety over  $k$ .
- (b)  $\pi: \text{Bl}_Y X \rightarrow X$  is birational, proper, and surjective.
- (c) if  $X$  is quasi-projective (resp. projective), then so is  $\text{Bl}_Y X$ , and  $\pi$  is a projective morphism.

*Proof.* See [Har77, Proposition II.7.16]. Note that [Har77] generally assumes an algebraically closed base field, but the proof for general  $k$  is identical.  $\square$

Proposition 2.2.7 allows us to make the following definition.

**Definition 2.2.8.** Let  $Y \subseteq X$  be a zero-dimensional subscheme of  $X$  and let  $\pi: \text{Bl}_Y X \rightarrow X$  be the blow-down morphism. The birational inverse to  $\pi$  is called the *blow-up map*.

**Definition 2.2.9.** Let  $X$  be a variety, let  $Y \subseteq X$  be a zero-dimensional subscheme, and let  $i: Z \hookrightarrow X$  be any subvariety of  $X$ . Let  $U := Z \setminus i^{-1}Y$ , let  $i_U$  be the restriction of  $i$  to  $U$ , and observe that  $i_U^{-1}\mathcal{O}_Y$  is invertible. By the universal property of blowing up, we have that there is an inclusion  $j: U \hookrightarrow \text{Bl}_Y X$ . We define the *strict transform* of  $Z$  to be the closure of  $j(U)$  in  $\text{Bl}_Y X$ .

There is an important corollary of the universal property for blow-ups that allows us to resolve the indeterminacy locus of certain rational maps.

**Proposition 2.2.10.** Let  $X/k$  be a projective variety, let  $\mathfrak{d}$  be a linear system on  $X$  whose scheme of base points  $Y$  is zero-dimensional, and let  $f: X \dashrightarrow \mathbb{P}^n$  be the rational map on  $X$  defined by  $\mathfrak{d}$ . Then there exists a morphism  $g: \text{Bl}_Y X \rightarrow \mathbb{P}^n$  such that the diagram

$$\begin{array}{ccc} \text{Bl}_Y X & & \\ \pi \downarrow & \searrow g & \\ X & \dashrightarrow f & \mathbb{P}^n \end{array}$$

commutes.

*Proof.* See [Har77, Example 3.17.3]. □

**Proposition 2.2.11.** Let  $X$  be a variety, let  $p$  be a point on  $X$  such that the associated scheme has codimension at least 2 and such that every divisor class has a representative whose support avoids  $p$ , and let  $e_p$  be the exceptional divisor of the blow-up  $\pi: \text{Bl}_p X \rightarrow X$ . Then the pull-back  $\pi^*: \text{Pic}(X) \rightarrow \text{Pic}(\text{Bl}_p X)$  is injective and

$$\text{Pic}(\text{Bl}_p X) = \mathbb{Z}[e_p] \oplus \pi^* \text{Pic}(X).$$

*Proof.* See [Har77, Exercise II.8.5]. □

## 2.2.2 Blow-ups of surfaces

The operation of blowing up a surface at a single point is useful in Section 2.8, and it is helpful for us to have a specific name for this operation.

**Definition 2.2.12.** If  $f: \tilde{X} \rightarrow X$  is a morphism over  $k$  such that there exists a point  $p \in X(k^{\text{al}})$  and an isomorphism  $g: \tilde{X} \rightarrow \text{Bl}_p X$  making

$$\begin{array}{ccc} \tilde{X} & \xrightarrow{g} & \text{Bl}_p X \\ & \searrow f & \downarrow \\ & & X \end{array}$$

commute, then  $f$  is said to be a *monoidal transformation*.

**Proposition 2.2.13.** Let  $X/k$  be a smooth surface and let  $p \in X(k)$  be a point. Then  $\text{Bl}_p X$  is a smooth surface over  $k$ . The exceptional divisor of the blow-up is a curve  $e$  isomorphic to  $\mathbb{P}^1$  and satisfies  $\langle e, e \rangle = -1$ .

*Proof.* See [Har77, Proposition V.3.1]. □

**Proposition 2.2.14.** Let  $f: Y \rightarrow X$  be a morphism of smooth surfaces over  $k^{\text{al}}$  with a birational inverse  $g$ . Then  $f$  can be factored into finitely many monoidal transformations.

*Proof.* See [Har77, Corollary V.5.4]. □

### 2.2.3 Elliptic surfaces

For our exposition on elliptic surfaces, we largely draw from [Sil94].

**Definition 2.2.15.** Let  $C/k$  be a smooth curve. An *elliptic surface* over  $C$  defined over  $k$  consists of the following data:

- a (possibly singular) surface  $\mathcal{E}$ .
- a morphism  $\pi: \mathcal{E} \rightarrow C$  defined over  $k$  such that for all but finitely many  $t \in C(k^{\text{al}})$ , the fibre

$$\mathcal{E}_t = \pi^{-1}(t)$$

is a smooth curve of genus 1.

- a section  $\sigma_0: C \rightarrow \mathcal{E}$  to  $\pi$ .

To abbreviate the defining data for an elliptic surface, we use the phrase “Let  $\pi: \mathcal{E} \rightarrow C$  be an elliptic surface”. If  $C/k$  is a curve over  $k$ , then  $\mathcal{E}$  is a  $k$ -variety as well; we use the phrase “Let  $\pi: \mathcal{E} \rightarrow C$  be an elliptic surface over  $k$ ” in place of “Let  $C/k$  be a curve and let  $\pi: \mathcal{E} \rightarrow C$  be an elliptic surface over  $C$ ”.

**Definition 2.2.16.** Let  $\pi: \mathcal{E} \rightarrow C$  be an elliptic surface over  $k$ , and let  $t \in C(k^{\text{al}})$ . Then  $\mathcal{E}_t = \pi^{-1}(t)$  is called a *special fibre* of the elliptic surface. If  $\text{Spec } k(C)$  is the generic point of  $C$ , then we call  $\mathcal{E}_{k(C)} := \mathcal{E} \times_C \text{Spec } k(C)$  the *generic fibre* of the elliptic surface.

**Definition 2.2.17.** Let  $\pi: \mathcal{E} \rightarrow C$  be an elliptic surface. A *multi-section* of  $\mathcal{E}$  is a curve  $M \subseteq \mathcal{E}$  such that the morphism  $\pi: M \rightarrow C$  is finite.

## Minimal models

At this point, we would like to define what it means for an elliptic surface  $\pi: \mathcal{E} \rightarrow C$  to have “\_\_\_\_\_ reduction at  $t \in C(k^{\text{al}})$ ”. The naive approach would be to classify the reduction type in terms of the isomorphism class of  $\mathcal{E}_t$ . The standard classification (as in [Sil94, Chapter IV.9]) requires that a well-behaved model for  $\mathcal{E}$  be chosen first. For simplicity, we only make these definitions for smooth minimal elliptic surfaces.

**Definition 2.2.18.** An elliptic surface  $\pi: \mathcal{E} \rightarrow C$  is *minimal (over  $C$ )* if for any commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\phi} & \mathcal{E} \\ & \searrow f & \downarrow \pi \\ & & C, \end{array}$$

where  $f: S \rightarrow C$  is an elliptic surface and  $\phi$  is a birational map, we have that  $\phi$  extends to a morphism over  $C$ .

We need a slightly more general definition of minimality since we momentarily wish to consider varieties over Dedekind domains; we do this in order to follow [Sil94]. In particular, we define what it means to be minimal for certain subschemes of an elliptic surface.

**Definition 2.2.19.** Let  $C/k$  be a smooth curve over  $k$ , let  $R \subseteq k(C)$  be a local Dedekind domain containing  $k$  whose field of fractions is  $k(C)$ . Let  $\mathcal{E}_R := \mathcal{E} \times_C \text{Spec } R$ . We say that  $\mathcal{E}_R$  is *minimal (over  $\text{Spec } R$ )* if for any commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\phi} & \mathcal{E}_R \\ & \searrow f & \downarrow \pi \\ & & \text{Spec } R, \end{array}$$

where  $S$  is an integral scheme of dimension 2 over  $k$ ,  $f: S \rightarrow \text{Spec } R$  is proper, and  $\phi$  is a birational map over  $\text{Spec } R$ , we have that  $\phi$  extends to a morphism over  $\text{Spec } R$ .

Note that the  $S$  appearing in Definition 2.2.19 is not necessarily a variety as  $S$  may not be of finite type over  $k$ . We apply the “Spreading out theorem” [Poo17, Theorem 3.2.1, Remark 3.2.2] to replace the base  $\text{Spec } R$  by an open subscheme of  $C$ .

**Lemma 2.2.20.** Let  $R$ , and  $\mathcal{E}_R$  be as in Definition 2.2.19. Let

$$\begin{array}{ccc} S & \xrightarrow{\phi} & \mathcal{E}_R \\ & \searrow f & \downarrow \pi \\ & & \text{Spec } R, \end{array}$$

be a commutative diagram with  $S$  an integral scheme of dimension 2 over  $k$ ,  $f: S \rightarrow \text{Spec } R$  a proper morphism, and  $\phi$  a birational map over  $\text{Spec } R$ . Then there is a commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\phi} & \mathcal{E}_B \\ & \searrow f & \downarrow \pi \\ & & B, \end{array}$$

where  $S$  is an open subscheme of a surface,  $B$  is an open subscheme of  $C$ , and  $\phi$  a birational map over  $B$ .

*Proof.* Applying [Pool17, Theorem 3.2.1, Remark 3.2.2], we obtain a commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\phi} & \mathcal{E}_B \\ & \searrow f & \downarrow \pi \\ & & B, \end{array}$$

where  $B$  is an open subscheme of  $C$  containing  $\text{Spec } R$ ,  $f$  is proper, and  $\phi$  a morphism over  $B$ . It remains to check that  $\phi$  is birational. Let  $K := k(C)$ , and note that  $K$  is also the fraction field of  $\text{Spec } R$  by definition. We have that  $\phi_K: S_K \rightarrow \mathcal{E}_K$  is an isomorphism over  $\text{Spec } K$ , and admits an inverse  $\phi_K^{-1}: \mathcal{E}_K \rightarrow S_K$ . Applying [Pool17, Theorem 3.2.1, Remark 3.2.2] to  $\phi_K^{-1}$  gives a birational inverse to  $\phi$  over  $B$ .  $\square$

**Lemma 2.2.21.** *Let  $\pi: \mathcal{E} \rightarrow C$  be a minimal elliptic surface and assume that  $\mathcal{E}$  is smooth. If  $R$  is a local Dedekind domain containing  $k$  such that  $i: \text{Spec } R \rightarrow C$  is an inclusion and  $k(C)$  is the field of fractions of  $R$ , then*

$$\pi_R: \mathcal{E} \times_C \text{Spec } R \rightarrow \text{Spec } R$$

*is proper,  $\mathcal{E} \times_C \text{Spec } R$  is regular, and  $\mathcal{E} \times_C \text{Spec } R$  is minimal.*

*Proof.* By Lemma 2.2.19, we may replace  $\text{Spec } R$  by an open subscheme  $B$  of  $C$  containing  $\text{Spec } R$ . Denote  $\mathcal{E}_B := \mathcal{E} \times_C B$ . Note that properness is preserved by base change. Smoothness is preserved under base change by an open immersion, and if  $\mathcal{E}_B$  is smooth then it is certainly regular. To prove minimality, let

$$\begin{array}{ccc} S & \xrightarrow{\phi} & \mathcal{E}_B \\ & \searrow f & \downarrow \pi \\ & & B \end{array}$$

be as in Definition 2.2.19. By Nagata's compactification theorem [Con07], there exists a proper morphism  $g: \hat{S} \rightarrow C$  and an open inclusion  $j: S \hookrightarrow \hat{S}$  such that the diagram

$$\begin{array}{ccc} S & \xrightarrow{j} & \hat{S} \\ f \downarrow & & \downarrow g \\ B & \xrightarrow{i} & C \end{array}$$

commutes. We now have that  $\phi \circ j^{-1}: \hat{S} \rightarrow \mathcal{E}$  is a birational map of surfaces that is proper over  $C$ , so it extends to a morphism  $\hat{\phi}$  by minimality of  $\mathcal{E}$ . The composition  $\hat{\phi} \circ j$  is a morphism. As  $\hat{\phi} \circ j$  restricts to a morphism over  $\text{Spec } R$  and we are done.  $\square$

**Remark 2.2.22.** We have shown in Lemma 2.2.21 that a smooth minimal elliptic surface is its own minimal proper regular model for all of the special fibres [Sil94, Theorem 4.5]. For further information on this topic, we direct the reader to [Sil94, Chapter IV].

We use [Sil94, Theorem 8.2] to make the following definition.

**Definition 2.2.23.** Let  $\pi: \mathcal{E} \rightarrow C$  be an elliptic surface over  $k$  such that  $\mathcal{E}$  is smooth and minimal. If  $\mathcal{E}_t$  is a special fibre, we say that it is *good* if it is a smooth  $k$ -variety and say that it is a *bad* fibre otherwise. Similarly we say that  $\mathcal{E}$  has *good reduction at*  $t \in C(k^{\text{al}})$  if  $\mathcal{E}_t$  is smooth and we say that it has *bad reduction at*  $t$  if not.

Let  $t \in C(k^{\text{al}})$  be a point such that  $\mathcal{E}_t$  is a bad fibre. We say that  $\mathcal{E}$  has *multiplicative reduction at*  $t$  if  $\mathcal{E}_t$  is isomorphic to either a rational curve with a node, or consists of  $n$  non-singular rational curves that can be labelled  $F_1, \dots, F_n$  such that

$$\langle F_i, F_j \rangle = \begin{cases} 1 & \text{if } i - j \equiv \pm 1 \pmod{n} \\ -2 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases},$$

and we say that  $\mathcal{E}$  has *additive reduction at*  $t$  otherwise.

## 2.3 Places, unramified extensions, and class groups

In this section we review the description of ramification of number fields in terms of discrete valuations and absolute values. At the end of this section we state an important result from algebraic number theory. We generally follow [BG06, Chapter 1].

**Definition 2.3.1.** Let  $|\cdot|_1, |\cdot|_2$  be two absolute values on a field  $K$ . We say they are *equivalent* if they define the same topology.

If  $K$  is a field, there is always an equivalence class of trivial absolute values defined by

$$|x| = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{otherwise} \end{cases}.$$

We exclude trivial absolute values from our considerations.

**Proposition 2.3.2.** *Two absolute values  $|\cdot|_1, |\cdot|_2$  on a field  $K$  are equivalent if and only if there is a positive real number  $s$  such that*

$$|x|_1 = |x|_2^s$$

for all  $x \in K$ .

*Proof.* See [BG06, Proposition 1.2.3]. □

**Definition 2.3.3.** A *place* of  $K$  is an equivalence class of non-trivial absolute values. For a place  $\nu$  of  $K$ , we denote by  $|\cdot|_\nu$  an absolute value in the equivalence class  $\nu$ .

**Definition 2.3.4.** Let  $L/K$  be an extension of fields. We say that a place  $w$  of  $L$  *extends* a place  $\nu$  of  $K$  if the restriction of any representative of  $w$  is a representative of  $\nu$ .

**Proposition 2.3.5.** *Let  $K$  be a field complete with respect to an absolute value  $|\cdot|_\nu$  and let  $L/K$  be a finite extension. Then there is a unique extension of  $|\cdot|_\nu$  to an absolute value  $|\cdot|_w$  of  $L$ . For any  $x \in L$  the equation*

$$|x|_w = \left| N_{L/K}(x) \right|_\nu^{\frac{1}{[L:K]}}$$

holds, where  $N_{L/K}$  is the relative norm. Moreover, the field  $L$  is complete with respect to  $|\cdot|_w$ .

*Proof.* See [BG06, Proposition 1.2.7]. □

**Definition 2.3.6.** A non-trivial absolute value  $|\cdot|$  on a field  $K$  is *non-archimedean* if for any  $x, y \in K$  we have that  $|x + y| \leq \max\{|x|, |y|\}$ . Otherwise, we say that  $|\cdot|$  is *archimedean*. A place  $\nu$  is *non-archimedean* if some (equivalently, any) representative is non-archimedean. Otherwise, we say  $\nu$  is *archimedean*.

We state the following theorem mainly for ease of terminology.

**Theorem 2.3.7** (Ostrowski). *The  $p$ -adic absolute values are a set of distinct representatives for the non-archimedean places of  $\mathbb{Q}$ . Furthermore, there is a unique archimedean place of  $\mathbb{Q}$ , and the classical absolute value is a representative of this place.*

*Proof.* See [BG06, Example 1.2.5]. □

If  $K/\mathbb{Q}$  is a number field and  $\nu$  is a place of  $K$ , we say that  $\nu$  is an *infinite place* if  $\nu$  restricts to an archimedean place of  $\mathbb{Q}$  and we say it is a *finite place* if  $\nu$  restricts to a non-archimedean place of  $\mathbb{Q}$ . In analogy with the case of  $K = \mathbb{Q}$ , we refer to the archimedean places of  $K$  as the *infinite primes* and refer to the non-archimedean places as the *finite primes*.

**Definition 2.3.8.** Let  $L/K$  be a finite extension and let  $|\cdot|_w$  be an absolute value extending a non-archimedean absolute value  $|\cdot|_\nu$ . The *value group* of  $\nu$  is the group  $|K^\times|_\nu$ . The index of  $|K^\times|_\nu$  in  $|L^\times|_w$  is called the *ramification index*  $e_{w/\nu}$  of  $w$  in  $\nu$ . We say that  $\nu$  is *discrete* if the value group  $|K^\times|_\nu$  is cyclic.

Let  $L/K$  be a finite extension and let  $\nu$  be a non-archimedean place of  $K$ . There is a canonical dense inclusion  $i: K \hookrightarrow K_\nu$ , where  $K_\nu$  denotes the completion of the field  $K$  with respect to the topology induced by  $\nu$ . If  $w$  is a place of  $L$  extending  $\nu$ , then there is a canonical dense inclusion  $j: L \hookrightarrow L_w$ . The restriction of  $w$  to  $K$  is  $\nu$ , so  $w$  and  $\nu$  induce the same topology on  $K$ . In particular, the topological closure of  $j(K)$  in  $L_w$  is canonically isomorphic to  $K_\nu$ . Moreover, the degree of the extension  $L_w/K_\nu$  is at most  $[L : K]$ , and the diagram

$$\begin{array}{ccc} L & \xrightarrow{j} & L_w \\ \cup & & \cup \\ K & \xrightarrow{i} & K_\nu \end{array}$$

commutes. See [BG06, Proposition 1.3.1] for further details.

**Proposition 2.3.9.** *Let  $L/K$  be a finite extension and let  $w$  be a place extending a non-archimedean place  $\nu$  of  $K$ . Then:*

- (a) *The ramification index is independent of the choice of representatives for  $w$  and  $\nu$ .*
- (b) *The ramification index does not change if we pass to completions.*
- (c) *The ramification index is at most  $[L : K]$ .*

*Proof.* See [BG06, Proposition 1.2.11]. □

**Definition 2.3.10.** Let  $L/K$  be a finite extension of number fields and let  $w$  be a non-archimedean place of  $L$  extending a place  $\nu$  of  $K$ . We say that the extension  $L/K$  is *ramified at  $w$*  if  $e_{w/\nu} > 1$  and say it is *unramified* otherwise. We say that the extension is *ramified over  $\nu$*  if there is a place  $w$  extending  $\nu$  which is ramified and say it is *unramified over  $\nu$*  otherwise.

At this point, we turn our attention to ramification for the archimedean places. There are multiple conventions regarding this topic [Neu99, Section III.3]. We adopt the convention present in [BG18].

**Definition 2.3.11.** Let  $L/K$  be a finite extension of number fields and let  $w$  be an archimedean place of  $L$  extending a place  $\nu$  of  $K$ . We say that the extension  $L/K$  is *ramified at  $w$*  if  $L_w = \mathbb{C}$  and  $K_\nu = \mathbb{R}$ , and we say the extension is *unramified at  $w$*  otherwise. We say that the extension is *ramified over  $\nu$*  if there is a place  $w$  extending  $\nu$  which is ramified and say it is *unramified over  $\nu$*  otherwise.

**Definition 2.3.12.** We say that an extension  $L/K$  is *unramified* if it is unramified over  $\nu$  for each place  $\nu$  of  $K$ . If  $S$  is a finite set of places of  $K$ , we say that the extension  $L/K$  is *unramified outside  $S$*  if for each  $\nu \notin S$  we have that the extension is unramified over  $\nu$ .

A convenient tool for calculating whether a place is ramified in an extension is the inertia group. Note that if  $L/K$  is Galois and  $w$  is a place of  $L$ , then  $L_w/K_\nu$  is also Galois and there is a natural inclusion  $\text{Gal}(L_w/K_\nu) \hookrightarrow \text{Gal}(L/K)$  whose image contains any  $\sigma \in \text{Gal}(L/K)$  continuous with respect to  $w$ .

**Definition 2.3.13.** Let  $L/K$  be a Galois extension and let  $w$  be a place extending a non-archimedean place  $\nu$ . We define the *decomposition group* of  $w$  over  $\nu$  to be

$$D_{w|\nu} = \{\sigma \in \text{Gal}(L/K) : |\sigma(x)|_w = |x|_w \text{ for all } x \in L_w\}.$$

The subgroup of  $D_{w|\nu}$  defined by

$$I_{w|\nu} = \{\sigma \in D_{w|\nu} : |\sigma(x) - x|_w < 1 \text{ for all } x \in O_L\}.$$

is called the *inertia group* of  $w$  over  $\nu$ . If  $\nu$  is clear from context, we write  $D_w$  and  $I_w$  instead.

Note by Proposition 2.3.2 that the decomposition and inertia groups are independent of the choice of absolute value  $|\cdot|_w$  in  $w$ . It is helpful to have a notion of the inertia group for an extension of archimedean places as well.

**Definition 2.3.14.** Let  $L/K$  be a Galois extension and let  $w$  be a place extending an archimedean place  $\nu$ . We define the *inertia group* of  $w$  over  $\nu$  to be the image of  $\text{Gal}(L_w/K_\nu)$  in  $\text{Gal}(L/K)$ . We denote the inertia group by  $I_{w|\nu}$ , or simply by  $I_w$ .

If  $L/K$  is a Galois extension and  $w$  is archimedean, then  $L_w/K_\nu$  is one of three possible extensions: either  $\mathbb{R}/\mathbb{R}$ ,  $\mathbb{C}/\mathbb{R}$ , or  $\mathbb{C}/\mathbb{C}$ . Moreover, we have that  $I_w \cong \text{Gal}(L_w/K_\nu)$  is either trivial or generated by complex conjugation.

**Proposition 2.3.15.** *Let  $L/K$  be a Galois extension and let  $w$  be a place extending a place  $\nu$ . Then  $L/K$  is unramified at  $w$  if and only if  $I_w$  is trivial.*

*Proof.* If  $w$  is non-archimedean, the result can be found at [Neu99, Proposition II.9.11]. The result in the archimedean case is a consequence of Definition 2.3.11.  $\square$

The following theorem is a central result of class field theory, and it allows us to generate classes in the class group of a number field by exhibiting a specific type of field extension.

**Theorem 2.3.16.** *Let  $L/K$  be an unramified abelian Galois extension of number fields. Then  $\text{Gal}(L/K)$  is isomorphic to a subgroup of  $\text{Cl}(K)$ .*

*Proof.* See [Neu99, p. 399], and in particular [Neu99, Proposition VI.6.9].  $\square$

## 2.4 The Chevalley-Weil theorem

In this section we discuss some versions of the Chevalley-Weil theorem. The description of results in Section 2.4.1 are particularly useful to us in Chapter 3. A morphism  $f: A \rightarrow B$  of local rings is *unramified* if  $\mathfrak{m}_B = B \cdot f(\mathfrak{m}_A)$  and the induced extension of residue fields  $(B/\mathfrak{m}_B)/(A/\mathfrak{m}_A)$  is finite and separable – here  $\mathfrak{m}_A, \mathfrak{m}_B$  denote the maximal ideals of  $A, B$  respectively. A morphism of varieties  $f: Y \rightarrow X$  over  $k$  is *unramified* if for every  $y \in Y(k^{\text{al}})$  we have that the induced morphism of local rings  $f^*: \mathcal{O}_{X, f(y)} \rightarrow \mathcal{O}_{Y, y}$  is unramified.

**Theorem 2.4.1.** *Let  $k$  be a number field and let  $f: Y \rightarrow X$  be an unramified finite morphism of  $k$ -varieties. If  $X$  is complete, then there is a non-zero  $\alpha \in O_k$  such that for any  $P \in Y(k^{\text{al}})$  and  $Q := f(P)$  the discriminant  $\mathfrak{d}_{P/Q}$  of  $O_{k(P)}$  over  $O_{k(Q)}$  contains  $\alpha$ .*

*Proof.* See [BG06, Theorem 10.3.7]. □

We obtain the immediate corollary:

**Corollary 2.4.2.** *Let  $k$  be a number field and let  $f: Y \rightarrow X$  be an unramified finite morphism of  $k$ -varieties, where  $X$  is complete. Then there is a finite set of places  $S$  of  $k$ , dependent only on  $f$ , such that for any  $P \in Y(k^{\text{al}})$  with  $f(P) \in X(k)$ , the set of places of  $k(P)$  where the extension  $k(P)/k$  is ramified is contained in the set of places of  $k(P)$  extending the places in  $S$ .*

*Proof.* In the set-up of Theorem 2.4.1, the only primes over which  $k(P)/k$  can ramify are either archimedean or contain  $\alpha$ . □

### 2.4.1 Chevalley-Weil for Jacobian varieties

We state an explicit version of Corollary 2.4.2 for the Jacobian variety of a curve that allows us to both compute the finite set of places over which there is possibly ramification, as well as provide explicit conditions to tell when the extension  $k(P)/k$  is unramified. In this section, we let  $k$  be a number field and we let  $C/k$  be a smooth projective curve of genus  $g$  and let  $J_C$  be its Jacobian. Note that the multiplication-by-2 morphism on  $J_C$  is separable [Mil86a, Theorem 8.2]. Finally, we let  $\tilde{S}$  denote the finite set of places of  $k$  which are either places of bad reduction for  $C$ , places dividing 2, or are archimedean places.

**Proposition 2.4.3.** *For any  $y \in J_C(k^{\text{sep}})$  such that  $[2]y \in J_C(k)$  we have that  $k(y)/k$  is unramified outside of  $\tilde{S}$ .*

*Proof.* See [HS00, Proposition C.1.5]. □

Following [Sch98, Section 2.2], we state an analogue for Proposition 2.4.3 for the primes in  $\tilde{S}$ .

**Theorem 2.4.4.** *Define*

$$\langle \cdot, \cdot \rangle: \frac{J_C(k)}{2J_C(k)} \times \text{Gal}(k^{\text{sep}}/k) \rightarrow J_C[2](k^{\text{sep}})$$

by  $\langle x, \sigma \rangle \mapsto [y^\sigma - y]$ , where  $y \in J_C(k^{\text{sep}})$  is any element such that  $[2]y = x$ . We have that  $\langle \cdot, \cdot \rangle$  is linear in the first factor and that the left kernel is trivial. Additionally, we have that  $\langle x, \sigma\tau \rangle = \langle x, \sigma \rangle^\tau \langle x, \tau \rangle$  for all  $x \in \frac{J_C(k)}{2J_C(k)}$  and  $\sigma, \tau \in \text{Gal}(k^{\text{sep}}/k)$ . In particular, if  $J_C[2](k) = J_C[2](k^{\text{sep}})$ , then  $\langle \cdot, \cdot \rangle$  is a bilinear pairing.

*Proof.* See [HS00, Proposition C.1.2]. □

The mapping in Theorem 2.4.4 is called the *Kummer pairing*. We see for any  $x \in \frac{J_C(k)}{2J_C(k)}$  that  $\langle x, \cdot \rangle$  defines an element of  $H^1(k, J_C[2])$ , so the Kummer pairing induces a morphism of abelian groups

$$\delta: \frac{J_C(k)}{2J_C(k)} \rightarrow H^1(k, J_C[2]).$$

If  $\text{rk}_2 J_C[2](k) = 2g$ , or equivalently, if  $J_C[2](k^{\text{sep}})$  is a trivial Galois module, then we may use  $\delta$  to modify the Kummer pairing to be more amenable to computation.

Let  $T \in J_C[2](k)$  and let  $w: J_C[2] \times J_C[2] \rightarrow \mu_2$  be the Weil-pairing. Both  $J_C[2](k^{\text{sep}})$  and  $\mu_2$  are trivial  $\text{Gal}(k^{\text{sep}}/k)$ -modules, and we have a morphism of abelian groups

$$b: \text{Hom}_{\text{Gal}(k^{\text{sep}}/k)}(J_C[2](k^{\text{sep}}), \mu_2) \rightarrow \text{Hom}(H^1(k, J_C[2]), H^1(k, \mu_2))$$

by functoriality of  $H^1(k, -)$ . The Weil pairing determines a morphism of Galois modules  $\lambda: J_C[2](k) \rightarrow \text{Hom}_{\text{Gal}(k^{\text{sep}}/k)}(J_C[2](k^{\text{sep}}), \mu_2)$ . The composition  $\psi := b(\lambda(-))$  gives us the pairing

$$w'(\cdot, \cdot): \begin{array}{ccc} H^1(k, J_C[2]) \times J_C[2](k) & \rightarrow & k^\times / k^{\times 2} \\ (\xi, T) & \mapsto & \psi(T)(\xi) \end{array}$$

By [Sch98, Section 2.2], the pairing  $w'$  has trivial right kernel.

**Definition 2.4.5.** We refer to the pairing

$$w'': \begin{array}{ccc} \frac{J_C(k)}{2J_C(k)} \times J_C[2](k) & \rightarrow & k^\times / k^{\times 2} \\ (x, T) & \mapsto & \psi(T)(\delta(x)) \end{array}$$

as the (*modified*) *Kummer pairing*.

This pairing is explicitly computable given representatives  $T_1, \dots, T_{2g}$  for a basis of  $J_C[2]$  as follows. As each  $[T_i]$  is a 2-torsion class, we have that there is a rational function  $h_i$  of  $C$  such that  $\text{div } h_i = 2T_i$ .

If  $D = \sum_{P \in C(k^{\text{al}})} n_P P \in \text{Div}^0(C/k)$  is a divisor representing a class  $[D] \in \text{Pic}^0(C)(k)$  such that  $n_P$  is zero for points of  $C$  which occur in the support of  $T_i$  (i.e the zeros and poles of  $h_i$ ), we

can define

$$\left\langle \left[ \sum_{P \in C(k^{\text{al}})} n_P P \right], [T_i] \right\rangle := \prod_{P \in C(k^{\text{al}})} h_i(P)^{n_P}.$$

Note that while the value of each  $h_i(P)$  lies in  $k^{\text{al}}$  the product lies in  $k^\times$  for any  $D$  as chosen above. We also note that every divisor class  $[D]$  has a representative of the form  $\sum_{P \in C(k^{\text{al}})} n_P P$  where  $n_P$  is zero for points of  $C$  which occur in the support of  $T_i$  [HS00, Lemma A.2.3.1]. Furthermore, if  $C(k) \neq \emptyset$  then every class  $[D] \in \text{Pic}^0(C)(k)$  has a representative in  $\text{Div}^0(C/k)$  [Sch98, Proposition 2.7]. The value of  $\prod_{P \in C(k^{\text{al}})} h_i(P)^{n_P}$  depends on the chosen representatives for the 2-torsion and the representative of  $[D]$  in  $\frac{J_C(k)}{2J_C(k)}$ . However, the square class of this value is independent of these choices so the pairing is well-defined [Sch98, Lemma 2.1].

**Remark 2.4.6.** We point out a feature of the description above that is essential to our computations. Once we fix a particular choice for  $h_1, \dots, h_{2g}$ , we may consider them as functions

$$h_i: \mathcal{D} \rightarrow k^\times$$

where  $\mathcal{D}$  denotes the subset of divisors in  $\text{Div}(C/k)$  with support avoiding the zeros and poles of the  $h_1, \dots, h_{2g}$ . If  $D \in \mathcal{D}$  has degree 0, then we have that  $(\lambda h_i)(D) = h_i(D)$  for all  $\lambda \in k^\times$  and all  $i \in \{1, \dots, 2g\}$ .

We are ready to state the well-known companion result to Proposition 2.4.3 for the bad places. We provide a proof lacking an immediate reference.

**Proposition 2.4.7.** *Let  $C/k$  be a curve of genus  $g \geq 1$  such that  $C(k) \neq \emptyset$  and such that  $\text{rk}_2 J_C[2](k) = 2g$ . Let  $\{T_1, \dots, T_{2g}\}$  be a basis for  $J_C[2](k)$ , and let  $h_1, \dots, h_{2g}$  be the maps  $h_i: \frac{J_C(k)}{2J_C(k)} \rightarrow k^\times/k^{\times 2}$  defined from the modified Kummer pairing. Let  $x \in J_C(k)$  and choose  $y \in J_C(k^{\text{sep}})$  such that  $[2]y = x$ . Then  $k(y)/k$  is unramified if both of the following hold:*

(a)  $\text{ord}_\nu h_i(x) \equiv 0 \pmod{2}$  for each  $i$  and each finite place  $\nu$  of  $k$ , where  $\text{ord}_\nu$  is normalized so that  $\text{ord}_\nu(O_k) = \mathbb{Z}$ .

(b) Each  $h_i(x)$  has a positive representative modulo  $k^{\times 2}$  at all real places.

*Proof.* Proposition 2.4.3 shows that it suffices to consider only those places contained in  $\tilde{S}$ . Let  $\nu \in \tilde{S}$  be a finite place and let  $\sigma \in I_\nu$  be an element in the inertia subgroup of  $\text{Gal}(k^{\text{sep}}/k)$ . Then we need to show that  $[\sigma y - y] = [0]$ . By Proposition 2.3.5, we may extend  $\text{ord}_\nu$  to a valuation on  $O_{k(y)}$  which restricts to  $\text{ord}_\nu$  on  $O_k$ . Observe that by definition of  $y$  we have  $[\sigma y - y] \in J_C[2](k)$ . Now

$$\langle [\sigma y - y], T_i \rangle = \frac{h_i(y)^\sigma}{h_i(y)}$$

Note again since  $[2]y = x$  that  $h_i(y)^2 = h_i(x) \pmod{k^{\times 2}}$ . Thus  $\text{ord}_\nu h_i(y) \in \mathbb{Z}$  so the inertia group acts trivially on  $h_i(y)$ . In particular each  $\langle [\sigma y - y], T_i \rangle$  is trivial.

For archimedean places  $\nu$  of  $\tilde{S}$ , we have that the inertia group  $I_\nu$  is trivial if  $\nu$  is a complex place. If  $\nu$  is a real place then we have assumed each  $h_i(x)$  has a positive representative at  $\nu$ , so

$$\langle [\sigma y - y], T_i \rangle = \frac{h_i(y)^\sigma}{h_i(y)}$$

is always trivial for  $\sigma \in I_\nu$ . Since the Kummer pairing has trivial left kernel we see that  $I_\nu$  acts trivially.  $\square$

## 2.5 Affine algebraic groups and categorical quotients

In this section we follow [MFK94, Chapters 0-1].

**Definition 2.5.1.** An algebraic group is a group object in the category of varieties over  $k$ . An *affine algebraic group* is a group object in the category of affine varieties over  $k$ .

**Remark 2.5.2.** Note that in some literature, particularly [MFK94], the term *linear algebraic group* is used instead (cf. [Con02]).

The prototypical example of an affine algebraic group is  $\mathrm{GL}_n/k$ . By a *subgroup* of an affine algebraic group  $G/k$ , we mean a subgroup object of  $G/k$  in the category of algebraic varieties over  $k$ .

**Definition 2.5.3.** An affine algebraic group is said to be *reductive* if the maximal normal connected solvable algebraic subgroup is a (possibly trivial) multiplicative torus.

Note that we allow disconnected reductive groups; in particular, finite groups are reductive.

**Definition 2.5.4.** Let  $\mathcal{C}$  be a category, let  $X$  be an object of  $\mathcal{C}$ , and let  $\sigma: G \times X \rightarrow X$  be a group action on  $X$ . We say that  $Y \in \mathcal{C}$  is a *categorical quotient* of  $X$  by  $G$  if there exists a morphism  $\pi: X \rightarrow Y$  such that

- $\pi$  is  $G$ -invariant. That is, we have that

$$\begin{array}{ccc} G \times X & \xrightarrow{\sigma} & X \\ & \searrow \pi \circ p_2 & \swarrow \pi \\ & & Y \end{array}$$

commutes, where  $p_2: G \times X \rightarrow X$  is the natural projection.

- If  $\phi: X \rightarrow Z$  is a  $G$ -invariant morphism, then  $\phi$  factors through  $\pi$  uniquely.

If  $Y$  exists, we denote it by  $X//G$ .

Note in Definition 2.5.4 that if the categorical  $X//G$  exists, then the universal property implies that it is unique up to unique isomorphism.

**Remark 2.5.5.** If  $\mathcal{D}$  is a subcategory of  $\mathcal{C}$ , and  $X \in \mathcal{D}$  is an object with a  $G$ -action, then the categorical quotient  $X//_{\mathcal{C}}G$  in  $\mathcal{C}$  is not necessarily the same as the categorical quotient  $X//_{\mathcal{D}}G$  in  $\mathcal{D}$ . If  $X/k$  is a scheme with an action by a group  $G/k$ , we always denote by  $X//G$  the categorical quotient in the category of schemes over  $k$ , provided the quotient exists. However, it is important for us to also view  $X/k$  and  $X//G$  as functors from  $\mathbf{k}\text{-alg}$  to  $\mathbf{Set}$ ; in Chapter 4 we use them to construct functors from  $\mathbf{k}\text{-alg}$  to  $\mathbf{Set}$  not necessarily representable by a scheme.

**Example 2.5.6.** We give a simple example of the dependence of a categorical quotient on the category. Let  $G := \mathbb{Z}/2$ , and let  $G$  act on the polynomial ring  $R := \mathbb{Q}[r_1, r_2]$  by permutation of the variables. The ring of invariants  $R^G$  is given by  $\mathbb{Q}[r_1r_2, r_1 + r_2]$ , so in particular we have that the categorical quotient of  $\text{Spec } R$  by  $G$  exists in the category of schemes and is isomorphic to  $\mathbb{A}_{\mathbb{Q}}^2$ . The quotient morphism is given by  $\pi: (\alpha_1, \alpha_2) \mapsto (\alpha_1\alpha_2, \alpha_1 + \alpha_2)$ , which we can view as the map sending  $(\alpha_1, \alpha_2)$  to the monic quadratic polynomial whose roots are  $\{\alpha_1, \alpha_2\}$ .

We may view any scheme over  $\mathbb{Q}$  as a functor from  $\mathbb{Q}\text{-alg}$  to  $\mathbf{Set}$ . In the category of functors from  $\mathbb{Q}$ -algebras to sets, we have that the functor

$$\mathcal{F}: A \mapsto \{ G\text{-orbits of } (\text{Spec } R)(A) \}$$

satisfies the universal property of categorical quotients. The natural map

$$\mathcal{F}(\mathbb{Q}) = G \backslash (\text{Spec}(R)(\mathbb{Q})) \hookrightarrow \text{Spec}(R^G)(\mathbb{Q})$$

is not a bijection, so in particular  $\text{Spec } R^G$  is not the categorical quotient of  $\text{Spec } R$  by  $G$  in the category of functors from  $\mathbb{Q}\text{-alg}$  to  $\mathbf{Set}$ .

**Definition 2.5.7.** Let  $X/k$  be a scheme with an action by a reductive algebraic group  $G/k$ . A geometric point  $x \in X(k^{\text{al}})$  is  *$G$ -pre-stable* if there exists a  $G$ -invariant affine open neighbourhood  $U$  of  $x$  such that the action morphism  $G \times U \rightarrow U$  is closed.

The set of pre-stable points of a scheme  $X$  is the set of geometric points of an open subscheme of  $X$  [MFK94, Section 1.4]. Thus, we may refer to the subscheme of pre-stable points of  $X$ .

**Definition 2.5.8.** Let  $X/k$  be a scheme with an action by a reductive algebraic group  $G/k$ . We say that  $G$  has a *prestable action* on  $X$  if the subscheme of pre-stable points of  $X$  is equal to  $X$ .

We require the notion of pre-stability of a point in order to express the technical condition Proposition 2.5.9. We only consider categorical quotients where this technical condition is satisfied.

**Proposition 2.5.9.** *Let  $X/k$  be a scheme and let  $G/k$  and  $H/k$  be reductive algebraic groups acting on  $X/k$  such that the actions of  $G$  and  $H$  commute. Then the following statements hold.*

- (a) *If the action of  $G$  on  $X$  is pre-stable, then  $X//G$  exists in the category of schemes,  $\pi_G: X \rightarrow X//G$  is a surjective affine morphism, and the action of  $H$  on  $X$  induces an action of  $H$  on  $X//G$ .*

(b) If the condition of part (a) holds and if the action of  $H$  on  $(X//G)$  is pre-stable, then we have that the action of  $G \times H$  on  $X$  is pre-stable, the action of  $H$  on  $X$  is pre-stable, and the action of  $G$  on  $X//H$  is pre-stable.

(c) If the condition of part (b) holds, then

$$(X//G)//H, \quad X//(G \times H), \quad (X//H)//G$$

all exist in the category of schemes and they are isomorphic.

**Remark 2.5.10.** A morphism  $f: X \rightarrow Y$  is *submersive* if for every set  $U \subseteq Y$ , we have that  $U$  is open if and only if  $f^{-1}U$  is open. As it turns out, categorical quotients by reductive groups, when they exist, are submersive [MFK94, Chapter 0].

*Proof.* (a) The existence of  $X//G$  and the fact that  $\pi_G: X \rightarrow X//G$  is surjective and affine follow immediately from [MFK94, Proposition 1.9]. To construct the  $H$ -action, we consider the morphisms

$$\begin{array}{ccc} H \times X & \xrightarrow{\sigma} & X \\ \text{id} \times \pi \downarrow & \searrow \pi\sigma & \downarrow \pi \\ H \times (X//G) & & (X//G). \end{array}$$

Let  $\sigma_G: G \times X \rightarrow X$  be the given  $G$ -action. We define a  $G$ -action  $\sigma'_G: G \times H \times X \rightarrow H \times X$  by  $\sigma'_G(g, h, x) := (h, \sigma_G(g, x))$ , i.e, letting  $G$  act trivially on the first factor and acting in the usual way on the second factor. The categorical quotient of  $H \times X$  by  $G$  exists and the morphism  $(\text{id} \times \pi): H \times X \rightarrow H \times (X//G)$  satisfies the universal property. Since the actions of  $H$  and  $G$  commute, we have that  $\pi\sigma$  is constant on  $G$ -orbits. By the universal property, we have an  $H$ -action  $\sigma: H \times (X//G) \rightarrow (X//G)$ .

(b) By our hypothesis, we can find an  $H$ -invariant affine open cover  $\{U_i\}$  of  $X//G$  such that the  $H$ -action is closed. Since  $\pi_G$  is affine, the pullback  $\{\pi_G^{-1}U_i\}$  is a  $G \times H$ -invariant affine open cover of  $X$ . Of course,  $\{\pi_G^{-1}U_i\}$  is in particular a covering by  $H$ -invariant open affine subschemes. Since  $\pi_G$  is submersive [MFK94, Proposition 1.9] and the  $H$ -action is closed on  $U_i$ , we have that the  $H$ -action is closed on  $\pi_G^{-1}U_i$ . Similarly, we have that the  $G \times H$ -action on each open patch is closed.

We now show that the natural action of  $G$  on  $X//H$  from part (a) is pre-stable. Let  $\pi_H: X \rightarrow X//H$  be the quotient morphism. We have that  $\pi_H$  restricts to the natural quotient

$$\pi_H: \pi_G^{-1}U_i \rightarrow (\pi_G^{-1}U_i)//H$$

on each invariant affine open patch. Let  $R_i$  be the ring such that  $\text{Spec } R_i = \pi_G^{-1}U_i$ . We have that  $\pi_H$  is induced by the inclusion

$$R_i^H \hookrightarrow R_i$$

where  $R_i^H$  denotes the ring of  $H$ -invariants. The action of  $G$  on  $R_i$  restricts to an action on  $R_i^H$ , and  $\{\text{Spec } R_i^H\}$  is an open affine  $G$ -invariant cover of  $X//H$ . We check that the action of  $G$  on each  $\text{Spec } R_i^H$  is closed. Let  $Z \subseteq G \times \text{Spec } R_i^H$  be a closed subscheme, and consider the diagram

$$\begin{array}{ccc} G \times \text{Spec } R_i & \xrightarrow{\sigma_G} & \text{Spec } R_i \\ \text{id} \times \pi_H \downarrow & & \downarrow \pi_H \\ G \times \text{Spec } R_i^H & \xrightarrow{\sigma'_G} & \text{Spec } R_i \end{array}$$

where the  $\sigma_G, \sigma'_G$  are the  $G$ -actions. Since  $\sigma_G$  is closed, we have that

$$\pi_H^{-1} \sigma'_G(Z) = \sigma_G \left( (\text{id} \times \pi_H)^{-1} Z \right)$$

is closed. Since  $\pi_H$  is submersive by [MFK94, Proposition 1.9], we have that  $\sigma'_G(Z)$  is closed. We now see that the action of  $G$  on  $X//H$  is prestable.

- (c) The existence of these schemes follows from part (b) and [MFK94, Proposition 1.9]. We have the various surjective quotient maps

$$\begin{aligned} X &\rightarrow X//G \rightarrow (X//G)//H \\ X &\rightarrow X//H \rightarrow (X//H)//G \\ X &\rightarrow X//(G \times H). \end{aligned}$$

The result now follows from multiple applications of the universal property of categorical quotients. □

## 2.6 Lie groups and Lie algebras

The main objective of this section is to give the definition of “the split group of type  $E_8$  over  $k$ ” as well as give some helpful preliminaries for understanding the modified construction of Lurie, described in Section 2.6.10.

Our exposition for Lie algebras, affine algebraic groups, and Lie groups draws from a number of different sources. We are primarily interested in Lie algebras and affine algebraic groups over a general field of characteristic 0, so we often refer to [Mil13] and [Bou68, Bou75]. We also require some facts regarding the complex geometry of Lie groups, for which we often refer to the book of Fulton and Harris [FH91].

## 2.6.1 Lie algebras

**Definition 2.6.1.** A Lie algebra over  $k$  is a  $k$ -vector space  $\mathfrak{g}$  endowed with a bilinear map  $[\cdot, \cdot]: \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$  satisfying the *Jacobi identity*:

$$[x, [y, z]] + [y, [z, x]] + [z, [y, x]] = 0 \quad \text{for all } x, y, z \in \mathfrak{g}.$$

The bilinear map is called the *Lie bracket*. A *Lie sub-algebra* of  $\mathfrak{g}$  is a sub-vector space  $\mathfrak{h}$  such that  $[\cdot, \cdot]$  restricts to a Lie bracket on  $\mathfrak{h}$ .

We only consider Lie algebras that are finite dimensional as  $k$ -vector spaces.

**Definition 2.6.2.** A morphism of Lie algebras  $f: \mathfrak{g} \rightarrow \mathfrak{h}$  is a morphism of the underlying vector spaces such that

$$f([x, y]) = [f(x), f(y)] \quad \text{for all } x, y \in \mathfrak{g}.$$

**Definition 2.6.3.** Let  $V$  be a finite dimensional  $k$ -vector space. We define the Lie algebra  $\mathfrak{gl}_V$  to be the vector space of endomorphisms of  $V$  with the Lie bracket

$$[A, B] := A \circ B - B \circ A \quad \text{for } A, B \in \mathfrak{gl}_V.$$

**Definition 2.6.4.** A *representation* of a Lie algebra  $\mathfrak{g}$  is a morphism  $\rho: \mathfrak{g} \rightarrow \mathfrak{gl}_V$  of Lie algebras. If  $V$  is a one-dimensional vector space, then we call  $\rho$  a *character*.

If  $\mathfrak{g}$  is a Lie algebra and  $x \in \mathfrak{g}$ , then  $[x, \cdot]: \mathfrak{g} \rightarrow \mathfrak{g}$  is an endomorphism of the underlying vector space. One easily sees by the Jacobi identity that the morphism  $x \mapsto [x, \cdot] \in \mathfrak{gl}_{\mathfrak{g}}$  respects Lie brackets, so it is in fact a morphism of Lie algebras.

**Definition 2.6.5.** Let  $\mathfrak{g}$  be a finite dimensional Lie algebra. The adjoint representation of  $\mathfrak{g}$  is the morphism of Lie algebras

$$\begin{aligned} \text{ad}: \mathfrak{g} &\rightarrow \mathfrak{gl}_{\mathfrak{g}} \\ x &\mapsto [x, \cdot]. \end{aligned}$$

**Definition 2.6.6.** An *ideal* of a Lie algebra  $\mathfrak{g}$  is a Lie algebra  $\mathfrak{h} \subseteq \mathfrak{g}$  such that  $[\mathfrak{g}, \mathfrak{h}] \subseteq \mathfrak{h}$ . An ideal is *trivial* if it is equal to either 0 or  $\mathfrak{g}$ . A Lie algebra is *simple* if it has no non-trivial ideals.

**Definition 2.6.7.** A Lie algebra  $\mathfrak{g}$  is *abelian* if  $[x, y] = 0$  for all  $x, y \in \mathfrak{g}$ .

**Remark 2.6.8.** If  $\mathfrak{g}$  is abelian and  $V$  is a one-dimensional vector space, then any morphism of vector spaces  $\rho: \mathfrak{g} \rightarrow \mathfrak{gl}_V$  is a character.

Of critical importance to us is the relationship between Lie algebras over  $k$  and affine algebraic groups defined over  $k$ .

**Lemma 2.6.9.** Let  $\mathfrak{g}$  be a Lie algebra over  $k$ . Then  $\text{Aut}(\mathfrak{g})$  has the structure of an affine algebraic group over  $k$ .

*Proof.* Since the Lie bracket is a  $k$ -bilinear map, we have that

$$\text{Aut}(\mathfrak{g}) := \{g \in \text{GL}(\mathfrak{g}) : g[X, Y] = [gX, gY] \text{ for all } X, Y \in \mathfrak{g}\}$$

is defined by algebraic conditions. □

**Example 2.6.10.** Let  $V = \mathbb{C}^n$  be the  $n$ -dimensional complex vector space. Let  $\mathfrak{gl}_V$  be the Lie algebra of endomorphisms as in Definition 2.6.3. We may of course identify  $\mathfrak{gl}_V$  with the lie algebra of  $n \times n$  complex matrices, which we denote by  $\mathfrak{gl}_n$ . The first sub-Lie algebra we shall look at is

$$\mathfrak{d}_n := \left\{ A \in \mathfrak{gl}_n : A = \begin{bmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{bmatrix} \right\},$$

the sub-algebra of diagonal matrices. It is easy to see that  $\mathfrak{d}_n$  is abelian.

The sub-algebra we look at more closely is

$$\mathfrak{sl}_n := \{A \in \mathfrak{gl}_n : \text{Tr}(A) = 0\}.$$

Since  $\text{Tr}(AB) = \text{Tr}(BA)$  for any matrices  $A, B \in \mathfrak{gl}_n$ , we have that  $\mathfrak{sl}_n$  is an ideal of  $\mathfrak{gl}_n$ .

## 2.6.2 Simple lie algebras

In this subsection we discuss some of the additional structure of simple Lie algebras. Note that many of the definitions and results in this section can be made for more general Lie algebras. We avoid doing so for the sake of brevity.

The following definition is from basic linear algebra, but allows us to clarify Definition 2.6.14.

**Theorem 2.6.11.** *For any  $X \in \text{End}(V_{\mathbb{C}})$ , there exist a unique pair of elements  $X_s, X_n \in \text{End}(V_{\mathbb{C}})$  such that  $X_s$  is diagonalizable,  $X_n$  is nilpotent,  $[X_s, X_n] = 0$ , and  $X = X_s + X_n$ .*

**Definition 2.6.12.** For  $X \in \text{End}(V_{\mathbb{C}})$ , the decomposition  $X = X_s + X_n$  from Theorem 2.6.11 is called the *Jordan decomposition* of  $X$ . We call  $X_s$  the *semi-simple part* and  $X_n$  the *nilpotent part*.

**Theorem 2.6.13.** *Let  $\mathfrak{g}$  be a simple Lie algebra. For all  $X \in \mathfrak{g}$ , there exist a unique pair of elements  $X_s, X_n \in \mathfrak{g}$  such that  $X = X_s + X_n$  and for any representation  $\rho$  of  $\mathfrak{g}$  we have*

$$\rho(X_s) = \rho(X)_s, \quad \rho(X_n) = \rho(X)_n.$$

*That is, there is an intrinsic Jordan decomposition for every element of a simple Lie algebra.*

**Definition 2.6.14.** Let  $\mathfrak{g}_{\mathbb{C}}$  be a simple complex Lie algebra. For  $X \in \mathfrak{g}_{\mathbb{C}}$ , the decomposition  $X = X_s + X_n$  from Theorem 2.6.13 is called the *Jordan decomposition* of  $X$ . We call  $X_s$  the *semi-simple part* and  $X_n$  the *nilpotent part*.

*Proof.* See [FH91, Theorem 9.20]. □

**Definition 2.6.15.** An element  $X \in \mathfrak{g}$  of a simple Lie algebra is *semi-simple* if it is equal to its semi-simple part.

**Definition 2.6.16.** Let  $\mathfrak{g}$  be a simple Lie algebra and let  $X \in \mathfrak{g}$ . The *centralizer* of  $X$  is the Lie sub-algebra defined by

$$\mathfrak{c}_{\mathfrak{g}}(x) := \{y \in \mathfrak{g} : [x, y] = 0\}.$$

An element  $X \in \mathfrak{g}$  is *regular* if its centralizer is of minimal dimension. That is, if

$$\dim \mathfrak{c}_{\mathfrak{g}}(X) = \min_{y \in \mathfrak{g}} \dim \mathfrak{c}_{\mathfrak{g}}(y).$$

**Definition 2.6.17.** An element  $X \in \mathfrak{g}$  of a simple Lie algebra is *regular semi-simple* if it is both regular and semi-simple. We denote the open subset of regular semi-simple elements of  $\mathfrak{g}$  by  $\mathfrak{g}^{\text{rss}}$ .

We caution that the following definition of a Cartan subalgebra from [FH91] is valid for simple Lie algebras, but not in general.

**Definition 2.6.18.** A Cartan subalgebra  $\mathfrak{t}$  of a simple Lie algebra  $\mathfrak{g}$  is an abelian Lie sub-algebra such that every  $X \in \mathfrak{t}$  is semi-simple and such that  $\mathfrak{t}$  is not contained in a larger abelian subalgebra of  $\mathfrak{g}$  with this property.

**Theorem 2.6.19.** *Every simple Lie algebra contains a Cartan subalgebra.*

*Proof.* See [Mil13, Corollary I.8.10]. □

**Definition 2.6.20.** A Cartan subalgebra of  $\mathfrak{g}$  is *splitting over  $k$*  if for every element  $x \in \mathfrak{t}$  we have that  $\text{ad } x$  is diagonalizable over  $k$ . We say that  $\mathfrak{g}$  is *split over  $k$*  if it has at least one splitting Cartan subalgebra.

Note that if  $k$  is algebraically closed, then every Cartan subalgebra of  $\mathfrak{g}$  is splitting.

**Definition 2.6.21.** Let  $\mathfrak{g}$  be a simple Lie algebra over  $k$  and let  $\mathfrak{t}$  be a splitting Cartan subalgebra of  $\mathfrak{g}$ . Let  $\mathfrak{t}^{\vee} := \text{Hom}_k(\mathfrak{t}, k)$  denote the linear dual to  $\mathfrak{t}$ . For any  $\alpha \in \mathfrak{t}^{\vee}$ , we let

$$\mathfrak{g}^{\alpha} := \{x \in \mathfrak{g} : (\text{ad}_{\mathfrak{g}} t)x = \alpha(t)x \text{ for all } t \in \mathfrak{t}\}.$$

If  $\mathfrak{g}^{\alpha} \neq 0$  and  $\alpha \neq 0$ , we call  $\alpha$  a *root* of  $(\mathfrak{g}, \mathfrak{t})$  [Bou75, Chapter 8, Section 2].

As  $\mathfrak{g}$  is a finite dimensional simple Lie algebra over  $k$ , there are only finitely many roots of  $(\mathfrak{g}, \mathfrak{t})$  for any splitting Cartan subalgebra  $\mathfrak{t}$  since  $\mathfrak{g}^{\alpha} \cap \mathfrak{g}^{\beta} = \{0\}$  for any two roots  $\alpha, \beta$ .

**Remark 2.6.22.** We can extend Definition 2.6.21 to non-split Lie algebras by defining the roots of  $(\mathfrak{g}, \mathfrak{t})$  to be the roots of  $(\mathfrak{g} \otimes_k k', \mathfrak{g} \otimes_k k')$ , where  $k'/k$  is the minimal extension such that  $\mathfrak{t} \otimes_k k'$  is a splitting Cartan subalgebra of  $\mathfrak{g} \otimes_k k'$ . It is not strictly necessary for us to do this.

**Theorem 2.6.23.** Let  $\Lambda \subseteq \mathfrak{t}^\vee$  denote the  $\mathbb{Z}$ -linear combinations of the roots. Then  $\Lambda$  is a free  $\mathbb{Z}$ -module of rank equal to  $\dim_k \mathfrak{t}^\vee$ . For any embedding  $i: k \hookrightarrow \mathbb{C}$ , the  $\mathbb{R}$ -linear combinations of the roots  $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \subseteq \mathfrak{t}^\vee \otimes_k \mathbb{C}$  is a real vector space of dimension  $\dim_k \mathfrak{t}^\vee$ .

*Proof.* See [FH91, pp. 198-199]. □

Note that the real vector space in Theorem 2.6.23 is not necessarily fixed by complex conjugation.

**Example 2.6.24.** Recall from Example 2.6.10 that  $\mathfrak{sl}_n$ , the Lie algebra of traceless  $n \times n$  complex matrices, is simple. We also recall the Lie sub-algebra of  $\mathfrak{gl}_n$  of diagonal matrices  $\mathfrak{d}_n$ . We see that  $\mathfrak{t} := \mathfrak{sl}_n \cap \mathfrak{d}_n$  is a Lie sub-algebra of  $\mathfrak{sl}_n$  which is abelian. By definition every element of  $\mathfrak{t}$  is diagonalizable, and elementary linear algebra shows that any  $y \in \mathfrak{sl}_n$  which is diagonalizable and satisfies  $[y, t] = 0$  for all  $t \in \mathfrak{t}$  (i.e, commutes with all elements in  $\mathfrak{t}$ ) must already lie in  $\mathfrak{t}$ .

To give an example of the roots of  $\mathfrak{sl}_n$ , we will restrict to  $n = 3$ . Let  $E_{i,j}$  be the  $3 \times 3$  complex matrix whose only non-zero entry is a 1 in the  $(i, j)$  position. We see for any diagonal matrix  $A := \text{diag}(a_1, a_2, a_3) \in \mathfrak{t}$  that

$$[A, E_{i,j}] = (a_i - a_j)E_{i,j}.$$

In particular, the  $E_{i,j}$  with  $i \neq j$  are eigenvectors for the adjoint action of  $\mathfrak{sl}_n$  on itself, where the associated eigenvalue (eigenfunctional) in  $\mathfrak{t}^\vee$  is

$$L_{i,j} \left( \begin{bmatrix} a_1 & & \\ & a_2 & \\ & & a_3 \end{bmatrix} \right) = a_i - a_j.$$

The six  $E_{i,j}$  together with two matrices that span  $\mathfrak{t}$  are a basis for  $\mathfrak{sl}_3$  as an 8-dimensional vector space. The  $L_{i,j}$  as elements of  $\mathfrak{t}^\vee$  are the 6 roots of  $\mathfrak{sl}_3$ .

**Example 2.6.25.** Consider the following sub-Lie-algebras of  $\mathfrak{sl}_2\mathbb{R}$ :

$$\mathfrak{t}_1 := \left\{ \begin{bmatrix} \lambda & 0 \\ 0 & -\lambda \end{bmatrix} : \lambda \in \mathbb{R} \right\}, \quad \mathfrak{t}_2 := \left\{ \begin{bmatrix} 0 & \lambda \\ -\lambda & 0 \end{bmatrix} : \lambda \in \mathbb{R} \right\}.$$

Similar to Example 2.6.24, we have that  $\mathfrak{t}_1$  is a splitting Cartan subalgebra and the functionals

$$\alpha_{\pm 2} \left( \begin{bmatrix} \lambda & 0 \\ 0 & -\lambda \end{bmatrix} \right) = \pm 2\lambda$$

are the roots. We have that  $\mathfrak{t}_2$  is a Cartan subalgebra, but that it is not splitting. The Cartan subalgebra becomes splitting after making a finite extension  $\mathbb{C}/\mathbb{R}$ , and we can calculate that the roots of  $(\mathfrak{sl}_2\mathbb{C}, \mathfrak{t}_2 \otimes_{\mathbb{R}} \mathbb{C})$  are

$$\alpha_{\pm 2i} \left( \begin{bmatrix} 0 & \lambda \\ -\lambda & 0 \end{bmatrix} \right) = \pm 2i\lambda, \quad \text{or equivalently,} \quad \alpha_{\pm 2i} \left( \begin{bmatrix} 0 & -i\lambda \\ i\lambda & 0 \end{bmatrix} \right) = \pm 2\lambda.$$

As expected, we see that the  $\mathbb{R}$ -linear combinations of  $\alpha_{\pm 2i}$  span a real space of dimension 1. We see that complex conjugation acts on this subspace non-trivially. Over the complex numbers, the two Cartan subalgebras  $\mathfrak{t}_1, \mathfrak{t}_2$  are conjugate, and the associated roots are similarly identified. It is possible to abstractly recover the Lie algebra  $\mathfrak{sl}_2\mathbb{R}$ , and hence the roots of  $(\mathfrak{sl}_2\mathbb{R}, \mathfrak{t}_1)$  embedded in  $\mathbb{R}^1$ , from  $\mathfrak{sl}_2\mathbb{C}$ ,  $\mathfrak{t}_2$ , and [Mil13, Theorem I.8.59].

**Definition 2.6.26.** Let  $B := \{e_1, \dots, e_n\}$  be a basis for a real vector space  $V$  of dimension  $n$ . We may define a lexicographic ordering  $\prec_B$  on the points of  $V$  by lexicographically ordering the  $B$ -coordinates. Let  $R$  be the roots of a split simple Lie algebra  $(\mathfrak{g}, \mathfrak{t})$ , and choose a basis  $B$  for the real subspace of  $\mathfrak{t}^\vee \otimes \mathbb{C}$  containing the roots. Any  $\alpha \in R$  such that  $0 \prec \alpha$  is called a *positive root*. Any positive root which is not the sum of two other positive roots is a *simple root* with respect to  $B$ .

**Theorem 2.6.27.** Let  $R$  be the roots of  $(\mathfrak{g}, \mathfrak{t})$ , let  $B$  be a basis for the real subspace  $V$  of  $\mathfrak{t}^\vee \otimes \mathbb{C}$  containing the roots, and let  $\Delta$  be the set of simple roots. Then  $\Delta$  is a basis for  $V$  and every positive root can be expressed as a sum

$$\sum_{\alpha \in \Delta} a_\alpha \alpha$$

where each  $a_\alpha \geq 0$ .

*Proof.* See [TY05, Theorem 18.7.4]. □

Let  $B$  be as in Definition 2.6.26 and let  $\Delta$  be the associated set of simple roots. It is clear by Theorem 2.6.27 that  $\Delta$  is a basis of the real subspace of  $\mathfrak{t}^\vee \otimes \mathbb{C}$  containing the roots. By definition of  $\Delta$ , we see that it is the set of simple roots with respect to the lexicographic ordering induced by  $\prec_B$ , as any positive root is a sum of roots from  $\Delta$  with positive coefficients. From now on, we dispense with the formality of first choosing a basis for  $\mathfrak{t}^\vee \otimes \mathbb{C}$ , and choose a basis of simple roots directly.

**Definition 2.6.28.** Let  $\Delta$  be a basis of simple roots. We define the *highest root*  $\alpha_\Delta$  with respect to  $\Delta$  as the maximal root with respect to the total ordering  $\prec_\Delta$ .

**Definition 2.6.29.** Let  $\Phi$  denote the set of roots of a split simple Lie algebra  $(\mathfrak{g}, \mathfrak{t})$ . The  $\mathbb{Z}$ -linear combinations of elements of  $\Phi$ , which we denote by  $\mathbb{Z}\Phi$ , form a lattice called the *root lattice* of  $(\mathfrak{g}, \mathfrak{t})$ . The root lattice spans  $\mathfrak{t}^\vee$  as a  $k$ -vector space, so we may declare it to be the *character lattice* of  $\mathfrak{t}$ .

**Definition 2.6.30.** Let  $\mathfrak{g}$  be a simple Lie algebra, let  $\mathfrak{t}$  be a Cartan subalgebra, and let  $G := \text{Aut}(\mathfrak{g})^\circ$ . Then the group

$$W(\mathfrak{g}, \mathfrak{t}) := N_G(\mathfrak{t})/C_G(\mathfrak{t})$$

is called the *Weyl group* of  $\mathfrak{g}$  with respect to  $\mathfrak{t}$ . If  $\mathfrak{g}$  is clear from context, we denote this group by  $W_{\mathfrak{t}}$ .

**Remark 2.6.31.** If  $k$  is algebraically closed, then  $\text{Aut}(\mathfrak{g})^\circ$  acts transitively on the set of Cartan subalgebras of  $\mathfrak{g}$  [Mil13, Theorem I.8.17]. Let  $\mathfrak{t}, \mathfrak{t}'$  be Cartan subalgebras of  $\mathfrak{g}$  and let  $\Psi \in \text{Aut}(\mathfrak{g})^\circ$

be an automorphism such that  $\Psi(\mathfrak{t}) = \mathfrak{t}'$ . Conjugation by  $\Psi$  sends  $N_{\text{Aut}(\mathfrak{g})^\circ}(\mathfrak{t})$  (i.e, the subgroup of  $\text{Aut}(\mathfrak{g})^\circ$  fixing the subspace  $\mathfrak{t}$ ) to  $N_{\text{Aut}(\mathfrak{g})^\circ}(\mathfrak{t}')$ . Similarly, conjugation by  $\Psi$  sends  $C_{\text{Aut}(\mathfrak{g})^\circ}(\mathfrak{t})$  (i.e, the element-wise stabilizer of  $\mathfrak{t}$ ) to  $C_{\text{Aut}(\mathfrak{g})^\circ}(\mathfrak{t}')$ . In particular, the isomorphism class of the group  $W(\mathfrak{g}, \mathfrak{t})$  and the root lattice of  $(\mathfrak{g}, \mathfrak{t})$  are independent of the choice of  $\mathfrak{t}$ .

### 2.6.3 Affine algebraic groups and Lie algebras

**Definition 2.6.32.** A (real/complex) Lie group is a group object in the category of (real/complex) manifolds.

We are not particularly concerned with Lie groups over real or complex fields, but rather with groups defined over an arbitrary base field  $k$  that behave like Lie groups. The objects that we are actually interested in are affine algebraic groups.

We mention Lie groups for the following two reasons. First, we require some methods from the theory of complex Lie groups in Section 2.6.7. Secondly, the proof of many facts about affine algebraic groups over a field  $k$  of characteristic 0 and cardinality at most that of  $\mathbb{C}$  often reduces to the proof of a similar statement for complex Lie groups.

There is a close connection between affine algebraic groups and Lie groups. Recall that the natural inclusion  $\text{GL}_n \mathbb{R} \hookrightarrow \mathbb{R}^{n \times n}$  (resp.  $\text{GL}_n \mathbb{C} \hookrightarrow \mathbb{C}^{n \times n}$ ) imbues  $\text{GL}_n \mathbb{R}$  (resp.  $\text{GL}_n \mathbb{C}$ ) with the structure of a real (resp. complex) manifold. The group law morphisms for  $\text{GL}_n \mathbb{R}$  and  $\text{GL}_n \mathbb{C}$  are smooth with respect to the manifold structure, so  $\text{GL}_n \mathbb{R}$  and  $\text{GL}_n \mathbb{C}$  naturally have the structure of a Lie group.

**Theorem 2.6.33.** *There is a canonical functor from the category of (real/complex) affine algebraic groups to (real/complex) Lie groups, which respects the tangent spaces at the identity; it takes  $\text{GL}_n$  to  $\text{GL}_n \mathbb{R}$  in the real case and takes  $\text{GL}_n$  to  $\text{GL}_n \mathbb{C}$  in the complex case. It is faithful on connected algebraic groups (all algebraic groups in the complex case).*

*Proof.* See [Mil13, Theorem III.2.1]. □

Let  $G$  be an affine algebraic group. For every  $g \in G$ , we obtain an inner automorphism of  $G$  defined by  $\Psi_g(x) := g^{-1}xg$ . As  $\Psi_g$  fixes the identity, we have that the differential of  $\Psi_g$  is an automorphism of  $T_e G$ . Consequently, there is a natural morphism of affine algebraic groups

$$\begin{aligned} \text{Ad}: G &\rightarrow \text{Aut}(T_e G) \\ g &\mapsto d\Psi_g. \end{aligned}$$

The differential of  $\text{Ad}$  at the origin, which we denote by  $\text{ad}$ , defines a morphism of vector spaces

$$\text{ad}: T_e G \rightarrow \text{End}(T_e G).$$

**Proposition 2.6.34.** *Let  $G$  be an affine algebraic group with identity element  $e$ . Then the tangent space at the identity  $T_e G$  with the Lie bracket*

$$[X, Y] := \text{ad}(X)(Y)$$

*is a Lie algebra.*

*Proof.* See [Mil13, Section II.3, p118]. □

Note that if  $T_e G$  is a finite dimensional  $k$ -vector space, then  $\text{End}(T_e G) = \mathfrak{gl}_{T_e G}$  and the adjoint map is exactly the map from Definition 2.6.5.

**Definition 2.6.35.** Let  $G$  be a simple connected affine algebraic group. A *maximal subtorus* is a diagonalizable, connected, abelian algebraic subgroup  $T \subseteq G$  not contained in any larger such group.

**Theorem 2.6.36.** *Let  $G$  be a connected simple affine algebraic group and let  $\mathfrak{g}$  be its Lie algebra. Then an algebraic subgroup of  $G$  is a maximal subtorus if and only if its corresponding Lie subalgebra is a Cartan subalgebra of  $\mathfrak{g}$ .*

*Proof.* See [Mil13, Lemma II.4.27]. □

**Example 2.6.37.** Let  $G := \text{SL}_n \mathbb{C}$ . The Lie algebra of  $G$  turns out to be the Lie algebra  $\mathfrak{sl}_n$  from Example 2.6.24, and the adjoint action of  $\text{SL}_n \mathbb{C}$  on  $\mathfrak{sl}_n$  is given by  $(g, X) \mapsto g^{-1} X g$ , where we view  $g$  and  $X$  as  $n \times n$  complex matrices. We have that  $G$  is connected and simple. The subgroup

$$T := \left\{ \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix} : a_1 \dots a_n = 1, a_i \in \mathbb{C} \right\}$$

is isomorphic to  $\mathbb{G}_m^n$ , and is a maximal connected diagonalizable abelian Lie subgroup. Its Lie algebra is

$$\mathfrak{t} := \left\{ \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix} : a_1 + \dots + a_n = 0, a_i \in \mathbb{C} \right\}$$

which we recognize as the Cartan subalgebra from Example 2.6.24.

## 2.6.4 Classification

**Theorem 2.6.38.** *Let  $\mathfrak{g}$  be a simple complex Lie algebra. Then  $\mathfrak{g}$  is determined up to isomorphism by its root lattice. Furthermore,  $\mathfrak{g}$  is isomorphic to one of the following:*

$$\begin{aligned} \mathfrak{sl}_{n+1} & \quad (\text{type } A_n) \\ \mathfrak{so}_{2n+1} & \quad (\text{type } B_n) \\ \mathfrak{sp}_{2n} & \quad (\text{type } C_n) \\ \mathfrak{so}_{2n} & \quad (\text{type } D_n) \\ \mathfrak{e}_6, \mathfrak{e}_7, \mathfrak{e}_8 & \quad (\text{type } E_6, E_7, E_8, \text{ resp.}) \\ \mathfrak{g}_2, \mathfrak{f}_4 & \quad (\text{other}). \end{aligned}$$

For an explicit description of the root systems of the Lie algebras appearing above, see [Bou68, Planche I-IX].

*Proof.* See [Mil13, Theorem I.8.60, Theorem I.8.61] and [Bou68, Planche I-IX]. □

If  $\mathfrak{g}$  is a simple Lie algebra over  $k$ , then the *Dynkin type* of  $\mathfrak{g}$  is the type of  $\mathfrak{g} \otimes_k \mathbb{C}$  specified in Theorem 2.6.38.

**Definition 2.6.39.** Let  $\mathfrak{g}$  be a simple Lie algebra over  $k$ . The algebraic group  $\text{Aut}(\mathfrak{g})^\circ$  is the *adjoint group* of type  $\mathfrak{g}$  over  $k$ .

**Theorem 2.6.40.** *Let  $\mathfrak{g}$  be a simple Lie algebra over  $k$  and let  $G$  be the adjoint group of type  $\mathfrak{g}$  over  $k$ . Then the Lie algebra of  $G$  is  $\mathfrak{g}$  and the centre of  $G$  is trivial.*

*Proof.* Note that we can canonically identify the Lie algebra of  $\text{Aut}(\mathfrak{g})^\circ$  with

$$\text{Der } \mathfrak{g} := \{df \in \text{End}(\mathfrak{g}) : df([x, y]) = [df(x), y] + [x, df(y)]\}$$

and that  $\text{ad} : \mathfrak{g} \rightarrow \text{Der}(\mathfrak{g})$  is a morphism of Lie algebras [FH91, Exercise 8.27, 8.28]. To prove that  $\text{ad} : \mathfrak{g} \rightarrow \text{Der}(\mathfrak{g})$  is an isomorphism and that  $\text{Aut}(\mathfrak{g})^\circ$  has trivial centre, it suffices to prove the result when  $k = \mathbb{C}$ . The result for  $k = \mathbb{C}$  can be found in [FH91, Proposition D.40]. Note that the definition for adjoint form appearing in [FH91, page 101] is different than the definition we use, but they are equivalent by [FH91, Proposition D.40]. □

**Example 2.6.41.** Let  $\mathfrak{sl}_n$  be as in Example 2.6.24. Then  $\text{SL}_n \mathbb{C}$  is a connected Lie group of type  $A_n$ . However, we notice that  $\text{SL}_n \mathbb{C}$  has a non-trivial centre given by

$$Z(\text{SL}_n \mathbb{C}) = \left\{ \begin{bmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{bmatrix} : \lambda \in \mu_n \right\}$$

so it is not the adjoint group of type  $A_n$ . However, the quotient  $\text{SL}_n \mathbb{C} / Z(\text{SL}_n \mathbb{C}) =: \text{PSL}_n \mathbb{C}$  is indeed the adjoint group of type  $A_n$ . For further details see [FH91, Section 7.3].

**Definition 2.6.42.** Let  $G$  be a simple affine algebraic group over  $k$ . We say that an element  $x \in G(k^{\text{al}})$  is *semi-simple* if  $x$  acts diagonalizably on  $\mathfrak{g}_{k^{\text{al}}}$ . We say that  $x$  is *regular* if its centralizer in  $G$  has minimal dimension, and say that  $x$  is *regular semi-simple* if it is both regular and semi-simple. We denote the open subscheme of regular semi-simple elements of  $G$  by  $G^{\text{rss}}$ . If  $T \subseteq G$  is a maximal subtorus of  $G$ , then we denote  $T^{\text{rss}} := T \cap G^{\text{rss}}$ .

Note that the containment  $T \subseteq G$  is essential in Definition 2.6.42; every element  $x \in T(k^{\text{sep}})$  acts diagonalizably on  $\mathfrak{t}$  and has centralizer equal to  $T$ .

### 2.6.5 The split Lie algebra of type $E_8$

In this section we define the root lattice  $\Lambda$  of type  $E_8$ . We use the following description which is from [Dol12, Section 8.2.2].

**Definition 2.6.43.** Let  $\{l, e_1, \dots, e_8\}$  be the free generators for a 9-dimensional lattice  $I_{1,8}$  where the generators are pairwise orthogonal,  $\langle e_i, e_i \rangle = -1$  for each  $i$ , and  $\langle l, l \rangle = 1$ . We define

$$\Lambda_{E_8} := \text{Span}\{\alpha \in I_{1,8} : \langle \alpha, \alpha \rangle = -2\}.$$

A *root lattice of type  $E_8$*  is an abstract lattice isomorphic to  $\Lambda_{E_8}$ . The *roots* of  $\Lambda_{E_8}$  are the elements  $\alpha$  such that  $\langle \alpha, \alpha \rangle = -2$ .

When discussing the root lattice of type  $E_8$ , it is helpful to refer to the explicit presentation used in Definition 2.6.43. Over a field  $k$ , we can non-canonically construct a Lie algebra of type  $\mathfrak{e}_8$  by using the root lattice of type  $E_8$ . Later in this chapter, we review a construction of Lurie that allows us to canonically construct a Lie algebra of type  $E_8$  over  $k$  from  $\Lambda_{E_8}$  and some additional data.

**Definition-Theorem 2.6.44.** Up to isomorphism, there exists a unique split Lie algebra over  $k$  whose root lattice  $\Lambda_{E_8}$  is a root lattice of type  $E_8$ . We denote this Lie algebra by  $\mathfrak{e}_8$  and refer to it as the *split Lie algebra of type  $E_8$* . The roots of  $\mathfrak{e}_8$  are exactly the roots of  $\Lambda_{E_8}$ .

*Proof.* See [Mil13, Theorems I.8.57 and Theorem I.8.61]. □

**Proposition 2.6.45.** Let  $\mathfrak{t}$  be a splitting Cartan subalgebra of  $\mathfrak{e}_8$  and let  $\Lambda$  be the associated root lattice. Then the Weyl group  $W_{\mathfrak{t}}$  is the group of isometries of  $\Lambda$ .

*Proof.* See [Bou68, Planche VII]. □

One particularly nice fact about the presentation in Definition 2.6.43 is the following.

**Proposition 2.6.46.** With the notation of Definition 2.6.43, we have that

$$\Lambda_{E_8} = \{v \in I_{1,8} : \langle v, \kappa \rangle = 0\}$$

where  $\kappa := e_1 + e_2 + \dots + e_8 - 3l$ .

*Proof.* The roots of  $\Lambda_{E_8}$  can be identified in [Bou68, Planche VII]. One can simply check that  $\langle \alpha, \kappa \rangle = 0$  for each root  $\alpha$ .  $\square$

By Remark 2.6.31, if  $k$  is algebraically closed then every Cartan subalgebra of  $\mathfrak{e}_8$  gives rise to the same Weyl group. For this reason, and Proposition 2.6.45, we denote by  $W_{E_8}$  the isometry group of  $\Lambda_{E_8}$  and refer to it as the Weyl group of  $E_8$ .

## 2.6.6 The split (adjoint simple) group of type $E_8$ over $k$

**Definition 2.6.47.** The *split (adjoint simple) group of type  $E_8$  over  $k$*  is the adjoint group of  $\mathfrak{e}_8$ , where  $\mathfrak{e}_8$  is the split Lie algebra of type  $E_8$  over  $k$ .

We see by Lemma 2.6.50 that the split adjoint simple group of type  $E_8$  is simply connected. In particular, any affine algebraic group over  $k$  whose Lie algebra is  $\mathfrak{e}_8$  is isomorphic to the adjoint group of type  $\mathfrak{e}_8$  [FH91, Section 7.3]. After the proof of Lemma 2.6.50, we simply refer to the group in Definition 2.6.47 as the split group of type  $E_8$  over  $k$ .

## 2.6.7 Connected components of centralizers

In this section, we review a result of [Ree10] which allows us to calculate the component group of the centralizer of an element of a simple complex Lie group. Of particular interest to us is the application of this technique to the split adjoint simple group of type  $E_8$ . In this subsection, we let  $\mathfrak{h}$  be a simple complex Lie algebra, let  $H$  be the adjoint group of type  $\mathfrak{h}$ , and let  $T$  be a maximal subtorus of  $H$ . The main result of this section is Corollary 2.6.51.

Let  $\Lambda$  be the character lattice of  $T$  and let  $Y = \text{Hom}(\Lambda, \mathbb{Z})$  be the co-character lattice of  $T$ . Let  $V := Y \otimes_{\mathbb{Z}} \mathbb{R}$ . We may regard  $V$  as the Lie algebra of the maximal (analytically) compact subtorus  $S \subseteq T$  via the exponential map (see [FH91, Section 8.3])

$$\exp: V \rightarrow S,$$

which is a surjective group homomorphism. The kernel of  $\exp$  is exactly  $Y$ , so in particular we have an isomorphism

$$\exp: V/Y \xrightarrow{\sim} S.$$

The action of the Weyl group  $W_T$  on  $\Lambda$  gives rise to a dual action on  $Y$  and hence on  $V$ .

The *coroot lattice* is the lattice  $\mathbb{Z}\Phi^\vee \subseteq Y$ . The action of the Weyl group on  $\Phi$  defines a dual action of the Weyl group on  $\Phi^\vee$ . There is a representation  $\rho: W_T \hookrightarrow \text{GL}_V$  such that for any  $g \in W_T$  and  $v \in \Phi^\vee$ , we have that  $gv = \rho(g)v$ ; that is, the dual action of  $W_T$  on  $\Phi$  is represented by linear transformations of  $V$  [FH91, Appendix D.4].

Note that in general  $\mathbb{Z}\Phi^\vee \neq Y$ , though we do have equality when  $\Lambda$  is a root lattice of type  $E_8$ .

**Lemma 2.6.48.** *The root lattice of type  $E_8$  is unimodular. In particular, the cocharacter lattice and coroot lattice coincide.*

*Proof.* The explicit description of  $\Lambda_{E_8}$  from Definition 2.6.43 allows us to compute a Gram matrix for a basis of  $\Lambda_{E_8}$ . For explicit details, see [Dol12, Lemma 8.2.6].  $\square$

We now recall some facts stated in [Ree10, Section 2.2]. Any element of  $H$  which acts on Lie  $H$  diagonalizably (over  $\mathbb{C}$ ) is  $H$ -conjugate to an element of  $T$ . Additionally, we have that two elements of  $T$  are  $H$ -conjugate if and only if they are conjugate by  $W_T$ . Any torsion element of  $H$  acts diagonalizably over  $\mathbb{C}$  and is conjugate to an element of  $S$ . The elements  $s = \exp(x)$  and  $s' = \exp(x')$  of  $S$  are conjugate if and only if  $x, x'$  are in the same orbit under action of the *extended affine Weyl group*

$$\widetilde{W}_T := W_T \rtimes Y$$

where  $Y$  acts on  $V$  by translations.

Let  $\Delta := \{\alpha_1, \dots, \alpha_\ell\}$  be a basis of simple roots of  $\Lambda$  and let  $\{\check{\omega}_1, \dots, \check{\omega}_\ell\}$  be the basis of the co-character lattice dual to  $\Delta$ . This means that under the natural pairing we have that  $\langle \alpha_i, \check{\omega}_j \rangle = \delta_{ij}$ , where  $\delta_{ij}$  denotes the Kronecker delta. Let  $\alpha_0 = \sum_{i=1}^{\ell} a_i \alpha_i$  be the highest root of  $\Lambda$  with respect to  $\Delta$  (here the  $a_i$  are positive integers). Let  $v_i := a_i^{-1} \check{\omega}_i$  for  $1 \leq i \leq \ell$  and let  $v_0 := 0$ .

The set

$$C = \left\{ \sum_{i=0}^{\ell} x_i v_i \in V : 0 < x_i < 1 \text{ and } \sum_{i=0}^{\ell} x_i = 1 \right\}$$

is the *alcove* determined by  $\Delta$  (for a proper definition of alcove see [Ree10, Section 2.2]). For each  $g \in \widetilde{W}_T$  we may write  $g \cdot C := \{x \in V : g^{-1}(x) \in C\}$ . Note that the closure of  $C$  is the simplex of dimension  $\ell$  given by the convex hull of  $\{v_0, \dots, v_\ell\}$ . It is a fact that  $g \cdot C \cap C \neq \emptyset$  if and only if  $g \cdot C = C$ . An important group related to  $H$  is the *alcove stabilizer*, which is defined as

$$\Omega := \{g \in \widetilde{W}_T : g \cdot C = C\}.$$

For  $x \in V$ , we further define  $\Omega_x$  to be the subgroup of  $\Omega$  stabilizing  $x$ . It is computationally useful to note that  $\Omega_b = \Omega$  if  $b$  is the barycentre of  $C$ . One has that  $\Omega \cong Y/\mathbb{Z}\Phi^\vee$  and that  $\Omega$  is isomorphic to the fundamental group of  $H$  (see [Ree10, Section 2.2]). The following useful result appears as [Ree10, Proposition 2.1].

**Proposition 2.6.49** (Reeder). *Let  $\bar{C}$  denote the closure of  $C$  in  $V$ . Denote by  $C_H(s)$  the centralizer of  $s$  in  $H$ . For  $s = \exp(x)$  with  $x \in \bar{C}$ , the component group of  $C_H(s)$  is isomorphic to  $\Omega_x$ .*

With the description of  $\Omega$  above, we can now prove some important technical facts about the split adjoint simple group of type  $E_8$ .

**Lemma 2.6.50.** *Let  $H$  be the split adjoint simple group of type  $E_8$  over  $\mathbb{C}$  and let  $\mathfrak{h}$  denote its Lie algebra (i.e,  $\mathfrak{e}_8$ ). Then:*

(a)  *$H$  is simply connected.*

(b)  *$\text{Aut}(\mathfrak{h})$  is connected.*

(c) For  $h \in H(\mathbb{C})$ , let  $\Psi_h$  denote the inner automorphism  $g \mapsto h^{-1}gh$ . Then the differential  $d: \text{Aut}(H) \rightarrow \text{Aut}(\mathfrak{h})$  is an isomorphism and the diagram

$$\begin{array}{ccc} \text{Aut}(H) & \xrightarrow{d} & \text{Aut}(\mathfrak{h}) \\ \uparrow h \mapsto \Psi_h & & \parallel \\ H & \xrightarrow{\text{Ad}} & \text{Aut}(\mathfrak{h})^\circ \end{array}$$

commutes.

(d)  $H$  is isomorphic to its group of automorphisms, and every automorphism is inner.

*Proof.* (a) By Lemma 2.6.48 and the preceding discussion, we have that  $H$  is simply connected.

(b) The result follows immediately from [Bou68, Planche VII] and [FH91, Proposition D.40].

(c) That the differential is an isomorphism follows from (b) and [FH91, Exercise 8.28]. That the diagram commutes follows from the definition of Ad and part (a).

(d) By Theorem 2.6.40 we have that  $h \mapsto \Psi_h$  is injective. The result is immediate from part (c) and the fact that  $H := \text{Aut}(\mathfrak{h})$  by definition. □

We now prove the main result of this section.

**Corollary 2.6.51.** *Let  $H$  be the split group of type  $E_8$  over  $k$  and let  $H_{\mathbb{C}}$  denote the base extension of  $H$  to  $\mathbb{C}$ . Let  $\theta: H_{\mathbb{C}} \rightarrow H_{\mathbb{C}}$  be an involution. Then  $H_{\mathbb{C}}^\theta(\mathbb{C})$  has a single connected component in the euclidian topology. In particular,  $H^\theta$  has a single Zariski connected component and  $H^\theta = (H^\theta)^\circ$ .*

*Proof.* We may assume by base change that  $H$  is a complex Lie group. Recall that  $\Omega \cong Y/\mathbb{Z}\Phi^\vee$  and that  $Y = \mathbb{Z}\Phi^\vee$  for root lattices of type  $E_8$ . By Lemma 2.6.50 we may choose an element  $s \in H(\mathbb{C})$  such that  $s = s^{-1}$  and  $\theta(h) = shs^{-1}$  for all  $h \in H$ . But  $\Omega$  is trivial, so by Proposition 2.6.49 the centralizer of any 2-torsion element has a single connected component. Since  $H^\theta = C_H(s)$  we are done. □

### 2.6.8 Background regarding groups of type $A, D, E$

We make use of some classical results of Vinberg theory, which can be found in [Tho16, Section 1D], [Ric82], or [Vin76]. Let  $H$  be a simple affine algebraic group over  $k$  and let  $\theta: H \rightarrow H$  be an involution over  $k$ . Then  $\theta$  induces an involution  $d\theta: \mathfrak{h} \rightarrow \mathfrak{h}$  on the Lie algebra of  $H$ , and the eigenspaces of  $d\theta$  define a  $(\mathbb{Z}/2)$ -grading of  $\mathfrak{h}$

$$\mathfrak{h} = \mathfrak{h}_0 \oplus \mathfrak{h}_1$$

such that  $[\mathfrak{h}_i, \mathfrak{h}_j] \subseteq \mathfrak{h}_{i+j}$ . We define the varieties

$$\begin{aligned} H^{\theta(h)=h^{-1}} &:= \{h \in H : \theta(h) = h^{-1}\} \\ \mathfrak{h}^{d\theta=-1} &:= \{X \in \mathfrak{h} : d\theta(X) = -X\}. \end{aligned}$$

The main result from Vinberg theory that we are interested in is a version of the Chevalley restriction theorem for  $(\mathbb{Z}/2)$ -graded Lie algebras. We begin with some technical details of the quotients of a rank 8 torus by  $W_{E_8}$  and  $\mathbb{G}_m$ .

**Proposition 2.6.52.** *Let  $T$  be a torus over  $k$  of rank 8 with the standard action by the Weyl group  $W_{E_8}$ . Then the categorical quotient  $T//W_T$  exists in the category of schemes, and  $T//W_T \cong \mathbb{A}_k^n$ .*

*Proof.* See [Ric82, Theorem 14.3]. □

**Lemma 2.6.53.** *Let  $\mathfrak{t}$  be a splitting Cartan subalgebra of the split group of type  $E_8$  over  $k$  and let  $\mathfrak{t}_0 := \mathfrak{t} \setminus \{0\}$ . Then  $\mathfrak{t}_0//W_{\mathfrak{t}}$  can be covered by affine open subsets which are  $\mathbb{G}_m$ -invariant. Consequently,  $\mathfrak{t}_0$  is covered by affine open subschemes invariant under  $W_{\mathfrak{t}} \times \mathbb{G}_m$ , and the action of  $W_{\mathfrak{t}} \times \mathbb{G}_m$  on these subschemes is closed.*

*Proof.* The ring of invariants of  $W_{\mathfrak{t}}$  acting on  $\mathfrak{t}$  is a polynomial ring where  $\mathbb{G}_m$  acts by scaling each variable by its weighted degree [RT17]. The principal open subsets with respect to the monomials give the invariant open cover. □

We now state some results of [Vin76] and [Ric82], as summarized in [Tho16]. Our Theorem 2.6.55 below is a slightly enhanced version of [Tho16, Theorem 1.10]; our enhancement is the addition of part (d). The change allows us to state our results in Chapter 4 for the  $\epsilon_8$  case without the extra data of a tangent vector required at various points for the  $\epsilon_6, \epsilon_7$  cases of Thorne's results.

**Theorem 2.6.54.** (a) *Let  $H$  be a split adjoint simple group of type  $A, D$ , or  $E$ . Let  $Y := (H^{\theta(h)=h^{-1}})^{\circ}$  and let  $G := (H^{\theta})^{\circ}$ . Let  $T$  be a maximal subtorus of  $Y$  and let  $W_T$  be the Weyl group of this torus. Then the inclusion  $T \subseteq Y$  induces an isomorphism*

$$T//W_T \cong Y//G.$$

(b) *Suppose that  $k = k^{\text{sep}}$  and let  $x, y$  be regular semisimple elements. Then  $x$  is  $G(k)$ -conjugate to  $y$  if and only if  $x, y$  have the same image in  $Y//G$ .*

(c) *There exists a discriminant polynomial  $\Delta \in k[Y]$  such that for all  $x \in Y$ ,  $x$  is regular semisimple if and only if  $\Delta(x) \neq 0$ . Furthermore, we have that  $x$  is regular semi-simple if and only if the  $G$ -orbit of  $x$  is closed in  $Y$  and  $\text{Stab}_G(x)$  is finite.*

*Proof.* See [Tho16, Theorem 1.11]. □

**Theorem 2.6.55.**

(a) Let  $H$  be a split adjoint simple group of type  $A, D$ , or  $E$  and let  $\mathfrak{h}$  be its Lie algebra. Let  $V := \mathfrak{h}^{d\theta=-1}$  and let  $G := (H^\theta)^\circ$ . Let  $\mathfrak{t}$  be a Cartan subalgebra of  $V$  and let  $W_{\mathfrak{t}}$  be the Weyl group. Then the inclusion  $\mathfrak{t} \subseteq V$  induces an isomorphism of  $k$ -varieties

$$\mathfrak{t} // W_{\mathfrak{t}} \cong V // G.$$

Additionally,  $V // G$  is isomorphic to affine space.

(b) Suppose that  $k = k^{\text{sep}}$  and let  $x, y$  be regular semisimple elements. Then  $x$  is  $G(k)$ -conjugate to  $y$  if and only if  $x, y$  have the same image in  $V // G$ .

(c) There exists a discriminant polynomial  $\Delta \in k[V]$  such that for all  $x \in V$ ,  $x$  is regular semisimple if and only if  $\Delta(x) \neq 0$ . Furthermore, we have that  $x$  is regular semisimple if and only if the  $G$ -orbit of  $x$  is closed in  $V$  and  $\text{Stab}_G(x)$  is finite.

(d) Moreover, we have that the isomorphism from part (a) induces isomorphisms

$$\begin{array}{ccc} \mathbb{P}\mathfrak{t} // W_{\mathfrak{t}} & \cong & \mathbb{P}V // G \\ \parallel & & \parallel \\ (\mathfrak{t} \setminus \{0\}) // (W_{\mathfrak{t}} \times \mathbb{G}_m) & \cong & (V \setminus \{0\}) // (G \times \mathbb{G}_m). \end{array}$$

*Proof.* The statements of parts (a-c) are directly from [Tho16, Theorem 1.10], so we need only prove the last claim.

By definition, we have that  $\mathbb{P}V := (V \setminus \{0\}) // \mathbb{G}_m$ , where  $\mathbb{G}_m$  acts on  $V$  via  $\lambda g \mapsto (\lambda \cdot \text{id}_V)(g)$ . In particular,  $\lambda$  acts on  $V$  through the centre of  $\text{GL}(V)$ , so we ascertain that  $G \times \mathbb{G}_m$  acts on  $V$ . Moreover, we have that  $G \times \mathbb{G}_m$  acts on  $\mathfrak{t}$  via the inclusion  $i: \mathfrak{t} \hookrightarrow V$ . The action of  $G \times \text{id}_{\mathbb{G}_m}$  on  $\mathfrak{t}$  factors through  $W_{\mathfrak{t}}$  by the first part of the theorem, and the action of  $\text{id}_G \times \mathbb{G}_m$  on  $\mathfrak{t}$  factors faithfully through the centre of  $\text{GL}(\mathfrak{t})$  since  $i$  is a morphism of Lie algebras. Thus, we see that  $W_{\mathfrak{t}} \times \mathbb{G}_m$  acts on  $\mathfrak{t}$  and that this action is compatible with the action of  $G \times \mathbb{G}_m$  on  $V$ .

From part (a), we have that  $i$  induces an isomorphism  $i: \mathfrak{t} // W_{\mathfrak{t}} \cong V // G$ . Since this induced isomorphism is also  $\mathbb{G}_m$ -equivariant, we have

$$\begin{aligned} ((\mathfrak{t} \setminus \{0\}) // \mathbb{G}_m) // W_{\mathfrak{t}} &\cong (\mathfrak{t} \setminus \{0\}) // (W_{\mathfrak{t}} \times \mathbb{G}_m) \\ &\cong ((\mathfrak{t} \setminus \{0\}) // W_{\mathfrak{t}}) // \mathbb{G}_m \stackrel{i}{\cong} ((V \setminus \{0\}) // G) // \mathbb{G}_m \\ &\cong (V \setminus \{0\}) // (G \times \mathbb{G}_m) \cong ((V \setminus \{0\}) // \mathbb{G}_m) // G \end{aligned}$$

which gives the result.  $\square$

We apply the results above to a particular type of involution, which we shall now describe. An involution  $\theta: H \rightarrow H$  over  $k$  is *split* if the affine algebraic group  $(H^\theta)^\circ$  is split. The specific

involutions we are interested in are the stable involutions (in the sense of [Tho13, Section 2]) which are also split.

**Proposition 2.6.56.** *Let  $H$  be a split adjoint simple group of type  $A$ ,  $D$ , or  $E$  over  $k$ . There exists a unique  $H(k)$ -conjugacy class of split involutions  $\theta$  of  $H$  such that  $\text{Tr}(d\theta: \mathfrak{h} \rightarrow \mathfrak{h}) = -\text{rk } H$ .*

*Proof.* See [Tho16, Proposition 1.9]. □

It is convenient to name the involutions satisfying the conditions of Proposition 2.6.56. We adopt the name used in [RLYG12] and [Tho13].

**Definition 2.6.57.** Let  $H$  be a split adjoint simple group of type  $A$ ,  $D$ , or  $E$  over  $k$ . We call an involution  $\theta: H \rightarrow H$  satisfying the conditions of Proposition 2.6.56 a *split stable involution*.

### 2.6.9 A representation of dimension 16

Let  $V_{16}$  be a 16-dimensional  $k$ -vector space and let  $q$  be a quadratic form on  $V_{16}$  with an isotropic  $k$ -subspace of dimension 8. Note that  $q$  is unique up to isometry by the Witt index theorem [Tit66]. It is straightforward to check by choosing an explicit representative for  $q$  that  $\mathfrak{so}(q)$  is the split Lie algebra of type  $D_8$ .

**Lemma 2.6.58.** *Let  $H$  be a split group of type  $E_8$  defined over  $k$  and let  $\theta: H \rightarrow H$  be a split stable involution. Then*

(a) *The Lie algebra  $\text{Lie } H^\theta$  is split and of Dynkin type  $D_8$ . In particular, there is an isomorphism  $\text{Lie } H^\theta \cong \mathfrak{so}(q)$  over  $k$ .*

(b) *The Standard representation of  $\text{Lie } H^\theta$  is a 16-dimensional representation.*

*Proof.* One need only determine the Dynkin type of  $H^\theta$  as the remaining statements are standard facts. By functoriality of Lie, we have that  $\text{Lie } H^\theta = \mathfrak{h}^{d\theta=1}$ , where  $\mathfrak{h}^{d\theta=1}$  denotes the  $+1$ -eigenspace of the involution  $d\theta$  acting on  $\mathfrak{h}$ . Additionally, we have that  $H \cong \text{Aut}(\mathfrak{h})^\circ$  since  $H$  is a split group of type  $E_8$ .

By Proposition 2.6.56 it suffices to demonstrate the claim for a particular split stable involution. Let  $\mathfrak{t}$  be a maximal splitting Cartan subalgebra of  $\mathfrak{h}$  and write

$$\mathfrak{h} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi(\mathfrak{h}, \mathfrak{t})} \mathfrak{h}^\alpha$$

with  $\Phi(\mathfrak{h}, \mathfrak{t})$  denoting the roots of  $\mathfrak{h}$  with respect to  $\mathfrak{t}$ . We fix an identification of  $\Phi(\mathfrak{h}, \mathfrak{t})$  with the  $E_8$  root system in  $\mathbb{R}^8$  (as in [Bou68, Planche 7]) and let  $\Phi_{\mathbb{Z}}(\mathfrak{h}, \mathfrak{t}) \subseteq \Phi(\mathfrak{h}, \mathfrak{t})$  be the roots whose coordinates have integer entries. Define  $d\theta$  by linearly extending

$$d\theta(x) := \begin{cases} x & \text{if } x \in \mathfrak{h}^\alpha, \alpha \in \Phi_{\mathbb{Z}}(\mathfrak{h}, \mathfrak{t}) \\ x & \text{if } x \in \mathfrak{t} \\ -x & \text{if } x \in \mathfrak{h}^\alpha, \alpha \in \Phi(\mathfrak{h}, \mathfrak{t}) \setminus \Phi_{\mathbb{Z}}(\mathfrak{h}, \mathfrak{t}) \end{cases}.$$

We note that for  $\alpha, \beta \in \Phi(\mathfrak{h}, \mathfrak{t})$ , we have that  $\alpha + \beta$  has non-integer coordinates precisely when exactly one of  $\alpha, \beta$  has non-integer coordinates. Using [FH91, Exercise D.5] it is a simple calculation to check that  $d\theta$  preserves the Lie bracket. Thus  $d\theta$  is a split involution of  $\mathfrak{h}$ , which corresponds to a split involution  $\theta \in H$ . Moreover, we see that  $\text{Tr}(d\theta) = -\text{rk } H$ , so  $\theta$  is a split stable involution. It is a standard fact that the Dynkin type of the root system  $\Phi_{\mathbb{Z}}(\mathfrak{h}, \mathfrak{t})$  is  $D_8$ .  $\square$

### 2.6.10 The refined construction of Lurie

We give a short summary of [Tho16, Section 2] as this is helpful to state the main result we rely on. For details the reader is encouraged to consult the original article.

We say that a root lattice  $\Lambda$  is *simply-laced* if the isometry group of the lattice acts transitively on the roots. The *Weyl group* of  $\Lambda$ , denoted by  $W_{\Lambda}$ , is the subgroup of the isometries of  $\Lambda$  generated by reflections through root hyperplanes. Consider the following collection of abstract data:

#### Data I:

1. An irreducible simply laced root lattice  $(\Lambda, \langle \cdot, \cdot \rangle)$  together with a continuous homomorphism  $\text{Gal}(k^{\text{sep}}/k) \rightarrow W_{\Lambda} \subseteq \text{Aut}(\Lambda)$ .
2. A central extension  $\tilde{V}$  of  $V := \Lambda/2\Lambda$ , where  $\tilde{V}$  satisfies

$$0 \longrightarrow \{\pm 1\} \longrightarrow \tilde{V} \longrightarrow V \longrightarrow 0$$

and for any  $\tilde{v} \in \tilde{V}$  we have that  $\tilde{v}^2 = (-1)^{\frac{\langle v, v \rangle}{2}}$ .

3. A continuous homomorphism  $\text{Gal}(k^{\text{sep}}/k) \rightarrow \text{Aut}(\tilde{V})$  leaving  $\{\pm 1\}$  invariant, compatible with  $\text{Gal}(k^{\text{sep}}/k) \rightarrow \text{Aut}(\Lambda) \rightarrow \text{Aut}(V)$ .
4. A finite dimensional  $k$ -vector space  $W$  and a homomorphism  $\rho: \tilde{V} \rightarrow \text{GL}(W)$  of  $k$ -groups.

We denote the ensemble of such data by a quadruplet  $(\Lambda, \tilde{V}, W, \rho)$ . We may form the category  $\mathcal{C}(k)$  of quadruplets satisfying conditions (1)-(4), whose morphisms are the obvious morphisms. Thorne [Tho16, Section 2] presents a modified construction of Lurie [Lur01], which given a quadruplet  $(\Lambda, \tilde{V}, W, \rho)$  produces:

#### Data II:

- (a) A simple Lie algebra  $\mathfrak{h}$  over  $k$  of type equal to the Dynkin type of  $\Lambda$ .
- (b) An affine algebraic group  $H$ , which is the adjoint group over  $k$  whose Lie algebra is  $\mathfrak{h}$ , and a maximal torus  $T$  of  $H$ . The torus  $T$  is canonically isomorphic to  $\text{Hom}(\Lambda, \mathbb{G}_m)$ .
- (c) An involution  $\theta: H \rightarrow H$  which acts on  $T$  by  $\theta(t) = t^{-1}$ .
- (d) An isomorphism  $T[2](k^{\text{sep}}) \cong V^{\vee}$  of Galois modules.
- (e) A Lie algebra homomorphism  $\rho: \mathfrak{h}^{d\theta=1} \rightarrow \mathfrak{gl}(W)$  defined over  $k$ .

We denote the ensemble of such data by a tuple  $(H, \theta, T, \rho)$ , and we may form a category  $\mathcal{D}(k)$  whose objects are tuples satisfying conditions (a)-(e) and whose morphisms are morphisms of the underlying affine algebraic groups  $\varphi: H_1 \rightarrow H_2$  over  $k$  such that  $\varphi$  intertwines the involutions  $\theta$  (i.e,  $\theta_2\varphi = \varphi\theta_1$ ), satisfies  $\rho_2 \circ d\varphi_e = \rho_1$ , and such that  $\varphi(T_1) \subseteq T_2$ . Note that while we require  $\varphi(T_1) \subseteq T_2$ , this inclusion is not necessarily canonically defined. We point out that in Lemma 4.4.3, we construct morphisms in  $\mathcal{D}(k)$  where the tori *are* canonically identified. We phrase the construction of Lurie as modified by Thorne in the following way:

**Theorem 2.6.59.** *For each field  $k$  of characteristic 0, there is a functor  $f_k: \mathcal{C}(k) \rightarrow \mathcal{D}(k)$  which is injective on objects.*

**Remark 2.6.60.** One can infer that this functor is injective on objects from the appendix of [Tho16], due to Kaletha.

## 2.7 Theta groups of curves

We follow [Tho16, Section 1C] for an exposition on theta groups and Heisenberg groups, with some extra details provided from [Mil86b].

Let  $C/k$  be a curve of genus  $g$ , let  $r$  be a positive integer, and denote

$$C^r := \underbrace{C \times \dots \times C}_{r \text{ times}}$$

There is a natural morphism given by

$$\begin{aligned} j^r: \quad C^r &\rightarrow \text{Pic}^r(C) \\ (P_1, \dots, P_r) &\mapsto [P_1 + \dots + P_r] \end{aligned}$$

where the square brackets indicate taking the divisor class. The image of  $j^{g-1}$  is an irreducible subvariety of  $\text{Pic}^{g-1}(C)$  of codimension 1, and we let  $W_{g-1}$  denote the corresponding divisor of  $\text{Pic}^{g-1}(C)$ . If  $P_0 \in C(k^{\text{sep}})$  is any point, then there is a morphism  $\tau_{(g-1)P_0}: \text{Pic}^0(C)_{k^{\text{sep}}} \rightarrow \text{Pic}^{g-1}(C)_{k^{\text{sep}}}$  given by translation by  $(g-1)P_0$ . The divisor  $\Xi := \tau_{(g-1)P_0}^* W_{g-1}$  of  $\text{Pic}^0(C)_{k^{\text{sep}}}$  is a *theta divisor* of  $\text{Pic}^0(C)_{k^{\text{sep}}}$ . See [Mil86b, Theorem 6.6] for further details.

**Definition 2.7.1.** Let  $C/k$  be a smooth projective curve of genus  $g$  and let  $\kappa_C$  denote the canonical divisor class of  $C$ . A *theta characteristic* is a divisor class  $\vartheta \in \text{Pic}^{g-1}(C)(k^{\text{sep}})$  such that  $2\vartheta = \kappa_C$ . We say that  $\vartheta$  is *odd* if the integer  $h^0(C, \vartheta)$  is odd and say it is even otherwise.

Recall that we may identify  $J_C$  and  $\text{Pic}^0(C)$ , and let  $\mathcal{L}_\vartheta := \mathcal{O}_{J_C}(2\tau_\vartheta^* W_{g-1})$ , where  $\tau_\vartheta: \text{Pic}^0(C) \rightarrow \text{Pic}^{g-1}(C)$  denotes the translation by  $\vartheta$ . Then the isomorphism class of  $\mathcal{L}_\vartheta$  is independent of the choice of  $\vartheta$ , and there is a line bundle  $\mathcal{L}_0$  defined over  $k$  such that  $(\mathcal{L}_0 \otimes_k k^{\text{sep}}) \cong (\mathcal{L}_\vartheta \otimes_k k^{\text{sep}})$ . Note that if  $\omega \in J_C[2]$ , then  $\tau_\omega^* \mathcal{L}_\vartheta \cong \mathcal{L}_\vartheta$  and in particular we have that  $\tau_\omega^* \mathcal{L}_0 \cong \mathcal{L}_0$  over  $k^{\text{sep}}$ . We direct the reader to [Tho16, Section 1C] for verification of these details.

Let  $A \in J_C(k)$  and choose a  $B \in J_C(k^{\text{sep}})$  such that  $[2]B = A$ . The isomorphism class of the line bundle  $\tau_B^* \mathcal{L}_0$  is independent of the choice of  $B$ , and there is a line bundle  $\mathcal{L}_B$  defined over  $k$  such that over  $k^{\text{sep}}$  there is an isomorphism  $\mathcal{L}_B \cong \tau_B^* \mathcal{L}_0$ . Furthermore, note that  $\mathcal{L}_0$  and  $\mathcal{L}_B$  are isomorphic over  $k(B)$ , but in general are not isomorphic over  $k$ . If  $A = B = 0 \in J_C(k)$ , then  $\tau_B^* \mathcal{L}_0 = \mathcal{L}_0$ . We refer to [Tho16, Section 1C] again for details. We make use of the following well-known fact about  $\mathcal{L}_0$  in Section 4.4.

**Lemma 2.7.2.** *Let  $B/k^{\text{sep}}$  be a genus  $g$  curve with theta characteristic  $\vartheta$ . Then*

$$h^0(\text{Pic}^0(B), \mathcal{L}_0) = 2^g.$$

*Proof.* See [BL04, Chapter IV, Section 8]. □

We may construct an important group from each of the line bundles considered above, which turns out to capture important information about the arithmetic of  $C$ .

**Definition 2.7.3.** Let  $\mathcal{L}$  be a line bundle on  $J_C$  defined over  $k$  such that  $\tau_\omega^* \mathcal{L} \cong \mathcal{L}$  for each  $\omega \in J_C[2](k^{\text{sep}})$ . The *Heisenberg group*  $\tilde{H}_{\mathcal{L}}$  associated to  $\mathcal{L}$  is the  $k$ -group of pairs  $(\phi, \omega)$  such that  $\omega \in J_C[2](k^{\text{sep}})$  and  $\phi: \mathcal{L} \rightarrow \tau_\omega^* \mathcal{L}$  is an isomorphism of line bundles of  $J_C$ .

To clarify Definition 2.7.3, we think of  $J_C[2]$  as a  $k$ -group in this context. We have the exact sequence of  $k$ -groups

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \tilde{H}_{\mathcal{L}} \longrightarrow J_C[2] \longrightarrow 0$$

with the last map given by the natural projection. If  $B \in J_C(k^{\text{sep}})$  such that  $[2]B \in J_C(k)$  then we have that, over  $k(B)$ , the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \tilde{H}_{\mathcal{L}_0} & \longrightarrow & J_C[2] \longrightarrow 0 \\ & & \parallel & & \downarrow \tau_B^* & & \parallel \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \tilde{H}_{\mathcal{L}_B} & \longrightarrow & J_C[2] \longrightarrow 0 \end{array}$$

commutes. Heisenberg groups are explicit examples of theta groups.

**Definition 2.7.4.** Let  $C/k$  be a curve. A *theta group* of  $J_C[2]$  is a central extension of  $k$ -groups

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \Theta \longrightarrow J_C[2] \longrightarrow 0$$

such that the commutator pairing on  $\Theta$  descends to the Weil pairing on  $J_C[2]$ . A *morphism of theta groups* is a morphism such that the following diagram commutes:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Theta_1 & \longrightarrow & J_C[2] \longrightarrow 0 \\ & & \parallel & & \downarrow \psi & & \parallel \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Theta_2 & \longrightarrow & J_C[2] \longrightarrow 0. \end{array}$$

We use the following well-known facts about theta groups of  $J_C[2]$ .

**Proposition 2.7.5.** *Let  $C/k$  be a curve of genus  $g$ .*

- (a) *Then there is a canonical identification between  $k$ -isomorphism classes of theta groups of  $C$  and elements of  $H^1(k, J_C[2])$  such that the isomorphism class of the Heisenberg group  $\tilde{H}_{\mathcal{L}_0}$  is identified with the trivial cocycle.*
- (b) *If  $\Theta$  is a theta group of  $J_C[2]$  and  $C(k) \neq \emptyset$ , there is an injective morphism of  $k$ -groups  $\rho: \Theta \rightarrow \mathrm{GL}_{2g}$ .*
- (c) *Let  $A \in J_C(k)$ , and let  $B \in J_C(k^{\mathrm{sep}})$  such that  $[2]B = A$ . Let  $\tau_B: J_C \rightarrow J_C$  be the translation-by- $B$  morphism and let  $\mathcal{L}_B = \tau_B^* \mathcal{L}$ . Then the cocycle class  $(\sigma \mapsto [B^\sigma - B]) \in H^1(k, J_C[2])$  corresponds to the isomorphism class of  $\tilde{H}_{\mathcal{L}_B}$ , and the isomorphism class of  $\tilde{H}_{\mathcal{L}_B}$  is independent of the choice of  $B$ .*

*Proof.* Statements (a) and (b) are well-known facts about theta groups. The result for elliptic curves can be found in [CFO<sup>+</sup>08, Section 1], and the results generalize with minimal modifications to the proofs. We provide a summary of the details we require in Appendix A. Statement (c) can be found in [Tho16, Section 1C].  $\square$

If  $\tilde{H}_{\mathcal{L}_B}$  is a Heisenberg group, we can describe the morphism  $\tilde{H}_{\mathcal{L}_B} \rightarrow \mathrm{GL}_{2g}$  from Proposition 2.7.5(b) more explicitly; the natural action of  $\tilde{H}_{\mathcal{L}_B}$  on  $H^0(\mathrm{Pic}^0(C), \mathcal{L}_B)$  induces a morphism  $\tilde{H}_{\mathcal{L}_B} \rightarrow \mathrm{GL}_{2g}$ . Additionally, the cocycle class  $(\sigma \mapsto [B^\sigma - B])$  in the statement of Proposition 2.7.5(c) is exactly the image of  $A \in \frac{J_C(k)}{2J_C(k)}$  under the connecting homomorphism of the long exact sequence in cohomology arising from the Kummer sequence

$$0 \longrightarrow J_C[2] \longrightarrow J_C \xrightarrow{[2]} J_C \longrightarrow 0.$$

For further details, see [HS00, Section C.4].

## 2.8 Uniquely trigonal genus 4 curves, del Pezzo surfaces of degree 1, and $E_8$

### 2.8.1 Del Pezzo surfaces

We state some facts regarding the connection between del Pezzo surfaces and certain genus 4 curves.

**Definition 2.8.1.** We say that eight points  $P_1, \dots, P_8 \in \mathbb{P}^2(k^{\mathrm{al}})$  are in *general position* if no two are coincident, no three lie on a line, no six lie on a conic, and any cubic passing through all eight points is non-singular at each of these points.

**Lemma 2.8.2.** *Let  $P_1, \dots, P_8$  be eight points of  $\mathbb{P}^2$  in general position. Then the vector space of cubic forms vanishing on  $P_1, \dots, P_8$  is 2-dimensional. Moreover, if  $f$  is such a cubic form, then it is irreducible.*

*Proof.* Let  $V$  be the space of cubic forms vanishing on  $P_1, \dots, P_8$ . Elementary linear algebra shows that  $\dim V \geq 2$ . If  $u, v, w \in V$  were 3 linearly independent cubics, then with  $(a : b : c) = P_1$  and  $f_x(P_1) := \frac{\partial f}{\partial x}(a, b, c)$ , we have for some non-zero  $(\lambda_1, \lambda_2, \lambda_3) \in k^3$  that

$$\lambda_1 \begin{bmatrix} u_x(P_1) \\ u_y(P_1) \\ u_z(P_1) \end{bmatrix} + \lambda_2 \begin{bmatrix} v_x(P_1) \\ v_y(P_1) \\ v_z(P_1) \end{bmatrix} + \lambda_3 \begin{bmatrix} w_x(P_1) \\ w_y(P_1) \\ w_z(P_1) \end{bmatrix} = 0,$$

since the tangent vectors of  $Z(u), Z(v), Z(w)$  at  $P_1$  must be linearly dependent. In particular, the cubic  $Z(\lambda_1 u + \lambda_2 v + \lambda_3 w)$  would pass through all 8 points and be singular at  $P_1$ , violating the general position assumption.

A reducible cubic through eight points must either have at least 3 points which lie on a linear component or have at least 6 points lie on a conic component, neither of which is admissible.  $\square$

**Definition 2.8.3.** A *del Pezzo surface of degree 1* is a smooth projective surface which is isomorphic over an algebraically closed field to the blow-up of  $\mathbb{P}^2$  at 8 points in general position.

Let  $S/k$  be a del Pezzo surface of degree 1 and let  $\kappa_S$  be the canonical divisor of  $S$ . We have that  $-3\kappa_S$  is very ample, and the model of  $S$  given by the associated linear system embeds  $S$  as a smooth sextic hypersurface in the weighted projective space  $\mathbb{P}(1 : 1 : 2 : 3)$  [Dol12, Section 8.3]. Conversely, any smooth sextic hypersurface in  $\mathbb{P}(1 : 1 : 2 : 3)$  is a del Pezzo surface of degree 1. If the characteristic of  $k$  is not equal to 2 then we can write

$$S: z^2 = c_0 w^3 + c_2(x, y)w^2 + c_4(x, y)w + c_6(x, y)$$

with each  $c_m$  homogeneous in  $x, y$  of degree  $m$  and  $c_0 \neq 0$ . The linear system associated to the divisor  $-2\kappa_S$  determines a rational map  $S \dashrightarrow \mathbb{P}(1 : 1 : 2)$  of generic degree 2 which is defined everywhere aside from the single base-point of  $|-2\kappa_S|$ . There is an order 2 automorphism of  $S$  which exchanges the branches of this rational map called the *Bertini involution*. The fixed locus of the Bertini involution is the union of a smooth irreducible curve and the isolated base-point. We call the component which is the smooth irreducible curve the *branch curve*. On the model above the Bertini involution is given by  $(x : y : w : z) \mapsto (x : y : w : -z)$ , and furthermore, we see that the fixed locus of the Bertini involution is the union of the point  $(0 : 0 : c_0 : c_0^2)$  and the subvariety of  $S$  where  $z$  vanishes. The vanishing locus of  $z$  has dimension 1. For details, see [Dol12, Section 8.8.2].

**Proposition 2.8.4** ([Vak01, Zar08]). *Let  $S$  be a del Pezzo surface of degree 1 defined over a characteristic 0 field  $k$  and let  $\iota: S \rightarrow S$  be the Bertini involution and let  $C$  be the irreducible 1-dimensional subvariety of the fixed locus of  $\iota$ . Let  $O$  be the base point of the linear system  $|-2\kappa_S|$ .*

(a) *Let  $\mathcal{E}$  be the blow-up of  $S$  at  $O$ . Then there is a morphism  $\pi: \mathcal{E} \rightarrow \mathbb{P}^1$  that gives  $\mathcal{E}$  the structure of an elliptic surface with identity section  $O$  and such that each fibre of  $\pi$  is the strict transform of a curve  $D$  on  $S$  whose associated Weil-divisor is an anti-canonical divisor of  $S$ .*

- (b) We have that  $C$  is a smooth non-hyperelliptic irreducible curve of genus 4. The strict transform of  $C$  in  $\mathcal{E}$  is the multi-section  $\mathcal{E}[2] \setminus \text{id}_{\mathcal{E}}$ . Moreover, the restriction of  $\pi$  to  $C$  is a morphism  $f: C \rightarrow \mathbb{P}^1$  of degree 3.
- (c) Denote by  $S_{k^{\text{sep}}}$  the base-change of  $S$  to  $k^{\text{sep}}$ . Each exceptional curve on  $S_{k^{\text{sep}}}$  corresponds to a unique class in  $\text{Pic } S_{k^{\text{sep}}}$ . Moreover,  $\text{Pic } S_{k^{\text{sep}}}$  is generated by the exceptional curves on  $S$ . Furthermore,  $\text{Pic } S_{k^{\text{sep}}}$  is generated by a set of 8 pairwise orthogonal exceptional curves and the canonical class.
- (d) Every exceptional curve on  $S_{k^{\text{sep}}}$  restricts to an odd theta characteristic of  $C$  and the anti-canonical divisor of  $S$  restricts to an even theta characteristic of  $C$ .
- (e)  $\text{rk Pic}(S)(k) - 1 \leq \text{rk}_2 J_C[2](k)$

We require a minor technical lemma to describe the fibres of the elliptic surface in Proposition 2.8.4.

**Lemma 2.8.5.** *Let  $S$  be a del Pezzo surface of degree 1 and let  $\pi: \mathcal{E} \rightarrow \mathbb{P}^1$  be the elliptic surface from Proposition 2.8.4. Then:*

- (a)  $\mathcal{E}$  is smooth.
- (b) The fibres of  $\pi$  are irreducible. Consequently, the special fibre  $\mathcal{E}_t$  has multiplicative reduction if and only if it is isomorphic to a nodal rational curve, and it has additive reduction if and only if it is isomorphic to a cuspidal rational curve.
- (c)  $\mathcal{E}$  is minimal over  $\mathbb{P}^1$ .

*Proof.* That  $\mathcal{E}$  is smooth follows from the fact that  $X$  is smooth and Proposition 2.2.13.

Note that it suffices to prove claims (b) and (c) over an algebraically closed field. For part (b), choose a model such that  $S$  is isomorphic to the blow-up of  $\mathbb{P}^2$  at eight points in general position. Let  $Z \subseteq \mathbb{P}^2$  denote this set of eight points, let  $O \in \mathbb{P}^2(k^{\text{al}})$  be the unique point such that any cubic passing through  $Z$  also passes through  $O$ , and let  $Z' := Z \cup \{O\}$ . In particular, we have that  $\mathcal{E} = \text{Bl}_{Z'} \mathbb{P}^2$ . Since the points of  $Z$  are in general position, we have that  $O \notin Z$  and that any cubic passing through the points of  $Z$  is irreducible. The blow-down of any fibre of  $\pi$  to  $\mathbb{P}^2$  is a plane cubic passing through the points of  $Z$ , so we are done by Lemma 2.8.2.

We now prove part (c). Let  $S$  be a minimal model of  $\mathcal{E}$  over  $\mathbb{P}^1$  and let  $\phi: \mathcal{E} \rightarrow S$  be a morphism over  $\mathbb{P}^1$  with birational inverse. By Proposition 2.2.14 we have that  $\phi$  factors over  $k^{\text{al}}$  into monoidal transformations. If  $E$  is an exceptional curve of one of these monoidal transformations, then  $\phi(E)$  is a single point. But  $\phi$  is a morphism over  $\mathbb{P}^1$ , so the only way this is possible is if  $E$  is contained in a fibre of  $\pi$ . This is a contradiction, as all of the fibres are irreducible and have self intersection 0.  $\square$

## 2.8.2 Uniquely trigonal genus 4 curves

We now describe the classically understood relation between the  $E_8$  lattice, del Pezzo surfaces of degree 1, and uniquely trigonal genus 4 curves. We point out that [Tho16] relies on the analogous connections between plane quartic curves, del Pezzo surfaces of degree 2, and the  $E_7$  lattice.

Generally, a genus 4 curve is trigonal in two different ways, and the corresponding linear systems of divisors can be found as follows. A canonical model of a non-hyperelliptic genus 4 curve is a complete intersection of a quadric and a cubic in  $\mathbb{P}^3$ . A linear system of lines on the quadric induces a linear system of degree 3 and dimension 1 on the curve. In the general case, the quadric is nonsingular and has two such linear systems. In the special case where the quadric has a singular point, there is only one such linear system. In that case the curve is trigonal in only one way.

**Definition 2.8.6.** Let  $C/k$  be a smooth curve of genus  $g$ . We say that  $C$  is a *uniquely trigonal* curve if there is a morphism  $f: C \rightarrow \mathbb{P}_k^1$  of degree 3 defined over  $k$  and if for any two morphisms  $f, f': C_{k^{\text{sep}}} \rightarrow \mathbb{P}_{k^{\text{sep}}}^1$  of degree 3, there is a  $\tau \in \text{Aut}(\mathbb{P}_{k^{\text{sep}}}^1)$  such that  $f = \tau \circ f'$ .

**Remark 2.8.7.** It is impossible for a smooth curve of genus greater than 2, defined over a characteristic 0 field, to be both trigonal and hyperelliptic [Vak01, Section 2.8].

Let  $C$  be the branch curve of the Bertini involution of a degree 1 del Pezzo surface  $S$ . The linear system associated to the divisor  $-\kappa_S$  determines a rational map  $\pi_S: S \dashrightarrow \mathbb{P}^1$  which restricts to a degree 3 morphism  $f_C: C \rightarrow \mathbb{P}^1$ . The sections of the anti-canonical bundle of  $S$  are precisely the fibres of  $\pi_S$ . For details, see [Dol12, Section 8.8.3]. Theorem 2.8.8 is a compilation of classical facts.

**Theorem 2.8.8.** *Let  $C/k$  be a curve of genus 4 which is not hyperelliptic. Then the following are equivalent:*

- (a) *The curve  $C/k^{\text{sep}}$  is a uniquely trigonal curve.*
- (b) *The canonical model of  $C$  is the intersection of a cubic and a quadric cone in  $\mathbb{P}^3$ .*
- (c) *There is a vanishing even theta characteristic of  $C$ . That is, there is an isomorphism class of line bundles on  $C_{k^{\text{sep}}}$  such that for any member  $\mathcal{L}_\vartheta$ , we have that  $\mathcal{L}_\vartheta^{\otimes 2}$  is isomorphic to the canonical bundle and  $h^0(C_{k^{\text{sep}}}, \mathcal{L}_\vartheta)$  is a positive even integer.*
- (d) *There is a unique vanishing even theta characteristic of  $C$ .*

*Furthermore,  $C/k$  is uniquely trigonal if and only if there is a del Pezzo surface  $S$  of degree 1 defined over  $k$  such that  $C$  is the branch curve of the Bertini involution on  $S$ . If  $k = k^{\text{sep}}$  then  $S$  is unique up to isomorphism.*

*Proof.* Parts (a), (b), (c), and the last assertion can be found in [Vak01, Section 2.8] and [Vak01, Proposition 3.2]. Part (c) follows trivially from part (d). To show (c) implies (d), if  $\mathcal{L}_{\vartheta_1}$  and  $\mathcal{L}_{\vartheta_2}$  are two line bundles corresponding to vanishing theta characteristics, then  $h^0(C_{k^{\text{sep}}}, \mathcal{L}_{\vartheta_1} \otimes \mathcal{L}_{\vartheta_2}) \geq 4$ .

The Riemann-Roch theorem shows that  $\mathcal{L}_{\vartheta_1} \otimes \mathcal{L}_{\vartheta_2}$  is equivalent to the canonical bundle, so it follows after a simple calculation that  $\mathcal{L}_{\vartheta_1} \cong \mathcal{L}_{\vartheta_2}$ .  $\square$

Let  $S/k$  be a del Pezzo surface of degree 1. It is a classical fact that  $\text{Pic } S_{k^{\text{sep}}} \cong \mathbb{Z}^9$  as a group, and that the intersection pairing  $\langle \cdot, \cdot \rangle$  on  $S$  imbues  $\text{Pic } S_{k^{\text{sep}}}$  with the structure of a lattice. As the canonical class  $\kappa_S$  is always defined over  $k$ , the sublattice

$$(\text{Pic } S_{k^{\text{sep}}})^\perp := \{x \in \text{Pic } S_{k^{\text{sep}}} : \langle x, \kappa_S \rangle = 0\}$$

is also defined over  $k$ . Moreover, it is a classical fact that  $(\text{Pic } S_{k^{\text{sep}}})^\perp$  is isomorphic to a simply laced lattice of Dynkin type  $E_8$ . Note that the Weyl group  $W_{E_8}$  is also the isometry group for this lattice. Additionally, the Bertini involution of  $S$  acts on  $(\text{Pic } S_{k^{\text{sep}}})^\perp$  via the unique nontrivial element of the centre of  $W_{E_8}$ . We label the elements of the centre of  $W_{E_8}$  by  $\pm 1$  and we let  $W_+ := W_{E_8}/\langle \pm 1 \rangle$ . For details, see [Zar08, Section 2.2].

**Definition 2.8.9.** A *marked del Pezzo surface* of degree 1 is a pair  $(S/k, B)$  with  $S/k$  a del Pezzo surface of degree 1 and  $B = \{e_1, \dots, e_8\}$  a subset of  $\text{Pic}(S_{k^{\text{sep}}})$  such that  $\langle e_i, e_i \rangle = -1$  for each  $i$  and  $\langle e_i, e_j \rangle = 0$  for all  $i \neq j$ . We refer to the choice of subset  $B$  as a *marking*. A marking is *Galois invariant* if the set  $B$  is Galois invariant.

If  $(S/k, B)$  is a del Pezzo surface of degree 1 with a Galois invariant marking, then there is a Galois invariant set  $Z$  of 8 points in  $\mathbb{P}^2(k^{\text{sep}})$  and an isomorphism  $\psi: \text{Bl}_Z \mathbb{P}^2 \rightarrow S/k$  defined over  $k$ . Additionally, if  $\{e'_1, \dots, e'_8\}$  are the eight exceptional curves of the blow-up, then  $\psi(e'_1), \dots, \psi(e'_8)$  are effective representatives for the elements of  $B$ . We make use of the following two classical results regarding degree 1 del Pezzo surfaces. These are analogous to the results used in [Tho16] for degree 2 del Pezzo surfaces.

**Proposition 2.8.10.** *Let  $C$  be the branch curve of the Bertini involution of a degree 1 del Pezzo surface  $S/k$  and let  $\Lambda := (\text{Pic } S_{k^{\text{sep}}})^\perp$ . Then there is a commutative diagram of finite  $k$ -groups*

$$\begin{array}{ccc} \Lambda^\vee/2\Lambda^\vee & \xrightarrow{\cong} & (\text{Pic}(C)/\mathbb{Z}\vartheta_C)[2] \\ \uparrow & & \uparrow \\ N_C & \xrightarrow{\cong} & \text{Pic}^0(C)[2] \end{array}$$

where  $N_C$  is the image of

$$\begin{array}{ccc} \gamma: \Lambda/2\Lambda & \rightarrow & \Lambda^\vee/2\Lambda^\vee \\ v & \mapsto & \langle v, \cdot \rangle \end{array}$$

and  $\vartheta_C$  is the divisor class of the vanishing even theta characteristic of  $C$ . In particular, there is a canonical surjection  $\Lambda/2\Lambda \rightarrow \text{Pic}^0(C)[2]$ .

**Proposition 2.8.11.** *Let  $\phi: \Lambda/2\Lambda \rightarrow \text{Pic}^0(C)[2]$  be the surjection of Proposition 2.8.10. Let  $\langle \cdot, \cdot \rangle_2$  be the natural symplectic form on  $\Lambda/2\Lambda$  induced by the form  $\langle \cdot, \cdot \rangle$  on the even lattice  $\Lambda$  and let  $e_2(\cdot, \cdot)$  be the Weil pairing on  $\text{Pic}^0(C)[2]$ . Then for all  $v_1, v_2 \in \Lambda/2\Lambda$  we have*

$$\langle v_1, v_2 \rangle_2 = e_2(\phi v_1, \phi v_2).$$

For the proofs of Proposition 2.8.10 and Proposition 2.8.11, see [Zar08, Lemma 2.4], [Zar08, Lemma 2.7], and [Zar08, Theorem 2.10]. From these propositions we see that a marking of a degree 1 del Pezzo surface determines a marking of the 2-torsion of its branch curve. Additionally, two markings  $B, B'$  of a del Pezzo surface  $S$  of degree 1 determine the same marking of the branch curve if and only if  $\iota(B) = B'$ , where  $\iota$  is the Bertini involution. For additional details, see [Çel18, Section 1.2.3]. Finally, we define a technical condition on uniquely trigonal genus 4 curves useful in Chapter 4 to identify the uniquely trigonal genus 4 curves arising from del Pezzo surfaces that are birational to  $\mathbb{P}^2$  over  $k$ .

**Definition 2.8.12.** A uniquely trigonal genus 4 curve is *of split type* if it is the branch curve of a del Pezzo surface of degree 1 with a Galois invariant marking.

## Chapter 3

# Class groups of cubic fields

### 3.1 Introduction

We explicitly construct an infinite family of cubic number fields and prove in Theorem 3.3.9 that the class group of “most” members of this family has 2-rank at least 8. To do this, we use a construction of trigonal genus 4 curves described in Section 3.2 that allows us good control over both the 2-torsion in the Jacobian and the ramification of the trigonal map. Finally, in Section 3.4 we consider the situation where  $C$  is a trigonal genus 4 curve,  $f: C \rightarrow \mathbb{P}_{\mathbb{Q}}^1$  is a degree 3 morphism to  $\mathbb{P}_{\mathbb{Q}}^1$ , and  $\text{Aut}_{\mathbb{Q}^{\text{al}}}(C/\mathbb{P}_{\mathbb{Q}}^1) \cong \mu_3$ . In this set-up, the cubic number fields defined by the fibres of  $f$  become Galois extensions of  $\mathbb{Q}(\mu_3)$  after tensoring with  $\mathbb{Q}(\mu_3)$ . We comment on the application of the method in Section 3.3 to this specific case.

### 3.2 Del Pezzo surfaces, elliptic surfaces, and curves of genus 4: Applications

In this section, we apply the results of Section 2.8 to construct a genus 4 curve essential to the proof of Theorem 3.3.9. We begin by providing some corollaries of Proposition 2.8.4.

**Proposition 3.2.1.** *Let  $X$  be a degree 1 del Pezzo surface defined over a number field  $k$ , let  $\mathcal{E}$  be the associated elliptic surface from Proposition 2.8.4, and let  $f: C \rightarrow \mathbb{P}_k^1$  be the degree 3 morphism from Proposition 2.8.4(b). Then the ramification of  $f$  over  $p \in \mathbb{P}_k^1$  is classified by the reduction type of the fibre  $\mathcal{E}_p$ . In particular, if one of the special fibres of  $\pi: \mathcal{E} \rightarrow \mathbb{P}_k^1$  has additive reduction then  $f$  has a totally ramified fibre.*

*Proof.* Since  $f$  is defined over a number field and  $\deg f = 3$  we can determine the set of ramification indices of points in the fibre over  $p$  by counting the number of  $k^{\text{al}}$ -points in the fibre over  $p$  on a smooth model of  $C$ . We can also determine the reduction type of  $\mathcal{E}_p$  by counting the number of  $k^{\text{al}}$ -points in  $(\mathcal{E}[2] \setminus \text{id}_{\mathcal{E}})_p$ . Since  $C$  is isomorphic to  $\mathcal{E}[2] \setminus \text{id}_{\mathcal{E}}$  as a subvariety of  $\mathcal{E}$  over  $\mathbb{P}_k^1$  and  $C$  is smooth, these two quantities are equal for every  $p \in \mathbb{P}^1(k^{\text{al}})$ .  $\square$

By using curves arising from del Pezzo surfaces we can control  $J_C(\mathbb{Q})[2]$  via  $\text{rk Pic}(X)(\mathbb{Q})$ ; the latter group is easier to control. To be specific, if  $X$  is the blow-up of eight (rational) points on  $\mathbb{P}^2$  in general position then  $\text{Pic}(X)$  is generated by the (rational) exceptional curves of the blow-up and the canonical divisor. Proposition 2.8.4 implies that  $\text{rk}_2 J_C[2](\mathbb{Q}) = 8$ , where  $C$  is the branch curve of the Bertini involution of  $X$ . Among the curves constructed in this way, we can easily identify those whose trigonal morphism has a totally ramified fibre.

**Proposition 3.2.2.** *Let  $X$  be a del Pezzo surface such that  $\text{rk Pic}(X)(\mathbb{Q}) = 9$  and let  $C$  be the branch curve of the Bertini involution with trigonal morphism  $f: C \rightarrow \mathbb{P}^1$ . Write  $X := \text{Bl}_Z \mathbb{P}^2$  where  $Z$  is a collection of 8 rational points in general position. Then there is a one-to-one correspondence between totally ramified points of  $f$  and cuspidal cubic plane curves through  $Z$ .*

*Proof.* Let  $Y$  be a cuspidal cubic passing through  $Z$ , let  $u$  be a cubic form defining  $Y$ , and let  $P \in Y$  be the cusp. Note the criterion that  $Z$  be in general position forces  $P \notin Z$  (points of  $Z$  being in general position, there is no cubic passing through the points of  $Z$  with a singularity at one of them).

The eight points of  $Z$  determine a pencil of cubic forms  $\{\lambda u + \mu v : (\mu : \lambda) \in \mathbb{P}^1\}$ . Such a pencil has a base locus which consists of 9 points, these being the points of  $Z$  as well as an additional point  $O$ . Intersection multiplicities ensure that  $O$  is not a cusp or node of any of the curves in the pencil.

It follows that the rational map  $g(x, y, z) \mapsto (u(x, y, z) : v(x, y, z))$  is defined outside of  $Z \cup O$ , so by the universal property of blowing up there is a morphism  $\pi$  such that the diagram

$$\begin{array}{ccc} & & \text{Bl}_{Z \cup O} \mathbb{P}^2 \\ & \swarrow \phi & \downarrow \pi \\ \mathbb{P}^2 & \xrightarrow{g} & \mathbb{P}^1 \end{array}$$

commutes, where  $\phi$  is the blow-down morphism. We have that  $\mathcal{E} := \text{Bl}_{Z \cup O} \mathbb{P}^2$  is an elliptic surface over  $\mathbb{P}^1$  whose identity section is the exceptional curve lying over  $O$ . Note by Lemma 2.8.5 that the fibres of  $\pi: \mathcal{E} \rightarrow \mathbb{P}^1$  are irreducible. Because  $Y$  is precisely the closure of the locus  $\{Q \in \mathbb{P}^2 : g(Q) = (0 : 1)\}$ , the strict transform of  $Y$  is in fact a fibre of  $\pi$ . Since  $P \notin Z \cup O$  we have that the strict transform of  $Y$  remains singular (with a cusp) in  $\mathcal{E}$ . Thus the fibre over  $(0 : 1)$  is a special fibre of  $\pi: \mathcal{E} \rightarrow \mathbb{P}^1$ . We see that  $\mathcal{E}$  has additive reduction at  $(0 : 1)$ , so by Proposition 3.2.1 corresponds to a totally ramified point of  $f: C \rightarrow \mathbb{P}^1$ .

Conversely, if  $Q$  is a totally ramified point of  $f: C \rightarrow \mathbb{P}^1$  then Proposition 3.2.1 shows it is the cusp of a special fibre  $\mathcal{E}_p$  whose reduction type is additive. In particular  $Q$  does not lie on  $\phi^{-1}(Z \cup O)$  so the blow-down of  $\mathcal{E}_p$  is a cuspidal plane curve. That it is cubic follows from the fact that every fibre of  $\mathcal{E}$  blows down to a cubic curve.  $\square$

We present here for the convenience of the reader the procedure given in [Zar08] to get explicit equations for the branch curve. Note that in our example  $\mathbb{P}^2$  and the del Pezzo surface  $X$  are bira-

tional over  $\mathbb{Q}$ , so we may identify their function fields. We have that  $\kappa_X = E_1 + \dots + E_8 - 3H$  is a canonical divisor for  $X$ , where  $H$  is the pullback of the hyperplane class on  $\mathbb{P}^2$  and the  $E_i$  are the 8 pairwise orthogonal exceptional curves lying over the blown up points of  $\mathbb{P}^2$ . Thus,

$$L(-\kappa_X) = \langle u, v \rangle$$

where  $u, v \in \mathbb{Q}[x, y, z]$  are cubic forms passing through the 8 base-points of the blow-up. Similarly, we have

$$L(-2\kappa_X) = \langle u^2, uv, v^2, w \rangle$$

with  $w$  a function on  $X$  not in the  $k$ -span of  $\{u^2, uv, v^2\}$ . We have that  $L(-2\kappa_X)$  defines a 2-to-1 rational map  $\varphi: \mathbb{P}^2 \rightarrow \mathbb{P}(1 : 1 : 2)$  via

$$\varphi: (x : y : z) \mapsto (u(x, y, z) : v(x, y, z) : w(x, y, z))$$

with a unique base-point that is  $O$ . In fact, if

$$X: z^2 = c_0 w^3 + c_2(u, v)w^2 + c_4(u, v)w + c_6(u, v)$$

is the model of  $X$  in  $\mathbb{P}(1 : 1 : 2 : 3)$  provided by  $L(-3\kappa_X)$  and  $\phi: X \rightarrow \mathbb{P}(1 : 1 : 2)$  is the projection onto  $(u : v : w)$ , then  $\phi$  and  $\varphi$  agree on  $X \setminus \{O\}$ . Since  $\phi$ , and therefore  $\varphi$ , is branched along  $C$  we can recover a model of the branch curve from a Jacobi criterion. That is,

$$C = Z(F) \subseteq \mathbb{P}^2 \quad \text{where } F := \det \begin{bmatrix} u_x & v_x & w_x \\ u_y & v_y & w_y \\ u_z & v_z & w_z \end{bmatrix}.$$

In general we have that  $C$  is a degree 9 plane curve with order 3 singularities at each of the eight base-points of the blow-up (see [Zar08, Section 5]).

**Remark 3.2.3.** Another way to see that the eight base-points of the blow-up correspond to singular points of  $Z(F)$  is as follows. Let  $P_1, \dots, P_8$  be the base-points of the blow-up and let  $E_1, \dots, E_8$  be the corresponding exceptional curves lying over these points. For clarity, we denote by  $C$  the model of the branch curve on  $\mathbb{P}^2$  (i.e.,  $C = Z(F)$ ) and denote by  $C'$  the model of the branch curve on  $X$ . The strict transform of the blow-up of  $C$  at the 8 base-points is  $C'$ . Each exceptional curve  $E_i$  of  $X$  corresponds to a class of  $\text{Pic } X$  that restricts to an odd theta characteristic on  $C'$  (by Proposition 2.8.4). As a divisor,  $E_i$  is effective, so it will restrict to an effective (degree 3) divisor of  $C'$ . However, each  $E_i$  intersects  $C'$  in three points (counting multiplicity) which lie over a single point  $P_i$  of  $C$ . We see that  $C$  has a singularity of order 3 at  $P_i$ .

In other words, once we have computed a model of the branch curve on  $\mathbb{P}^2$  we can immediately identify effective representatives of 8 odd theta characteristics of  $C'$ . Additionally, the anti-canonical divisor of  $X$  provides us with an even theta characteristic of  $C$  by Proposition 2.8.4.

**Example 3.2.4.** Let  $X$  be the del Pezzo surface defined by blowing up  $\mathbb{P}^2$  at the points

$$(0 : -2 : 1), (3 : -9 : 1), (3 : 7 : 1), (8 : 26 : 1), \\ (15 : 63 : 1), (24 : 124 : 1), (48 : 342 : 1), (0 : 0 : 1).$$

We choose  $u, v \in \mathbb{Q}[x, y, z]$  to be two independent cubic forms vanishing at all 8 points. For convenience, we choose  $u$  to be the form  $(x + z)^3 - (y + z)^2z$  and we choose

$$v := 79846x^3 - 41034x^2y - 431517x^2z + 6971xy^2 + 145213xyz \\ + 384942xz^2 - 389y^3 - 12596y^2z - 23636yz^2.$$

We let<sup>1</sup>  $w$  be a sextic form with double roots at each of the points listed above; we further require that  $w$  is not in the span of  $\{u^2, uv, v^2\}$ . Note that  $L(-2\kappa_X)$  is spanned by  $u^2, uv, v^2, w$ . Thus the zero-locus of

$$F := \det \begin{bmatrix} u_x & v_x & w_x \\ u_y & v_y & w_y \\ u_z & v_z & w_z \end{bmatrix}$$

is a (singular) model of the branch curve of  $X$ . With  $\varphi(x, y, z) := (u : v : w)$  as before, we let  $t := u/v$  and  $W := w$ . Using the MAGMA [BCP97] computer algebra package we can compute the image of  $C$  under  $\varphi$  and write the defining equation in terms of  $t, W$  [Kul16]. We have that

$$C: 0 = 23200074887895098984232713028 t^6 - 2457892462046662336694429 t^5 + \\ 1338378986926042827721/16 t^4 - 9000960055643209/8 t^3 + \\ 158059424789/16 t^2 + 11025 t \\ + W (24403582287284966245 t^4 - 13786310912398097/8 t^3 + \\ 234505995159/8 t^2 - 316801/4 t) \\ + W^2(136902207241/16 t^2 - 1208223/4 t) \\ + W^3$$

is an affine model for the branch curve of  $X$ . The morphism induced by the projection  $(t, W) \mapsto t$  is the degree 3 morphism  $f: C \rightarrow \mathbb{P}_k^1$  from Proposition 2.8.4(b). Our choice of  $u$ , via Proposition 3.2.2, ensures that there is a totally ramified fibre at  $t = 0$ . We may view the fibres of  $f$  as effective degree 3 divisors of  $C$ . By the discussion above and Proposition 2.8.4(d), we see that the divisor class of the fibre at  $t = 0$  (and hence any fibre of  $f$ ) is an even theta characteristic. We use the representatives of the theta characteristics to compute data presented in Example 3.3.4.

<sup>1</sup>To compute the explicit model of the branch curve  $C$ , we also make an explicit choice of  $w$  in [Kul16]. However, the expression for  $w$  is too cumbersome to print.

### 3.3 Recovering large class groups from curves with large rational 2-torsion

We fix some notation to be used for the remainder of this section. Using the procedure in the previous section we may choose a trigonal morphism  $f: C \rightarrow \mathbb{P}_{\mathbb{Q}}^1$  with  $C$  a genus 4 curve such that  $\text{rk}_2 J_C[2](\mathbb{Q}) = 8$  and let  $P_0$  be a rational totally ramified point of  $f$ . Denote  $p_0 := f(P_0)$ . Let  $S$  be the places of bad reduction for  $C/\mathbb{Q}$  as well as the archimedean places and places extending  $|\cdot|_2$ .

Conveniently, the Abel-Jacobi map with base-point  $P_0$  provides an embedding of  $C$  into its Jacobian. This map, which we denote by  $j$ , is defined over  $\mathbb{Q}$  and is given by  $j(Q) := [Q - P_0]$ . In particular,  $j(P_0)$  is the identity point of  $J_C$ .

Corollary 2.11 of [GL12], with our explicit choice of  $f: C \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ , gives that for all but  $O(\sqrt{N})$  of the  $t$  in  $\{1, \dots, N\}$  that  $[\mathbb{Q}(P_t) : \mathbb{Q}] = 3$  and

$$\text{rk}_2 \text{Cl}(\mathbb{Q}(P_t)) \geq 8 + \#S - \text{rk } O_{\mathbb{Q}(P_t), S}^*$$

where  $S$  is the set of bad primes for  $C$  together with the archimedean primes and those dividing 2,  $P_t := f^{-1}(t)$ , and  $O_{\mathbb{Q}(P_t), S}^*$  is the group of  $S$ -units in the number field  $\mathbb{Q}(P_t)$ . By applying the ideas of [Mes83] to the curves arising from our construction it is possible to avoid the penalty on the bound introduced by  $S$ -units. The overarching idea of the method we use is to directly exhibit a subfield of the Hilbert class field of  $\mathbb{Q}(P)$ , where  $[\mathbb{Q}(P) : \mathbb{Q}] = 3$  and  $f(P) \in \mathbb{P}^1(\mathbb{Q})$ , for  $P \in C(\mathbb{Q}^{\text{al}})$  which lie in fibres that satisfy a local condition at finitely many places, thereby demonstrating that the class groups of the fields associated to these fibres have large 2-rank. Bilu and Gillibert have provided a generalized description of this framework in [BG18]. Nevertheless, we provide proofs as our computations closely mirror the arguments.

The main idea introduced by [Mes83] is to use the fact that the fibres of the multiplication-by-2 morphism of the Jacobian of a curve  $C$  are precisely described. Specifically:

**Lemma 3.3.1.** *Let  $K$  be a number field, let  $x \in J_C(K)$  be a closed point of degree  $[K : \mathbb{Q}]$  on  $J_C$  (i.e.  $x \cong \text{Spec } K$ ) such that the fibre of  $[2]: J_C \rightarrow J_C$  over  $x$  is irreducible over  $K$ . Let  $L$  be the residue field of  $[2]^{-1}(x)$ . If  $J_C[2](\mathbb{Q}) \cong (\mathbb{Z}/2)^{2g}$ , then  $L/K$  is Galois with Galois group  $(\mathbb{Z}/2)^{2g}$  and there is a fixed finite set of places  $S$  of  $K$ , independent of  $L$ , such that  $L/K$  is unramified outside of  $S$ .*

In fact, we can say even more; the ramification at the bad places is explicitly described by Proposition 2.4.7. (To loosely paraphrase Proposition 2.4.7, that we can give a criteria for the extension  $k([2]^{-1}x)/k$  to be unramified over the places in  $S$  in terms of the values of  $2g$  explicitly computable functions  $h_1, \dots, h_{2g}$  at  $x$ .)

In what follows we devote ourselves to ensuring the conditions of Proposition 2.4.7 are met. We will need to apply Proposition 2.4.7 to points on  $C$  defined over different cubic number fields. As these number fields vary, so too does the set of places  $\tilde{S}$  extending the places of  $\mathbb{Q}$  of bad reduction. We will use the totally ramified point of  $f: C \rightarrow \mathbb{P}^1$  to accommodate for this variation.

Fix a basis  $T_1, \dots, T_8$  for  $J_C[2]$  and rational functions  $h_1, \dots, h_8$  corresponding to the modified Kummer pairing – see Section 2.4.1 and Remark 2.4.6. We note that once we find divisors representing  $T_1, \dots, T_8$ , we can write down each  $h_i$  explicitly, and up to changing the divisors representing the  $T_i$  we can assume that each  $h_i$  is regular at  $P_0$ .

At this point it is helpful to let  $t \in k(C)$  be the function field element corresponding to  $f$ . Note that if  $C$  is the curve from Example 3.2.4 then this assignment agrees with the assignment of  $t$  from that example. Let  $\alpha$  be a uniformizing element for  $\mathcal{O}_{C, P_0}$ . Then the image of  $P \mapsto (t(P), \alpha(P))$  is an affine plane model of  $C$  which is non-singular at  $P_0$ . In other words:

**Lemma 3.3.2.** *We may compute an affine plane model  $C_{\text{aff}}$  of  $C$  such that:*

(A) *the morphism*

$$\begin{aligned} f: C_{\text{aff}} &\rightarrow \mathbb{P}_{\mathbb{Q}}^1 \\ (t, W) &\mapsto (t : 1) \end{aligned}$$

*extends to the trigonal morphism  $f: C \rightarrow \mathbb{P}_{\mathbb{Q}}^1$ , and*

(B) *there is a regular point  $(0, 0) \in C_{\text{aff}}(\mathbb{Q})$  which is identified with  $P_0$ .*

For convenience we will denote

$$\|(x_1, y_1) - (x_2, y_2)\|_w := \max\{|x_1 - x_2|_w, |y_1 - y_2|_w\}$$

for a place  $w$  of a number field  $K$  and points  $(x_1, y_1), (x_2, y_2) \in \mathbb{A}^2(K)$ . Similarly, for  $p_0 = (0 : 1) \in \mathbb{P}^1(K)$  and  $q = (a : b) \in \mathbb{P}^1(K)$ , we denote

$$|q - p_0|_w := \begin{cases} \left| \frac{a}{b} \right|_w & \text{if } q \neq (1, 0) \\ \infty & \text{otherwise} \end{cases}.$$

**Lemma 3.3.3.** *Fix an affine plane model  $C_{\text{aff}} \subseteq \mathbb{A}_{\mathbb{Q}}^2$  of  $C$  with properties (A) and (B) from Lemma 3.3.2. Let  $\nu \in S$  be a finite place. Then there is a constant  $\ell_\nu$  (dependent on  $C_{\text{aff}}$ ) such that the following statement holds:*

*If  $q \in \mathbb{P}^1(\mathbb{Q})$  satisfies  $|q - p_0|_\nu < \ell_\nu$ , then  $\left| \frac{h_i(Q)}{h_i(P_0)} - 1 \right|_w < 1$  for every  $Q \in f^{-1}(q)(\mathbb{Q}^{\text{al}})$ , for every  $i \in \{1, \dots, 8\}$ , and for each  $w$  a place of  $\mathbb{Q}(Q)$  extending  $\nu$ .*

*Proof.* As each  $h_i$  is a rational function on  $C$  with coefficients in  $\mathbb{Q}$  and regular at  $P_0$ , we see that there is a constant  $\lambda$  depending only on the affine plane model of  $C$  such that for any place  $w$  of a number field  $K/\mathbb{Q}$  we have that

$$Q \in C(K) \cap \mathbb{A}^2(K) \text{ and } \|Q - P_0\|_w < \lambda \implies \left| \frac{h_i(Q)}{h_i(P_0)} - 1 \right|_w < 1$$

for each  $1 \leq i \leq 8$ . One way to see this is to write  $h_i \in \mathcal{O}_{C, P_0}$  as a power series in the uniformizer  $\alpha$ .

Let  $\nu \in S$  and let

$$C_{\text{aff}}: 0 = W^3 + a(t)W^2 + b(t)W + c(t)$$

be the affine plane model which is the image of  $P \mapsto (t(P), \alpha(P))$ , where we may assume that  $P_0$  maps to the origin and  $t(P_0) = 0$ . Since the fibre over  $t(P_0)$  contains a unique point and  $P_0$  is a non-singular point of the model, we may rewrite our model as

$$C_{\text{aff}}: 0 = W^3 + ta(t)W^2 + tb(t)W + tc(t)$$

with  $a(t), b(t), c(t)$  regular at  $P_0$ . By taking  $|t_1|_\nu$  less than  $\lambda$  and sufficiently small in terms of the coefficients of  $a(t), b(t), c(t)$  we see that the slopes of the Newton polygon of

$$0 = W^3 + t_1a(t_1)W^2 + t_1b(t_1)W + t_1c(t_1)$$

will all be at least  $-\frac{1}{3} \log_p \lambda$ . In particular, all of the roots have  $\|\beta_i\|_w < \lambda$  for every place  $w$  of  $\mathbb{Q}(Q)$  extending  $\nu$ . So each  $\|(t_1, \beta_i) - (0, 0)\|_w < \lambda$  and we are done.  $\square$

**Example 3.3.4.** We provide a MAGMA script, available at [Kul16], which shows how to explicitly compute an appropriate  $\ell_\nu$  to apply Lemma 3.3.3 to Example 3.2.4. Note that the defining equation for  $C_{\text{aff}}$  has integral coefficients up to powers of 2.

In characteristic greater than 5, the branch curve of any degree 1 del Pezzo surface is smooth (cf. the proof of [Vak01, Proposition 3.2]). Thus, any prime  $p$  for which the reductions of the 8 base points (considered as points of  $\mathbb{P}_{\mathbb{F}_p}^2$ ) remain in general position is a prime of good reduction for  $C$ . Using MAGMA we can compute that the primes of bad reduction for  $C$  are contained in

$$S' := \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 59, 61, 71, \\ 83, 103, 107, 179, 223, 241, 389, 449, 599, 809, 1019\}.$$

Recall from Example 3.2.4 that the effective degree 3 divisor of  $C_{\text{aff}}$  given by the places of  $k(C_{\text{aff}})$  over  $t = \infty$  is a representative of an even theta characteristic of  $C$ ; we call this divisor  $O_E$ . The function associated to the divisor  $[\Theta_1 - O_E]$ , with  $\Theta_1$  the divisor corresponding to the places of  $k(C_{\text{aff}})$  over  $(3 : 7 : 1)$ , is given on the affine model (up to a square constant) by

$$h(t, W) := -484335370397555869540982096 t^2 + 21745428828566997697489 t - \\ 184765518741585604 W + 22709411000816400$$

(recall that  $C_{\text{aff}}$  is defined via the blow-up of a singular plane curve). One can apply the explicit method of Lemma 3.3.3 to find the required sufficiently small constants. These are listed below.

Place	$-\log_p \ell_p$	Place	$-\log_p \ell_p$
2	33	59	1
3	21	61	1
5	21	71	1
7	21	83	1
11	5	103	1
13	5	107	1
17	1	179	5
19	5	223	1
23	9	241	1
29	1	389	1
31	5	449	5
37	1	599	5
41	1	809	5
43	5	1019	1
47	1		

**Lemma 3.3.5.** Fix an affine plane model  $C_{\text{aff}} \subseteq \mathbb{A}_{\mathbb{Q}}^2$  of  $C$  with properties (A) and (B) from Lemma 3.3.2. Let  $\nu \in S$  be an archimedean place, let  $q \in \mathbb{P}^1(\mathbb{Q})$ , and let  $Q \in f^{-1}(q)(\mathbb{Q}^{\text{al}})$ . Then there is a constant  $\ell_\nu$  (dependent on  $C_{\text{aff}}$ ) such that

$$|q - p_0|_\nu < \ell_\nu \implies \left| \frac{h_i(Q)}{h_i(P_0)} - 1 \right|_w < 1$$

for each  $w$  a place of  $\mathbb{Q}(Q)$  extending  $\nu$ .

*Proof.* The place  $w$  determines an embedding  $C_{\text{aff}}(\mathbb{Q}(Q)) \hookrightarrow C_{\text{aff}}(\mathbb{C})$ . On the complex points we have that the functions

$$|h_i| : C_{\text{aff}}(\mathbb{C}) \rightarrow \mathbb{R}$$

are continuous and positive in a small neighbourhood  $U$  around  $P_0$ . Since  $P_0$  is a totally ramified point of  $f$  it follows that the pullback of a small interval  $B$  containing  $p$  will be contained in  $U$ . Since the embedding of  $P_0$  into  $C_{\text{aff}}(\mathbb{C})$  does not depend on  $w$  we see that  $U$  and  $B$  are independent of  $w$  as well.  $\square$

We will use the result of Bilu and Gillibert, based on a result of Dvornicich and Zannier [DZ94] and Hilbert's Irreducibility Theorem, to ensure that there are infinitely many non-isomorphic cubic number fields in the family we have constructed. Here, we have specialized the statement of [BG18, Theorem 3.1] to the particular case where the number field in question is  $\mathbb{Q}$ . We follow the terminology of [BG18].

**Definition 3.3.6.** We call  $\mathcal{U} \subseteq \mathbb{Q}$  a basic thin subset of  $\mathbb{Q}$  if there exists a smooth geometrically irreducible curve  $C$  defined over  $\mathbb{Q}$  and a non-constant rational function  $u \in K(C)$  of degree at least 2 such that  $\mathcal{U} \subseteq u(C(\mathbb{Q}))$ . A thin subset of  $\mathbb{Q}$  is a union of finitely many basic thin subsets.

**Remark 3.3.7.** Let  $f: C \rightarrow \mathbb{P}_{\mathbb{Q}}^1$  be a morphism of degree  $d$  greater than 1. The set of  $\alpha \in \mathbb{Q}$  such that  $\mathbb{Q}(P_t)$  is not a number field of degree  $d$  over  $\mathbb{Q}$ , where  $P_t = f^{-1}(\alpha : 1)$ , is a thin subset of  $\mathbb{Q}$  [BG18, Proposition 3.5].

**Theorem 3.3.8** ([BG18, Theorem 3.1]). *Let  $C$  be a curve over  $\mathbb{Q}$  and let  $t: C \rightarrow \mathbb{P}^1$  be a non-constant morphism with  $\deg t > 1$ . Let  $S$  be a finite set of places of  $\mathbb{Q}$  possibly containing the archimedean place. Further, let  $0 < \epsilon \leq 1/2$  and let  $\mathcal{U}$  be a thin subset of  $\mathbb{Q}$ . Then there exist positive numbers  $c = c(\mathbb{Q}, C, t, S, \epsilon)$  and  $B_0 = B_0(\mathbb{Q}, C, t, S, \epsilon, \mathcal{U})$  such that for every  $B \geq B_0$  the following holds. Consider the points  $P \in C(\mathbb{Q}^{\text{al}})$  satisfying*

$$\begin{aligned} t(P) &\in \mathbb{Q} \setminus \mathcal{U}, \\ |t(P)|_{\nu} &< \epsilon \quad (\nu \in S), \\ H(t(P)) &\leq B. \end{aligned}$$

*Then among the number fields  $\mathbb{Q}(P)$ , where  $P$  satisfies the conditions above, there are at least  $cB / \log B$  distinct fields of degree  $d$  over  $\mathbb{Q}$ .*

**Theorem 3.3.9.** *Let  $C$  be the curve from Example 3.3.4, let  $f: C \rightarrow \mathbb{P}_k^1$  be the trigonal morphism from Example 3.2.4, and  $S'$  the finite set of places from Example 3.3.4 together with the archimedean place. By Lemma 3.3.3 and Lemma 3.3.5 choose constants  $\ell_{\nu}$  for each  $\nu \in S'$ . Let  $\epsilon = \min\{\{\ell_{\nu} : \nu \in S'\}, 1/2\}$ .*

*Let  $T := \{t_1, \dots, t_r\}$  enumerate the points of  $\mathbb{A}^1(\mathbb{Q})$  of height less than  $B$  which satisfy  $|t_i|_{\nu} < \epsilon$  for each  $\nu \in S'$ , and let  $P_{t_i} := f^{-1}(t_i)$  be the corresponding fibres. Then aside from a thin set of exceptions, we have that  $\mathbb{Q}(P_{t_i})$  is a cubic extension of  $\mathbb{Q}$  with  $\text{rk}_2 \text{Cl}(\mathbb{Q}(P_{t_i}))[2] \geq 8$ . Moreover, letting  $\eta(B)$  be the number of isomorphism classes of number fields in the set  $\{\mathbb{Q}(P_t) : t \in T\}$ , we have that  $\eta(B) \gg \frac{B}{\log B}$ .*

*Proof.* Let  $X := [2]^{-1}C$  be the (irreducible) unramified degree  $2^8$  cover of  $C$  obtained from pulling back  $C$  along  $[2]$  in  $J_C$ . By applying Remark 3.3.7 to the composition  $g: X \xrightarrow{[2]} C \xrightarrow{f} \mathbb{P}^1$  we see, aside from a thin set of exceptions  $\mathcal{U}$ , that  $\mathbb{Q}(g^{-1}(t))$  is a degree  $2^8 \cdot 3$  extension of  $\mathbb{Q}$ . In particular  $\mathbb{Q}(P_t) := \mathbb{Q}(f^{-1}(t))$  is a cubic extension of  $\mathbb{Q}$  and  $\mathbb{Q}([2]^{-1}(P_t))/\mathbb{Q}(P_t)$  is a degree  $2^8$  field extension. Additionally, the number of isomorphism classes of cubic number fields in  $\{\mathbb{Q}(P_t) : t \in T\}$  is an immediate consequence of Theorem 3.3.8.

For the remainder of the argument fix such a  $t \in T$  and denote  $[2]^{-1}P_t := \text{Spec } K$ . By Proposition 2.4.3 we see that the extension  $K/\mathbb{Q}(P_t)$  is unramified outside of places extending those in  $S'$ . Moreover,  $K/\mathbb{Q}(P_t)$  is Galois with Galois group  $(\mathbb{Z}/2)^8$  by Lemma 3.3.1.

By Lemma 3.3.3 we have chosen  $\ell_\nu$  for each finite  $\nu \in S'$  such that whenever  $|t - p_0|_\nu < \ell_\nu$  we have

$$|h_i([P_t - P_0]) - 1|_w < 1$$

for every place of  $\mathbb{Q}(P_t)$  extending  $\nu$ . But  $\text{ord}_w h_i([P_t - P_0]) = 0$ , so by Proposition 2.4.7 we conclude that  $K/\mathbb{Q}(P_t)$  is unramified at every finite place of  $\mathbb{Q}(P_t)$ . To ensure that these extensions are unramified at the archimedean places we apply Lemma 3.3.5. By Theorem 2.3.16 we conclude that  $\text{rk}_2 \text{Cl}(\mathbb{Q}(P_t))[2] \geq 8$ .  $\square$

**Remark 3.3.10.** We see that we obtain an improvement of the bound presented in [GL12]. The quantity  $\text{rk } O_{\mathbb{Q}(P), S'}^* - \#S'$  which occurs in their estimate is minimized at  $\left\lfloor \frac{\deg f - 1}{2} \right\rfloor = 1$ , giving a lower bound of 7 for the 2-rank of the class groups in a family.

### 3.4 Families of Galois cubic fields from genus 4 curves

In Section 3.3 we obtained families of cubic number fields whose class groups have high 2-rank from genus 4 curves. It is natural to ask if we can modify our construction to create families of cubic number fields that have class groups with large 2-rank with additional structural properties. For instance, we could attempt to construct an infinite family of cubic number fields  $\{K_j : j \in \mathbb{N}\}$  such that  $\text{rk}_2 \text{Cl}(K_j)[2] \geq r$  and such that  $K_j(\zeta_3)/\mathbb{Q}(\zeta_3)$  is a Galois extension.

In comparison with Section 3.3, a natural strategy would be to attempt to construct a curve with an affine plane model of the form  $w^3 = f(t)$  whose Jacobian variety has  $r$  rational 2-torsion points, thereby giving rise to a family of cubic number fields that become Galois after adjoining a primitive third root of unity and have a class group with 2-rank at least  $r$ . However, the condition that the curve  $C$  of genus 4 admits a  $\mu_3$ -automorphism imposes a non-trivial upper bound on  $r = \text{rk}_2 J_C[2](\mathbb{Q})$ . More precisely, we prove Proposition 3.4.2, which shows that it is impossible to find genus 4 curves which are a  $\mu_3$ -cover of  $\mathbb{P}_{\mathbb{Q}}^1$  with fully rational 2-torsion.

**Definition 3.4.1.** We say that a curve  $C$  is a  $\mu_3$ -cover of  $\mathbb{P}_{\mathbb{Q}}^1$  if there exists a (possibly singular) affine plane model for  $C$  of the form  $w^3 = f(t)$  with  $f(t) \in \mathbb{Q}(t)$  non-constant. In general, we say that a morphism of curves  $\pi: C \rightarrow B$  defined over  $\mathbb{Q}$  is a  $\mu_3$ -cover if there is a non-constant  $f(t) \in \mathbb{Q}(B)$  such that  $\mathbb{Q}(C) = (\pi^*\mathbb{Q}(B))(\sqrt[3]{f})$ .

To clarify Definition 3.4.1, we use the term cover to refer to branched coverings as well.

**Proposition 3.4.2.** *Let  $C/\mathbb{Q}$  be a  $\mu_3$ -cover of  $\mathbb{P}_{\mathbb{Q}}^1$  of genus 4. Then  $\text{rk}_2 J_C[2](\mathbb{Q}) \leq 6$ .*

Notice that for curves satisfying the hypotheses of Proposition 3.4.2 that Galois acts both on the  $[2]$ -torsion of  $C$  and on  $\text{Aut}(C/\mathbb{P}_{\mathbb{Q}}^1) \cong \mu_3$ . In order to prove the proposition we need to assemble all of these group actions together in a nice way.

**Lemma 3.4.3.** *Let  $\pi: C \rightarrow B$  be a  $\mu_3$ -covering of curves defined over  $\mathbb{Q}$  and let  $g(C)$  be the genus of  $C$ . Let  $\rho: \text{Gal}(\mathbb{Q}^{\text{al}}/\mathbb{Q}) \rightarrow \text{Sp}(2g(C), \mathbb{F}_2)$  be the representation of Galois arising from the action of  $\text{Gal}(\mathbb{Q}^{\text{al}}/\mathbb{Q})$  on  $J_C[2]$  and define the action of  $\tau \in \text{Gal}(\mathbb{Q}^{\text{al}}/\mathbb{Q})$  on  $g \in \text{Sp}(2g(C), \mathbb{F}_2)$  by*

$$\tau g := \rho(\tau)g\rho(\tau)^{-1}.$$

*Then the representation  $\psi: \text{Aut}(C/B) \rightarrow \text{Sp}(2g(C), \mathbb{F}_2)$  corresponding to the action of  $\text{Aut}(C/B)$  on divisor classes commutes with the action by Galois, meaning that*

$$\psi(\tau\sigma) = \rho(\tau)\psi(\sigma)\rho(\tau)^{-1}$$

*for all  $\tau \in \text{Gal}(\mathbb{Q}^{\text{al}}/\mathbb{Q})$  and  $\sigma \in \text{Aut}(C/B)$ .*

*Proof.* Since  $\pi$  is a  $\mu_3$ -cover defined over  $\mathbb{Q}$ , there is an  $f \in \mathbb{Q}(B)$  such that  $\mathbb{Q}(C) = \mathbb{Q}(B)(\sqrt[3]{f})$  and such that for some  $\sigma$  generating  $\text{Aut}(C/B)$  we have that  $\sigma^*$  acts on  $\sqrt[3]{f}$  by multiplication by  $\zeta_3$ . Let  $\Gamma \subseteq \mathbb{P}^1 \times B$  be the possibly singular model of  $C$  given by the image of

$$\phi: P \mapsto (\sqrt[3]{f}(P), \pi(P)).$$

Conveniently,  $\sigma$  is explicitly described on points of  $\Gamma$  as  $\sigma: (w, t) \mapsto (\zeta_3 w, t)$ . We see that  $(\tau\sigma)P = (\tau\sigma\tau^{-1})P$  for every  $\mathbb{Q}^{\text{al}}$ -point  $P$  of  $\Gamma$ , so  $\tau\sigma$  and  $\tau\sigma\tau^{-1}$  have the same action on the divisors of  $\Gamma$ . Let  $\Delta$  be the singular locus of  $\Gamma$ . By [HS00, Lemma A.2.3.1] every divisor on  $C$  is linearly equivalent to a divisor  $D' = \sum_{P \in C(\mathbb{Q}^{\text{al}})} n_P P$  such that  $n_P = 0$  for each  $P \in \phi^{-1}(\Delta)(\mathbb{Q}^{\text{al}})$ . It follows that the actions of  $\tau\sigma$  and  $\tau\sigma\tau^{-1}$  on  $\text{Pic}(C)(\mathbb{Q}^{\text{al}})$ , and in particular on  $\text{Pic}(C)(\mathbb{Q}^{\text{al}})[2]$  are equal.  $\square$

**Lemma 3.4.4.** *Let  $\pi: C \rightarrow B$  be a  $\mu_3$ -branched cover of curves defined over  $\mathbb{Q}$  with  $g(C) > 1$ . Then*

$$(i) \text{rk}_2 J_C[2](\mathbb{Q}) < 2g(C).$$

$$(ii) \text{ If in addition } B \text{ has genus } 0, \text{ then } \text{rk}_2 J_C[2](\mathbb{Q}) \leq \log_2 \frac{2^{2g(C)+2}}{3}.$$

*Proof.* (i) Let  $\sigma$  be a non-trivial element of  $\text{Aut}(C/B)$  and let  $D \in J_C[2](\mathbb{Q})$ . Note that the image of  $\pi^*: J_B[2] \rightarrow J_C[2]$  consists of exactly the 2-torsion classes fixed by  $\sigma$ . Indeed if  $D$  is  $\sigma$ -stable then

$$D = [3]D = D + \sigma D + \sigma^2 D \in \pi^*(J_B).$$

Since the genus of  $C$  is greater than 1, we have that  $g(B) < g(C)$  and hence that  $\pi^*$  is not surjective. Thus we either have  $\text{rk}_2 J_C[2](\mathbb{Q}) < 2g(C)$  or we can find a  $D \in J_C[2](\mathbb{Q})$  which is not  $\sigma$ -invariant. But now, if  $\tau$  is complex conjugation and  $\rho: \text{Gal}(\mathbb{Q}^{\text{al}}/\mathbb{Q}) \rightarrow \text{Sp}(8, \mathbb{F}_2)$  is the representation of Galois acting on  $J_C[2]$ , we have

$$\rho(\tau)\sigma(D) = \rho(\tau)\sigma\rho(\tau)^{-1}(D) = \tau\sigma(D) = \sigma^{-1}(D) \neq \sigma(D)$$

so  $J_C[2]$  is not fully rational.

- (ii) Let  $D$  be a non-trivial 2-torsion class of  $J_C[2]$ . We see from the calculation in part (i) that if  $B = \mathbb{P}_{\mathbb{Q}}^1$  then  $D$  cannot be fixed by  $\sigma$ . Since  $D$  is not  $\sigma$ -stable it follows by the argument in part (i) that at most one of  $D, \sigma D, \sigma^2 D$  is rational. The quantity  $\frac{2^{2g(C)+2}}{3}$  is the number of  $\langle \sigma \rangle$ -orbits in  $J_C[2]$ .

□

Proposition 3.4.2 follows immediately from Lemma 3.4.4. We note that it is possible to construct a genus 4 curve  $C/\mathbb{Q}$  which is a  $\mu_3$ -branched cover of another curve  $B$  and has  $\text{rk}_2 J_C[2](\mathbb{Q}) = 6$  using del Pezzo surfaces. The eight points

$$(0 : 1 : 0), (0 : 0 : 1), (1 : 1 : 1), (1 : \zeta_3 : \zeta_3^2), \\ (1 : \zeta_3^2 : \zeta_3), (3 : 4 : 5), (3 : 4\zeta_3 : 5\zeta_3^2), (3 : 4\zeta_3^2 : 5\zeta_3)$$

are in general position, invariant under a linear  $\mu_3$  automorphism of  $\mathbb{P}^2$ , and have six distinct Galois orbits. Consequently, the associated genus 4 curve  $C$  is defined over  $\mathbb{Q}$  and has  $\mu_3 \subseteq \text{Aut}(C)$  and  $\text{rk}_2 J_C[2](\mathbb{Q}) = 6$ . However,  $C/\mu_3$  is not isomorphic to  $\mathbb{P}^1$ .

In [Kul18a] the question of whether there exists a curve  $C/\mathbb{Q}$  that is  $\mu_3$ -cover of  $\mathbb{P}_{\mathbb{Q}}^1$  of genus 4 with  $\text{rk}_2 J_C[2](\mathbb{Q}) = 6$  was left open. It turns out that such a curve does not exist.

**Proposition 3.4.5.** *If  $C$  is a  $\mu_3$ -cover of  $\mathbb{P}_{\mathbb{Q}}^1$  of genus 4 then  $\text{rk}_2 J_C[2](\mathbb{R}) \leq 4$ . Moreover, the curve*

$$C': X^3 - t^6 + \frac{165}{2^3}t^5 - \frac{14883}{2^6}t^4 + \frac{805255}{2^9}t^3 - \frac{43923}{2^9}t^2 - \frac{118372485}{2^{12}}t + \frac{7134076147}{2^{17}}$$

is a  $\mu_3$ -cover of  $\mathbb{P}_{\mathbb{Q}}^1$  of genus 4 with  $\text{rk}_2 J_{C'}[2](\mathbb{Q}) = 4$ .

*Proof.* Let  $C$  be a  $\mu_3$ -cover of  $\mathbb{P}_{\mathbb{Q}}^1$ , let  $\sigma: C \rightarrow C$  be a non-trivial element of  $\text{Aut}(C/\mathbb{P}_{\mathbb{Q}}^1)$ , let  $H \subseteq \text{Sp}(8, \mathbb{F}_2)$  be the subgroup generated by the action of  $\sigma$  on  $J_C[2]$ , and let  $\tau \in \text{Sp}(8, \mathbb{F}_2)$  be the element determined by the action of complex conjugation on  $J_C[2]$ . By the proof of Lemma 3.4.4, we have that  $J_C[2](\mathbb{Q}^{\text{al}})^H$  is trivial. By Lemma 3.4.3, we have that  $\tau\sigma\tau^{-1} = \sigma^{-1}$ .

By our computations in the MAGMA script [Kul18b], there is exactly one subgroup  $H \subseteq \text{Sp}(8, \mathbb{F}_2)$  up to conjugation such that  $\#H = 3$  and such that  $J_C[2](\mathbb{Q}^{\text{al}})^H$  is trivial. Thus, we may assume that  $H$  is some explicit representative of this conjugacy class. By further computations in [Kul18b], if  $\tau \in \text{Sp}(8, \mathbb{F}_2)$  is an element of order 2 such that  $\tau\sigma\tau^{-1} = \sigma^{-1}$ , then  $\text{rk}_2 J_C(\mathbb{Q}^{\text{al}})^{\langle \tau \rangle} \leq 4$ . This completes the first part of the claim.

Consider the del Pezzo surface of degree 1 defined by the zero locus of the weighted sextic

$$S: Z^2 = X^3 - t^6 + \frac{165}{2^3}t^5s - \frac{14883}{2^6}t^4s^2 + \frac{805255}{2^9}t^3s^3 - \frac{43923}{2^9}t^2s^4 - \frac{118372485}{2^{12}}ts^5 + \frac{7134076147}{2^{17}}s^6$$

in  $\mathbb{P}(1 : 1 : 2 : 3)$ . Let  $s_i: \mathbb{P}^1 \rightarrow X$ , where

$$\begin{aligned} s_1: (s : t) &\mapsto \left( s : t : \frac{32}{1323}t^2 - \frac{220}{1323}ts + \frac{5324}{1323}s^2 : \frac{704}{9261}t^2s - \frac{4840}{9261}ts^2 + \frac{150403}{18522}s^3 \right), \\ s_2: (s : t) &\mapsto \left( s : t : \frac{176}{1323}t^2 + \frac{176}{1323}ts - \frac{1210}{1323}s^2 : \frac{64}{1323}t^3 + \frac{704}{9261}t^2s - \frac{4840}{9261}ts^2 + \frac{1331}{18522}s^3 \right), \\ s_3: (s : t) &\mapsto \left( s : t : \frac{176}{1323}t^2 - \frac{2596}{1323}ts + \frac{33275}{5292}s^2 : \frac{64}{1323}t^3 - \frac{9944}{9261}t^2s + \frac{68365}{9261}ts^2 - \frac{389983}{24696}s^3 \right), \\ s_4: (s : t) &\mapsto \left( s : t : \frac{32}{1323}t^2 - \frac{220}{1323}ts + \frac{968}{1323}s^2 : -\frac{968}{3087}ts^2 + \frac{6655}{6174}s^3 \right), \end{aligned}$$

and let  $D_i := \overline{\text{Im}(s_i)}$  be an effective divisor on  $S$ . Our computations in [Kul18b] verify that each  $s_i$  is a well-defined morphism and that

$$\text{rank} \begin{bmatrix} \langle D_1, D_1 \rangle & \dots & \langle D_1, D_4 \rangle & \langle D_1, \kappa_S \rangle \\ \vdots & \ddots & \vdots & \dots \\ \langle D_4, D_1 \rangle & \dots & \langle D_4, D_4 \rangle & \langle D_4, \kappa_S \rangle \\ \langle \kappa_S, D_1 \rangle & \dots & \langle \kappa_S, D_4 \rangle & \langle \kappa_S, \kappa_S \rangle \end{bmatrix} = 5,$$

where  $\langle \cdot, \cdot \rangle$  denotes the intersection pairing on  $S$ . We have that  $C'$  is the branch curve of the Bertini involution of  $S$ , so by Proposition 2.8.4 we have that  $\text{rk}_2 J_{C'}[2](\mathbb{Q}) \geq 4$ .  $\square$

**Remark 3.4.6.** To construct the curve  $C'$  and the maps  $s_i$  appearing in the proof of Proposition 3.4.5, we adapted the script <http://www.cecm.sfu.ca/~nbruin/c3xc3/equations.m> accompanying [BFT14]. Since only the explicit equations for  $C'$  and  $s_1, \dots, s_4$  are important for the proof of Proposition 3.4.5, we will not elaborate on these details.

## Chapter 4

# On the arithmetic of uniquely trigonal genus 4 curves and stable involutions of $E_8$

### 4.1 Introduction

In this chapter, we construct an assignment of the elements of  $J_C(k)/2J_C(k)$  to the orbits of an algebraic group when  $C/k$  is a uniquely trigonal genus 4 curve with some additional data using techniques from Vinberg theory. The technical statements of our results appear in Section 4.1.2. Unlike [Tho16], our results Theorem 4.1.2- $\epsilon_8$ , Theorem 4.1.3- $\epsilon_8$ , Theorem 4.1.4- $\epsilon_8$  are expressed purely in terms of the pointed genus 4 curve in the hypotheses, and we do not require the extra data of a tangent vector at the marked point. This is due to the slight modification of [Tho16, Theorem 1.10] given in Section 2.6.8. Having established the results of Section 2.8, we obtain our results by following the method of [Tho16]. We also reorganize the argument in [Tho16] to emphasize the generality of the method. Our eventual goal is to obtain a result in the style of [BG13] and [RT17]; namely, to calculate an upper bound for the average<sup>1</sup> rank of  $J_C(k)$  as  $C$  varies over the uniquely trigonal genus 4 curves. We hope that this will be a topic of future study.

**Remark 4.1.1.** The family of affine plane curves in [RT17, Tho13] given by

$$y^3 = x^5 + y(c_2x^3 + c_8x^2 + c_{14}x + c_{20}) + c_{12}x^3 + c_{18}x^2 + c_{24}x + c_{30} \quad (\star)$$

is in fact a family of uniquely trigonal genus 4 curves. We point out that our construction treats a more general curve as the trigonal morphism  $\pi : (y, x) \rightarrow (x : 1)$  will always have a totally ramified fibre over the point at infinity for any curve of the form  $(\star)$ . Our procedure identifies how the family considered in [RT17, Tho13] connects to the general case. Specifically, the family of pairs  $(C, P)$  with  $C$  a curve in  $(\star)$  and  $P$  the totally ramified point on  $C$  at infinity is treated in the  $\epsilon_8$  case

<sup>1</sup>In a natural well-defined sense. c.f. [BG13].

of our argument. Moreover, if  $C/k$  is a uniquely trigonal curve of split type of the form  $(\star)$ , our results augment [Tho13, Theorem 4.14]<sup>2</sup> by constructing an orbit for every class in  $J_C(k)/2J_C(k)$ , as opposed to just those classes in the image of the Abel-Jacobi map, i.e, those classes relevant to a two-cover descent.

We now describe the layout of this chapter. We fix some further notation in Subsection 4.1.1 specific to this chapter. Our main results are stated in Subsection 4.1.2. In Section 4.2 we give a brief summary of the techniques introduced in [Tho16]. In Section 4.3 we prove Theorem 4.1.2. Finally, we prove Theorem 4.1.3 and Theorem 4.1.4 in Section 4.4.

### 4.1.1 Notation and conventions

We denote the moduli functor for smooth uniquely trigonal genus 4 curves by  $\mathcal{T}_4$ . We denote the moduli functor for smooth uniquely trigonal genus 4 curves, together with a marked ramification point, simple ramification point, or totally ramified point by  $\mathcal{T}_4^{\text{ram}}$ ,  $\mathcal{T}_4^{\text{s.ram}}$ , or  $\mathcal{T}_4^{\text{t.ram}}$  respectively. We denote the sub-functor for smooth uniquely trigonal genus 4 curves of split type, together with a marked ramification point, simple ramification point, or totally ramified point by  $\mathcal{U}_4^{\text{ram}}$ ,  $\mathcal{U}_4^{\text{s.ram}}$ , or  $\mathcal{U}_4^{\text{t.ram}}$  respectively.

We denote the moduli functor for smooth genus 3 curves by  $\mathcal{M}_3$ , and the moduli functor for pointed smooth genus 3 curves by  $\mathcal{M}_3^1$ . i.e,  $\mathcal{M}_3^1$  is the moduli functor of smooth genus 3 curves together with a marked point. If  $\mathcal{F}$  is one of the aforementioned moduli functors of curves then we denote by  $\mathcal{F}(2)$  the moduli functor of curves parametrized by  $\mathcal{F}$  with marked 2-torsion of their Jacobian variety.

### 4.1.2 Statement of our main results

Let  $C/k$  be a uniquely trigonal genus 4 curve and let  $P \in C(k)$  be a ramification point of the unique (up to  $\text{PGL}_2$ ) morphism  $\pi: C \rightarrow \mathbb{P}^1$  of degree 3. We split our analysis into two cases:

Case  $E_8$ : The ramification index of  $P$  with respect to  $\pi$  is 2 (the generic case, where  $P$  is a simple ramification point).

Case  $\epsilon_8$ : The ramification index of  $P$  with respect to  $\pi$  is 3 ( $P$  is a totally ramified point of  $\pi$ ).

As in [Tho16], the names indicate the affine algebraic group or Lie algebra used to construct the appropriate orbit spaces. We prove the direct analogues of Thorne's results.

<sup>2</sup>A restatement of [Tho13, Theorem 4.14] applied specifically to the family  $(\star)$  appears as [RT17, Theorem 2.10].

**Theorem 4.1.2.**

$E_8$ : If  $k = k^{\text{sep}}$ , then there is a bijection

$$\mathcal{T}_4^{\text{s.ram}}(k) \rightarrow (T^{\text{rss}} // W_T)(k)$$

with  $\Lambda$  the root lattice of type  $E_8$  and  $T = \text{Hom}(\Lambda, \mathbb{G}_m)$  the split torus of rank 8.

$\epsilon_8$ : If  $k = k^{\text{sep}}$ , then there is a bijection

$$\mathcal{T}_4^{\text{t.ram}}(k) \rightarrow (\mathbb{P}\mathfrak{t}^{\text{rss}} // W_T)(k)$$

with  $\mathfrak{t}$  the Lie algebra of the torus  $T$ .

Theorem 4.1.2 was actually known in the theory of surface singularities, and was in fact known to A. Coble (see [DO88, Chapter VII]) and other classical algebraic geometers. We provide a proof of Theorem 4.1.2 since the argument we use is closely related to the assignment we ultimately consider.

**Theorem 4.1.3.**

$E_8$ : Let  $H$  be the split group of type  $E_8$  over  $k$ , let  $\theta$  be an involution of  $H$  satisfying the conditions of Proposition 2.6.56, and let  $X := (H^{\theta(h)=h^{-1}})^\circ$  be the theta inverted subvariety. Let  $G := (H^\theta)^\circ$ . Let  $X^{\text{rss}}$  be the open subset of regular semi-simple elements. Then the assignment  $(C, P) \mapsto \varkappa_C$  of Theorem 4.1.2- $E_8$  determines a map

$$\mathcal{U}_4^{\text{s.ram}}(k) \rightarrow G(k) \backslash X^{\text{rss}}(k).$$

If  $k = k^{\text{sep}}$ , then this map is a bijection.

$\epsilon_8$ : Let  $H$  be as above, let  $X := \mathfrak{h}^{d\theta=-1}$  be the Lie algebra of  $(H^{\theta(h)=h^{-1}})^\circ$ , and let  $X^{\text{rss}}$  be the open subset of regular semi-simple elements. Then the assignment  $(C, P) \mapsto \varkappa_C$  of Theorem 4.1.2- $\epsilon_8$  determines a map

$$\mathcal{U}_4^{\text{t.ram}}(k) \rightarrow G(k) \backslash \mathbb{P}X^{\text{rss}}(k).$$

If  $k = k^{\text{sep}}$ , then this map is a bijection.

**Theorem 4.1.4.**

$E_8$ : Fix an  $x = (C, P) \in \mathcal{U}_4^{\text{s.ram}}(k)$  and by abuse of notation we denote by  $x$  the image of  $(C, P)$  in  $T // W_T$ . Let  $\pi: X \rightarrow X // G$  denote the natural quotient map, where  $X, G$  are as in Theorem 4.1.3- $E_8$ . Note that  $X // G$  is canonically isomorphic to  $T // W_T$ . Let  $X_x$  be the fibre of  $\pi$  over  $x$  and let  $J_x = J_C$ . Then there is a canonical injective map

$$\frac{J_x(k)}{2J_x(k)} \hookrightarrow G(k) \backslash X_x(k).$$

$\epsilon_8$ : Fix an  $x = (C, P) \in \mathcal{U}_4^{\text{t.ram}}(k)$  and by abuse of notation we denote by  $x$  the image of  $(C, P)$  in  $\mathbb{P}^4 // W_T$ . Let  $\pi: \mathbb{P}X \rightarrow \mathbb{P}X // G$  denote the natural quotient map, where  $X, G$  are as in Theorem 4.1.3- $\epsilon_8$ . Let  $\mathbb{P}X_x$  be the fibre of  $\pi$  over  $x$  and let  $J_x = J_C$ . Then there is a canonical injective map

$$\frac{J_x(k)}{2J_x(k)} \hookrightarrow G(k) \backslash \mathbb{P}X_x(k).$$

**Remark 4.1.5.** In [Tho13, Theorem 4.14], Thorne shows that the mapping  $\mathcal{U}_4^{\text{t.ram}}(k) \hookrightarrow G(k) \backslash \mathbb{P}X^{\text{rss}}(k)$  of Theorem 4.1.3- $\epsilon_8$  extends to a map  $\mathcal{T}_4^{\text{t.ram}}(k) \hookrightarrow G(k) \backslash \mathbb{P}X^{\text{rss}}(k)$ . However, this does not allow us to strengthen Theorem 4.1.4- $\epsilon_8$  as our construction of orbits depends on the ‘‘split type’’ condition.

## 4.2 A summary of Thorne’s construction of orbits

In this section, we give a summary of Thorne’s construction of orbits since we will ultimately be following the same overarching strategy. The identification of pointed plane quartic curves  $(C, P)$  to orbits is split into four cases depending on the properties of the tangent line at  $P$  to the curve  $C$ . These are:

Case  $E_7$ : The tangent line to  $P$  meets  $C$  at exactly 3 points (the generic case).

Case  $\epsilon_7$ : The tangent line to  $P$  meets  $C$  at exactly 2 points, with contact order 3 at  $P$  (i.e  $P$  is a flex).

Case  $E_6$ : The tangent line to  $P$  meets  $C$  at exactly 2 points, with contact order 2 at  $P$  (i.e  $P$  lies on a bitangent).

Case  $\epsilon_6$ : The tangent line to  $P$  meets  $C$  at exactly 1 point, with contact order 4 (i.e  $P$  is a hyperflex)

The name of each case refers to the simple affine algebraic group, or simple Lie algebra used to construct the orbit space which parametrizes points of the noted type on plane quartic curves.

For simplicity we describe the argument of [Tho16] for the  $E_7$  case only, but we note that the other cases are treated similarly. The argument is guided along three milestone theorems. We list these as Theorem 4.2.1, Theorem 4.2.2, and Theorem 4.2.3 and outline the arguments used in proving them. Let  $\mathcal{S}$  be the subfunctor of  $\mathcal{M}_3^1$  parameterizing non-hyperelliptic pointed genus 3 curves, whose marked point  $P$  in the canonical model is not a flex and does not lie on a bitangent.

**Theorem 4.2.1** ([Tho16, Theorem 3.4]). *If  $k = k^{\text{sep}}$ , then there is a bijection*

$$\mathcal{S}(k) \rightarrow (T^{\text{rss}} // W_T)(k)$$

with  $\Lambda$  the root lattice of type  $E_7$  and  $T = \text{Hom}(\Lambda, \mathbb{G}_m)$  the split torus of rank 7.

Theorem 4.2.1 is a reformulation of some results of [Loo93]. The result is established by using a connection between non-hyperelliptic genus 4 curves and del Pezzo surfaces of degree 2. Theorem 4.2.1 or [Loo93, Proposition 1.8] shows that  $\mathcal{S}(2)$  is naturally isomorphic to an open subset of a rank 7 ( $= \dim \mathcal{M}_3^1$ ) torus. This isomorphism arises from the relationship between smooth plane quartics and del Pezzo surfaces of degree 2. Namely, every del Pezzo surface of degree 2 is a double cover of  $\mathbb{P}^2$  branched along a smooth plane quartic, and every smooth plane quartic arises in this way. The result in [Loo93, Proposition 1.8] shows that the additional data of an anti-canonical section of a degree 2 del Pezzo surface corresponds (generically) to the data of a point on the associated plane quartic.

Thorne then takes advantage of the fact that del Pezzo surfaces of degree 2 have a strong connection to split adjoint simple groups of type  $E_7$  and uses classical results on affine algebraic groups to strengthen Theorem 4.2.1 to Theorem 4.2.2 below. In particular, [Tho16, Theorem 1.11] gives an isomorphism  $T^{\text{rss}} // W_T \cong X^{\text{rss}} // G$ , and [Tho16, Section 2] provides a construction of the larger algebraic group using a root datum and auxiliary data. The final step of this argument is to show that this extra abstract data is supplied by the choice of plane quartic and point.

**Theorem 4.2.2** ([Tho16, Theorem 3.5]). *Let  $H$  be the split adjoint simple group of type  $E_7$  over  $k$ , let  $\theta$  be an involution of  $H$  satisfying the conditions of Proposition 2.6.56, and let  $X := (H^{\theta(h)=h^{-1}})^\circ$  be the theta inverted subvariety. Let  $G := (H^\theta)^\circ$ . Let  $X^{\text{rss}}$  be the open subset of regular semi-simple elements. Then the assignment  $(C, P) \mapsto \varkappa_C$  of Theorem 4.2.1 determines a map*

$$\mathcal{S}(k) \rightarrow G(k) \backslash X^{\text{rss}}(k).$$

Finally, Theorem 4.2.2 is twisted to become Theorem 4.2.3. The auxiliary data provided by a plane quartic and point  $(C, P)$  in the proof of Theorem 4.2.2 depends on a chosen translate of  $2W_{g-1}$ , where  $W_{g-1}$  is a theta divisor of  $J_C$ . In turn, for a fixed curve  $C$ , the choices of non-equivalent translates of  $2W_{g-1}$  over a field  $k$  are parametrized by the choices of  $[D] \in \frac{J_C(k)}{2J_C(k)}$ . In Theorem 4.2.2 this choice can be made systematically among all pointed plane quartics since  $\frac{J_C(k)}{2J_C(k)}$  always contains the trivial class<sup>3</sup>. However, for a fixed pointed curve  $(C, P)$  there are potentially many choices of a class in  $\frac{J_C(k)}{2J_C(k)}$ , and thus many choices of translates of  $2W_{g-1}$ . The  $G(k^{\text{sep}})$ -orbit assigned to  $(C, P)$  decomposes into several  $G(k)$ -orbits, and there is an assignment of one of these  $G(k)$ -orbits to each choice of translate of  $2W_{g-1}$ . For the technical details one should consult [Tho16, Section 1] and the proof of Theorem 4.2.3.

<sup>3</sup>As one is parameterizing plane quartic curves with a  $k$ -rational point, one could also systematically choose the class  $[4P - \mathcal{K}_C]$  among all pointed curves, where here  $\mathcal{K}_C$  is the canonical class of  $C$ .

$$\begin{array}{ccccc}
(C, P) =: x & \longrightarrow & \mathcal{S}(k) & \hookrightarrow & (T//W_T)(k) \\
& & \downarrow & & \uparrow \wr \\
\frac{J_x(k)}{2J_x(k)} & \hookrightarrow & G(k)\backslash X_x(k) & \hookrightarrow & G(k)\backslash X(k) \xrightarrow{\rho} (X//G)(k) \\
& & & & \uparrow \pi \\
& & & & X
\end{array}$$

Figure 4.1: Diagram of functors.

**Theorem 4.2.3** ([Tho16, Theorem 3.6]). *Fix an  $x = (C, P) \in \mathcal{S}(k)$  and by abuse of notation we denote by  $x$  the image of  $(C, P)$  in  $T//W_T$ . Let  $\pi: X \rightarrow X//G$  denote the natural quotient map. Note that  $X//G$  is canonically isomorphic to  $T//W_T$ . Let  $X_x$  be the fibre of  $\pi$  over  $x$ . Then there is a canonical injection*

$$\frac{J_x(k)}{2J_x(k)} \hookrightarrow G(k)\backslash X_x(k)$$

such that the image of  $x$  in  $G(k)\backslash X(k)$  is the image of  $[0] \in \frac{J_x(k)}{2J_x(k)}$ .

Figure 4.1 is a diagrammatic description of the relations between the functors noted in the three theorems above. Note that in general  $\rho$  is not a bijection, though it is a bijection when  $k$  is separably closed.

### 4.3 Points on maximal tori in $E_8$

Theorem 2.8.8 provides a relationship between the uniquely trigonal genus 4 curves and del Pezzo surfaces of degree 1. Similar to the relationship between plane quartic curves and degree 2 del Pezzo surfaces in [Loo93], we can ask what the datum of an anti-canonical section of a degree 1 del Pezzo surface marks on the associated uniquely trigonal genus 4 curve. Corollary 4.3.3 provides the answer to this question. We will use the presentation of the root lattice  $\Lambda$  of type  $E_8$  from Definition 2.6.43. As in Section 2.8.2, we denote by  $W_+$  the quotient of the Weyl group  $W_{E_8}$  by its central subgroup of order 2.

**Remark 4.3.1.** Let  $\Lambda$  be a root lattice of type  $E_8$  and let  $T = \text{Hom}_k(\Lambda, \mathbb{G}_m)$  be a torus. Then  $\chi \in T^{\text{rss}}$  if and only if  $\chi$  does not lie on a root hyperplane, which is equivalent to  $\chi(\alpha) \neq 1$  for every root  $\alpha$  [Loo93, Section 1].

We prove an analogue of [Loo93, Proposition 1.8] for degree 1 del Pezzo surfaces. We let  $\widetilde{\mathcal{DP}}_1$  denote the moduli space of marked degree 1 del Pezzo surfaces and let  $\widetilde{\mathcal{DP}}_1(\text{node})$  denote the moduli space of marked degree 1 del Pezzo surfaces together with a singular nodal anti-canonical section.

**Proposition 4.3.2.** *If  $k = k^{\text{sep}}$ , then there is a  $W_+$ -equivariant isomorphism*

$$\widetilde{\mathcal{DP}}_1(\text{node}) \cong T^{\text{rss}}/\langle \pm 1 \rangle$$

with  $T := \text{Hom}(\Lambda, \mathbb{G}_m)$  and  $\Lambda$  a split root lattice of type  $E_8$ .

*Proof.* Let  $K$  be an abstract nodal genus 0 curve and let  $K_{\text{reg}}$  be its subscheme of regular points. Then  $\text{Pic}^0(K)$  is isomorphic to  $\mathbb{G}_m$  in a unique way up to inversion. Fix a choice of  $P_1 \in K_{\text{reg}}(k^{\text{sep}})$  and corresponding isomorphism  $\tau_{P_1} : \text{Pic}^0(K) \rightarrow \text{Pic}^1(K) \cong K_{\text{reg}}$  given by translation by  $P_1$ .

Let  $\chi \in T^{\text{rss}}(k^{\text{sep}})$  be a point of the torus  $T = \text{Hom}(\Lambda, \mathbb{G}_m)$ . For each  $i \in \{1, \dots, 7\}$  we define  $P_{i+1}$  to be the unique point of  $K_{\text{reg}}(k^{\text{sep}})$  such that the divisor  $P_{i+1}$  is linearly equivalent to  $P_i + \chi(e_{i+1} - e_i)$ . Notice that for any  $i, j \in \{1, \dots, 8\}$  we have that  $(P_i - P_j) = \chi(e_i - e_j)$ .

The linear system associated to the degree 3 divisor

$$D := \chi(l - e_1 - e_2 - e_3) + P_1 + P_2 + P_3$$

determines an embedding of  $K$  into the projective plane. We claim that under this embedding the points  $P_1, \dots, P_8$  are in general position.

We see that two points coincide if and only if  $\chi(e_i - e_j) = \text{id}$  for some distinct  $i, j$ . We see that  $P_{i_1}, P_{i_2}, P_{i_3}$  lie on a line if and only if we have

$$\begin{aligned} \text{div } h &= D - (P_{i_1} + P_{i_2} + P_{i_3}) \\ &= \chi(l - e_1 - e_2 - e_3) + P_1 - P_{i_1} + P_2 - P_{i_2} + P_3 - P_{i_3} \\ &= \chi(l - e_1 - e_2 - e_3) + \chi(e_{i_1} - e_1) + \chi(e_{i_2} - e_1) + \chi(e_{i_3} - e_1) \\ &= \chi(l - e_{i_1} - e_{i_2} - e_{i_3}) \end{aligned}$$

for some  $h \in k(K)$ . Similar calculations show that six of these points lie on a conic if and only if  $\chi(2l - e_{i_1} - \dots - e_{i_6}) = \text{id}$  for some distinct  $i_j \in \{1, \dots, 8\}$  and there is a cubic passing through all eight of these points with a singularity at one of them if and only if  $\chi(3l - e_{i_1} - \dots - e_{i_7} - 2e_{i_8}) = \text{id}$  for some distinct  $i_j \in \{1, \dots, 8\}$ . To recapitulate, the points  $P_1, \dots, P_8$  lie in general position if and only if  $\chi(\alpha) \neq 1$  for each root  $\alpha$  of  $\Lambda$ .

The blow-up of  $\mathbb{P}^2$  at the eight points  $P_1, \dots, P_8$  is a marked degree 1 del Pezzo surface with a marked nodal anti-canonical curve  $(S, \{e_1, \dots, e_8\}, K')$ , where  $K'$  is the strict transform of  $K$  under the blow-up.

If the construction above sends  $\chi$  to  $(S, \{e_1, \dots, e_8\}, K')$ , then it sends  $-\chi$  to  $(S, \{\iota(e_1), \dots, \iota(e_8)\}, K')$ , where  $\iota$  is the Bertini involution of  $S$ . It is clear that every marked degree 1 del Pezzo surface with a marked nodal section is obtained by this construction in a unique way up to inversion on  $T$ . (In fact, we describe the explicit inverse in Remark 4.3.6.) Additionally, this map is  $W_{E_8}$ -equivariant, so we obtain a  $W_+$ -equivariant map  $T/\langle \pm 1 \rangle \rightarrow \widetilde{\mathcal{DP}}_1(\text{node})$ .  $\square$

**Corollary 4.3.3.** *There is a  $W_+$ -equivariant inclusion  $T^{\text{rss}} \hookrightarrow \mathcal{T}_4^{\text{s.ram}}(2)$ .*

*Proof.* Proposition 4.3.2 supplies a  $W_+$ -equivariant isomorphism  $T^{\text{rss}} \cong \widetilde{\mathcal{DP}}_1(\text{node})$ . There is also a  $W_+$ -equivariant inclusion  $\psi: \widetilde{\mathcal{DP}}_1(\text{node}) \hookrightarrow \mathcal{T}_4^{\text{ram}}(2)$ . Explicitly, if  $(S, B, s)$  is a marked degree 1 del Pezzo surface with a marked nodal section of the anticanonical divisor, we obtain a uniquely trigonal genus 4 curve  $C$  by taking the branch curve of the Bertini involution. By Proposition 3.2.2, the section  $s$  corresponds to a unique ramification point of index 2. Furthermore, Proposition 2.8.10 and Proposition 2.8.11 show that  $B$  determines a marking of the 2-level structure of  $C$ .  $\square$

If  $K$  is an abstract cuspidal genus 0 curve, then we may choose an isomorphism  $\mathbb{G}_a \cong \text{Pic}^0(K)$ . This choice of isomorphism is unique up to  $\text{Aut}(\mathbb{G}_a) = \mathbb{G}_m$ , and the  $-1$  element of  $\mathbb{G}_m$  acts on  $\mathbb{G}_a$  by inversion. Thus, if  $\Lambda$  is the character lattice of a torus  $T$ , then  $\text{Aut}(\mathbb{G}_a)$  acts on  $\mathfrak{t} := \text{Hom}(\Lambda, \mathbb{G}_a)$  and we have  $(\mathfrak{t} \setminus \{0\}) // \text{Aut}(\mathbb{G}_a) = \mathbb{P}\mathfrak{t}$ .

Let  $\widetilde{\mathcal{DP}}_1(\text{cusp})$  denote the moduli space of marked degree 1 del Pezzo surfaces together with a singular cuspidal anti-canonical section. By replacing the singular nodal cubic in the proof of Proposition 4.3.2 with a cuspidal plane cubic we can prove using an identical argument:

**Proposition 4.3.4.** *If  $k = k^{\text{sep}}$ , there is a  $W_+$ -equivariant isomorphism*

$$\widetilde{\mathcal{DP}}_1(\text{cusp}) \cong \mathbb{P}\mathfrak{t}^{\text{rss}}$$

with  $\mathfrak{t} := \text{Hom}(\Lambda, \mathbb{G}_a)$  and  $\Lambda$  a split root lattice of type  $E_8$ .

In the proposition above, one can think of  $\mathfrak{t}$  as the Lie algebra of a maximal subtorus of a split group of type  $E_8$ . As before we also obtain:

**Corollary 4.3.5.** *There is a  $W_+$ -equivariant inclusion  $\mathbb{P}\mathfrak{t}^{\text{rss}} \hookrightarrow \mathcal{T}_4^{\text{t.ram}}(2)$ .*

**Remark 4.3.6.** Let  $\Lambda$  be the simply laced lattice of Dynkin type  $E_8$ . Let  $C/k$  be a uniquely trigonal genus 4 curve, let  $\pi: C \rightarrow \mathbb{P}^1$  be the trigonal morphism (which is unique up to  $\text{PGL}_2$ ), and let  $P$  be a ramified point of  $\pi$ . We give the details of the assignment of  $(C, P) \in \mathcal{T}_4^{\text{s.ram}}(k)$  to a rational point on the torus  $T = \text{Hom}(\Lambda, \mathbb{G}_m)(k)$  which is well-defined up to  $W_{E_8} \cong \text{Aut}(\Lambda)$ .

The canonical model of  $C$  lies on a quadric cone in  $\mathbb{P}^3$ . We may identify the quadric cone with  $\mathbb{P}(1 : 1 : 2)$  and up to automorphisms of  $\mathbb{P}^3$  we see that  $C$  is given by a model of the form

$$C: 0 = f_0 w^3 + f_2(s, t) w^2 + f_4(s, t) w + f_6(s, t).$$

Since  $C$  is not hyperelliptic, we have that  $f_0 \neq 0$ . The uniquely trigonal morphism  $\pi$  is induced by the projection  $\pi: (s, t, w) \mapsto (s, t)$ . We let  $S/k$  be the degree 1 del Pezzo surface defined by the sextic equation in  $\mathbb{P}(1 : 1 : 2 : 3)$

$$S: z^2 = f_0 w^3 + f_2(s, t) w^2 + f_4(s, t) w + f_6(s, t).$$

Using the marked point  $P = (s_0, t_0, w_0)$  on  $C$  we define an anti-canonical section on  $S$ . The map

$$\begin{aligned} \pi: \quad S &\rightarrow \mathbb{P}^1 \\ (s, t, w, z) &\mapsto (s, t) \end{aligned}$$

is a rational map which is regular outside the base-point of  $S$ . The Weil divisor  $D = \overline{\pi^{-1}(s_0, t_0)}$  is an anti-canonical divisor of  $S$ . Moreover, by the assumption that  $P$  is a simply ramified point of  $\pi$ , we see that  $D$  as a scheme is isomorphic to a nodal genus 0 curve. The restriction  $\text{Pic}(S_{k^{\text{sep}}}) \rightarrow \text{Pic}(D)$  induces a homomorphism of Galois modules

$$\text{Pic}(S_{k^{\text{sep}}})^\perp \rightarrow \text{Pic}^0(D).$$

Up to  $\text{Aut}(\Lambda)$  we may choose an identification  $\Lambda \cong \text{Pic}(S_{k^{\text{sep}}})^\perp$ . Such an identification is uniquely determined by a marking of  $S_{k^{\text{sep}}}$ ; if  $\{l, e_1, \dots, e_8\}$  is the standard basis for  $I_{1,8}$  as in Definition 2.6.43 and  $B := \{e'_1, \dots, e'_8\}$  is any marking of  $\text{Pic}(S_{k^{\text{sep}}})$ , there is a class  $l' \in \text{Pic}(S_{k^{\text{sep}}})$  such that  $3l' = e'_1 + \dots + e'_8 - \kappa_S$ . Since  $\text{Pic} S_{k^{\text{sep}}} \cong \mathbb{Z}^9$  is torsion-free, the class  $l'$  is the unique class satisfying  $3l' = e'_1 + \dots + e'_8 - \kappa_S$ . An isomorphism is given by restricting  $c_0l + c_1e_1 + \dots + c_8e_8 \mapsto c_0l' + c_1e'_1 + \dots + c_8e'_8$  to  $\Lambda$ .

We may also choose an identification  $\text{Pic}^0(D) \cong \mathbb{G}_m$ , and the choice of this identification is unique up to inversion. We obtain a Galois action on  $\Lambda$  by inheriting the Galois action on  $\text{Pic}(S_{k^{\text{sep}}})^\perp$ . Thus, we obtain a point  $\varkappa_C \in \text{Hom}(\Lambda, \mathbb{G}_m)(k)$  and this point is unambiguously defined up to  $\text{Aut}(\Lambda)$ . We produce a similar assignment  $\mathcal{T}_4^{\text{t.ram}}(k) \dashrightarrow \mathbb{P}\text{Hom}(\Lambda, \mathbb{G}_a)(k)$  in an analogous fashion. In the case where  $C$  is of split type, we may choose  $S$  to have a Galois invariant marking.

Via Corollary 4.3.3, Corollary 4.3.5, and Remark 4.3.6 we obtain:

**Theorem 4.1.2.**

$E_8$ : If  $k = k^{\text{sep}}$ , then the assignment of Remark 4.3.6 induces a bijection

$$\mathcal{T}_4^{\text{s.ram}}(k) \rightarrow (T^{\text{rss}} // W_T)(k)$$

with  $\Lambda$  the root lattice of type  $E_8$  and  $T = \text{Hom}(\Lambda, \mathbb{G}_m)$  the split torus of rank 8.

$\mathfrak{e}_8$ : If  $k = k^{\text{sep}}$ , then the assignment of Remark 4.3.6 induces a bijection

$$\mathcal{T}_4^{\text{t.ram}}(k) \rightarrow (\mathbb{P}\mathfrak{t}^{\text{rss}} // W_T)(k)$$

with  $\mathfrak{t}$  the Lie algebra of the torus  $T$ .

**Remark 4.3.7.** An additional advantage of using the space  $\mathbb{P}\mathfrak{t}$  instead of  $\mathfrak{t}$  is pointed out in [Loo93, Section 1.16]. Namely, that there is a natural way to fit together the isomorphisms from Proposition 4.3.2 and Proposition 4.3.4.

## 4.4 Construction of orbits for the $E_8$ case

In this section we prove the main results stated in Section 4.1.2.

### 4.4.1 Proof of Theorem 4.1.3

#### Theorem 4.1.3.

$E_8$ : Let  $H$  be the split group of type  $E_8$  over  $k$ , let  $\theta$  be a split stable involution of  $H$ , and let  $X := (H^{\theta(h)=h^{-1}})^\circ$  be the theta inverted subvariety. Let  $G := (H^\theta)^\circ$ . Let  $X^{\text{rss}}$  be the open subset of regular semi-simple elements. Then the assignment  $(C, P) \mapsto \varkappa_C$  of Theorem 4.1.2- $E_8$  determines a map

$$\mathcal{U}_4^{\text{s.ram}}(k) \rightarrow G(k) \backslash X^{\text{rss}}(k).$$

If  $k = k^{\text{sep}}$ , then this map is a bijection.

$\varepsilon_8$ : Let  $H$  be as above, let  $X := \mathfrak{h}^{d\theta=-1}$  be the Lie algebra of  $(H^{\theta(h)=h^{-1}})^\circ$ , and let  $X^{\text{rss}}$  be the open subset of regular semi-simple elements. Then the assignment  $(C, P) \mapsto \varkappa_C$  of Theorem 4.1.2- $\varepsilon_8$  determines a map

$$\mathcal{U}_4^{\text{t.ram}}(k) \rightarrow G(k) \backslash \mathbb{P}X^{\text{rss}}(k).$$

If  $k = k^{\text{sep}}$ , then this map is a bijection.

**Remark 4.4.1.** We often make use of an assignment  $(C, P) \dashrightarrow \text{Hom}(\Lambda, \mathbb{G}_m)(k)$  which is only well-defined up to  $W_{E_8}$ . However, we are only interested in this assignment insofar as to construct a  $G(k)$ -orbit. Via the isomorphisms of Theorem 2.6.55 and Theorem 2.6.54 we resolve the ambiguity introduced by  $W_{E_8}$  when assigning  $(C, P)$  to a point  $\varkappa_C \in \text{Hom}(\Lambda, \mathbb{G}_m)(k)$  (resp.  $\mathbb{P}\text{Hom}(\Lambda, \mathbb{G}_a)(k)$ ).

We prove this theorem by closely following the proof of [Tho16, Theorem 3.5].

*Proof.* Let  $(C, P) \in \mathcal{U}_4^{\text{s.ram}}(k)$  and let  $V = \Lambda/2\Lambda$ . Let  $\langle \cdot, \cdot \rangle$  be the pairing defined on  $\Lambda$  and let  $\langle \cdot, \cdot \rangle_2: V \rightarrow \mathbb{F}_2$  denote the reduction of  $\langle \cdot, \cdot \rangle$  modulo 2. Let  $q: V \rightarrow \mathbb{F}_2$  be the quadratic form defined by  $q(v) := \frac{\langle v', v' \rangle}{2} \pmod{2}$ , where  $v'$  is a lift of  $v \in V$  to  $\Lambda$ . We remark that  $q$  is well-defined since the bilinear form on any lattice of type  $E$  is even. Recall from Remark 4.3.6 that we may view  $\varkappa_C$  as an element of  $T_0 := \text{Hom}(\Lambda, \mathbb{G}_m)(k)$  which is well-defined up to inversion and the Weyl group of  $T_0$ . Additionally, we have that  $\Lambda$  is endowed with a Galois action from this assignment.

We now use the curve  $C$  to produce the data needed for Lurie's construction, as described in Section 2.6.10. Let  $\mathcal{L}_0$  be the distinguished line bundle on  $C$  from Section 2.7 and let  $\tilde{H}_{\mathcal{L}_0}$  be the associated Heisenberg group. We have the exact sequence

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \tilde{H}_{\mathcal{L}_0} \longrightarrow \text{Pic}^0(C)[2] \longrightarrow 1$$

and by Proposition 2.8.10 an injection  $\text{Pic}^0(C)[2] \hookrightarrow \Lambda^\vee/2\Lambda^\vee$  induced from restriction of divisor classes. This gives us the diagram with exact rows via duality and pullback

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \tilde{H}_{\mathcal{L}_0} & \longrightarrow & \text{Pic}^0(C)[2] \longrightarrow 1 \\ & & \parallel & & \uparrow & & \uparrow \gamma \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \tilde{E} & \xrightarrow{\psi} & V \longrightarrow 1. \end{array}$$

Note that the commutator pairing on  $\tilde{H}_{\mathcal{L}_0}$  descends to the Weil pairing on  $\text{Pic}^0(C)[2]$ . Since by definition the kernel of  $\gamma$  is the radical of  $\langle \cdot, \cdot \rangle_2$ , it follows that the commutator pairing on  $\tilde{E}$  descends to  $\langle \cdot, \cdot \rangle_2$  on  $V$ .

Define a character of  $\tilde{E}$  by  $\chi_q(\tilde{e}) = \tilde{e}^2(-1)^{q(\psi\tilde{e})}$ . Note that  $\chi_q$  is well-defined since  $\tilde{e}^2 \in \mathbb{G}_m$ . Letting  $\tilde{V} := \ker \chi_q$  gives us the extension

$$1 \longrightarrow \{\pm 1\} \longrightarrow \tilde{V} \longrightarrow V \longrightarrow 1.$$

We define  $W := H^0(\text{Pic}^0(C), \mathcal{L})$ . Note that  $\tilde{H}_{\mathcal{L}_0}$  acts on  $W$  by pullback of sections, so we define  $\tilde{V}$  to act on  $W$  via the surjective homomorphism  $\tilde{V} \rightarrow \tilde{H}_{\mathcal{L}_0}$ . If  $k = k^{\text{sep}}$ , then this is a 16-dimensional irreducible representation of  $\tilde{V}(k^{\text{sep}})$  sending  $-1$  to  $-\text{id}_W$ . It is clear this action is Galois equivariant.

We have now constructed a quadruplet  $(\Lambda, \tilde{V}, W, \rho)$  satisfying the conditions of Data I in Section 2.6.10. Thus, by Theorem 2.6.59, we obtain a simple adjoint group  $H_0$  of type  $E_8$ , an involution  $\theta_0$  leaving the maximal torus  $T_0 \subseteq H_0$  stable, and a representation of  $\mathfrak{g}_0 = \mathfrak{h}_0^{d\theta=1}$ . We have that  $\theta_0$  acts on  $T_0$  by  $t \mapsto t^{-1}$  and that  $T_0$  is canonically identified with  $\text{Hom}(\Lambda, \mathbb{G}_m)$ . From now on we view  $\varkappa_C$  as a point of  $T_0$ .

We now show that  $\theta_0$  is split. Since  $C$  is of split type, we may assume by Remark 4.3.6 that  $\Lambda = \text{Pic}(S)^\perp$ , where  $(S/k, \{e_1, \dots, e_8\})$  is a del Pezzo surface of degree 1 with a Galois invariant marking. Since  $S/k$  is isomorphic to the blow-up of  $\mathbb{P}^2$  at eight points, we obtain a divisor class  $l \in \text{Pic}(S)$  from the hyperplane class in  $\mathbb{P}^2$ . The class  $l$  satisfies  $\langle l, l \rangle = 1$  and  $\langle l, e_i \rangle = 0$  for all  $i \in \{1 \dots 8\}$ . Setting  $\kappa_S := e_1 + \dots + e_8 - 3l$ , we have that the set of roots  $\{e_1 + \kappa_S, \dots, e_8 + \kappa_S\}$  determines a set of positive roots  $\Phi^+$  of  $\Lambda$ . Because  $\{l, e_1, \dots, e_8\}$  is Galois invariant, both  $\Delta$  and  $\Phi^+$  are as well. For each  $\alpha \in \Phi^+$ , let  $X_\alpha$  be a non-zero element in the corresponding root space. By a MAGMA calculation [Kul18c], we see that  $\sum_{\alpha \in \Phi^+} X_\alpha$  is a regular nilpotent element. By [Tho13, Lemma 2.14] and [Tho16, proof of Proposition 1.9], we have that  $\theta_0$  is split.

By Proposition 2.6.56 there is an isomorphism  $\varphi: H \rightarrow H_0$ , unique up to  $H^\theta(k)$ -conjugacy, satisfying  $\theta_0\varphi = \varphi\theta$ . By Corollary 2.6.51 this isomorphism is unique up to  $G(k)$ -conjugacy as well. The subtorus  $T := \varphi^{-1}(T_0)$  of  $H$  is maximal and  $\theta$  acts on  $T$  by  $t \mapsto t^{-1}$ .

It follows that the orbit  $G(k) \cdot \varphi^{-1}(\varkappa_C) \in G(k) \backslash X(k)$  is well-defined. By Theorem 4.1.2 and Theorem 2.6.54 this orbit is stable (regular semi-simple) and the map  $\mathcal{U}_4^{\text{s,ram}}(k) \rightarrow G(k) \backslash X^{\text{rss}}(k)$

is bijective when  $k = k^{\text{sep}}$ . We are now finished with the  $E_8$  case. The proof of the  $\epsilon_8$  case is nearly identical, with the maximal tori of  $H$  replaced by Cartan subalgebras of  $\mathfrak{h}$ .  $\square$

#### 4.4.2 Proof of Theorem 4.1.4

To prove Theorem 4.1.4, one could transplant the proof of [Tho16, Theorem 3.6] as the arguments almost directly apply to our situation. We have chosen to corral the parts of the argument of [Tho16, Theorem 3.6] that depend only on Lurie's construction into Lemma 4.4.2 and Lemma 4.4.3 in the hopes that it might be of referential convenience.

The data that a curve  $C$  provides to the construction of Lurie is functorial in the theta groups of  $J_C[2]$ . We express this fact as the following two lemmas. Note that the data of a marked ramification point on  $C$  is not necessary to produce the data needed for Lurie's construction. Rather, it is needed at a later point in the argument to mark an orbit in the appropriate orbit space.

**Lemma 4.4.2.** *Let  $\Lambda$  be an irreducible simply laced root lattice and let  $V = \Lambda/2\Lambda$ . Let  $C$  be any curve such that there exists a surjection  $\gamma: V \rightarrow \text{Pic}^0(C)[2]$  such that the natural pairing on  $V$  descends to the Weil pairing. Then the construction of Lurie from Section 2.6.10 defines a map*

$$\{\text{theta groups of } J_C[2]\} \rightarrow \mathcal{D}(k).$$

*Moreover, if  $(H_0, \theta_0, T_0, \rho_0)$  is a quadruple in the image of this map, then  $T_0$  is canonically identified with the torus  $\text{Hom}(\Lambda, \mathbb{G}_m)$ .*

*Proof.* The result is established by the first two paragraphs of the proof of [Tho16, Theorem 3.6]. Alternatively, one can consult the proof of Theorem 4.1.3 above and replace the choice of Heisenberg group with any theta group of  $J_C[2]$ .  $\square$

**Lemma 4.4.3.** *Let  $C/k$  be a curve satisfying the conditions of the previous lemma, let  $A \in J_C(k)$  represent a class in  $J_C(k)/2$  and let  $B \in J_C(k^{\text{sep}})$  be such that  $[2]B = A$ . Let  $\psi_B$  be the morphism of theta groups*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \tilde{H}_{\mathcal{L}} & \longrightarrow & J_C[2] \longrightarrow 0 \\ & & \parallel & & \downarrow \psi_B & & \parallel \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \tilde{H}_{\mathcal{L}_B} & \longrightarrow & J_C[2] \longrightarrow 0 \end{array}$$

*defined over  $k^{\text{sep}}$  induced by translation by  $B$ . Then the construction of Lurie gives a corresponding morphism of tuples  $\psi_B: (H_0, \theta_0, T_0, \rho_0) \rightarrow (H_B, \theta_B, T_B, \rho_B)$ . Moreover, if  $i_0, i_B$  are the canonical identifications of  $\text{Hom}(\Lambda, \mathbb{G}_m)$  with  $T_0, T_B$  respectively, then  $\psi_B i_0 = i_B$ . Furthermore, this morphism is exactly the morphism induced by the image of  $\sigma \mapsto [B^\sigma - B]$  under the inclusion  $J_C[2] \hookrightarrow V^\vee$  via [Tho16, Lemma 2.4].*

*Proof.* Functoriality is established by the comments preceding [Tho16, Lemma 2.4]. The remaining details can be found in paragraph 5 of the proof of [Tho16, Theorem 3.6].  $\square$

We now arrive at the main result of this section.

**Theorem 4.1.4.**

$E_8$ : Fix an  $x = (C, P) \in \mathcal{U}_4^{\text{s,ram}}(k)$  and by abuse of notation we denote by  $x$  the image of  $(C, P)$  in  $T//W_T$ . Let  $\pi: X \rightarrow X//G$  denote the natural quotient map, where  $X, G$  are as in Theorem 4.1.3- $E_8$ . Note that  $X//G$  is canonically isomorphic to  $T//W_T$ . Let  $X_x$  be the fibre of  $\pi$  over  $x$  and let  $J_x = J_C$ . Then there is a canonical injective map

$$\frac{J_x(k)}{2J_x(k)} \hookrightarrow G(k) \backslash X_x(k).$$

$e_8$ : Fix an  $x = (C, P) \in \mathcal{U}_4^{\text{t,ram}}(k)$  and by abuse of notation we denote by  $x$  the image of  $(C, P)$  in  $\mathbb{P}t//W_T$ . Let  $\pi: \mathbb{P}X \rightarrow \mathbb{P}X//G$  denote the natural quotient map, where  $X, G$  are as in Theorem 4.1.3- $e_8$ . Let  $\mathbb{P}X_x$  be the fibre of  $\pi$  over  $x$  and let  $J_x = J_C$ . Then there is a canonical injective map

$$\frac{J_x(k)}{2J_x(k)} \hookrightarrow G(k) \backslash \mathbb{P}X_x(k).$$

*Proof.* Let  $\Lambda$  be a simply laced lattice of Dynkin type  $E_8$  and let  $V = \Lambda/2\Lambda$ . Let  $A \in J_x(k)$  be a rational point and choose  $B \in J_x(k^{\text{sep}})$  such that  $[2]B = A$ . As before, we have by Proposition 2.8.10 that there is an isomorphism  $V \rightarrow J_x[2]$  of  $k$ -groups. As before, the natural pairing on  $\Lambda$  descends to the Weil pairing on  $J_x[2]$ .

Translation by  $B$  induces an isomorphism of theta groups  $\tilde{H}_{\mathcal{L}_0} \cong \tilde{H}_{\mathcal{L}_B}$  defined over  $k^{\text{sep}}$ . By Lemma 4.4.2 we obtain quadruples  $(H_0, \theta_0, T_0, \rho_0)$  and  $(H_B, \theta_B, T_B, \rho_B)$  from  $\tilde{H}_{\mathcal{L}_0}$  and  $\tilde{H}_{\mathcal{L}_B}$  respectively, and by Lemma 4.4.3 we obtain an isomorphism of these tuples  $F: (H_0, \theta_0, T_0, \rho_0) \xrightarrow{\sim} (H_B, \theta_B, T_B, \rho_B)$  defined over  $k^{\text{sep}}$ . From Lemma 4.4.3, we see that the cocycle  $\sigma \mapsto F^{-1}F^\sigma$  is canonically identified with the cocycle  $\sigma \mapsto [B^\sigma - B]$ . Note if  $A = B = 0$  then all of these isomorphisms are in fact identity maps.

By Remark 4.3.6 we choose a point in  $\text{Hom}(\Lambda, \mathbb{G}_m)^{\text{rss}}(k)$  lying over  $x \in T//W_T(k)$ , which we will denote by  $\varkappa_C$ . We use  $\varkappa_C$  to construct a  $G(k)$ -orbit in  $X_x(k)$ . As in Theorem 4.1.3 we obtain morphisms

$$\begin{aligned} \varphi_0: (H, \theta, T, \rho) &\rightarrow (H_0, \theta_0, T_0, \rho_0) \\ \varphi_B: (H, \theta, T', \rho') &\rightarrow (H_B, \theta_B, T_B, \rho_B) \end{aligned}$$

defined over  $k$ . The morphisms  $\varphi_0, \varphi_B$  are unique up to  $G(k)$ -conjugacy. Via the canonical identifications of  $\text{Hom}(\Lambda, \mathbb{G}_m)$  with  $T_0, T_B$  we obtain points  $\varkappa_C^0 \in T_0(k), \varkappa_C^B \in T_B(k)$ . We have that  $\varphi_0^{-1}(\varkappa_C^0) \in X_x(k)$  is the point constructed in Theorem 4.1.3 and we obtain the corresponding  $G(k)$ -orbit  $G(k) \cdot \varphi_0^{-1}(\varkappa_C^0)$ . Similarly, we obtain the point  $\varphi_B^{-1}(\varkappa_C^B)$  and the orbit  $G(k) \cdot \varphi_B^{-1}(\varkappa_C^B)$ . Note by Remark 4.4.1 the  $G(k)$ -orbits  $G(k) \cdot \varphi_0^{-1}(\varkappa_C^0)$  and  $G(k) \cdot \varphi_B^{-1}(\varkappa_C^B)$  are independent of the choice of  $\varkappa_C \in \text{Hom}(\Lambda, \mathbb{G}_m)^{\text{rss}}(k)$  lying over  $x$ .

Note that  $F_x := \varphi_B^{-1} F \varphi_0$  is an automorphism of  $H$  which commutes with  $\theta$ . Additionally, we see that the image under  $F$  of  $T_0$  is exactly  $T_B$  by Lemma 4.4.3, and again by Lemma 4.4.3 we have that  $F(\varkappa_C^0) = \varkappa_C^B$ . Thus, both orbits  $G(k) \cdot \varphi_0^{-1}(\varkappa_C^0)$  and  $G(k) \cdot \varphi_B^{-1}(\varkappa_C^B)$  lie in the slice  $X_x$  and we have that  $F$  induces an automorphism  $F_x: X_x \rightarrow X_x$  defined over  $k^{\text{sep}}$  sending the orbit of  $\varphi_0^{-1}(\varkappa_C^0)$  to the orbit of  $\varphi_B^{-1}(\varkappa_C^B)$ .

As in the proof of [Tho16, Theorem 3.6] we have a canonical bijection from [BG14, Proposition 1]

$$G(k) \backslash X_x(k) \cong \ker(\mathrm{H}^1(k, Z_G(\varphi_0^{-1}(\varkappa_C^0))) \rightarrow \mathrm{H}^1(k, G))$$

under which the orbit  $G(k) \cdot \varphi_0^{-1}(\varkappa_C^0)$  is sent to the zero element and under which the orbit  $G(k) \cdot \varphi_B^{-1}(\varkappa_C^B)$  is sent to the cocycle  $\sigma \mapsto F_x^{-1} F_x^\sigma$ . We also have the canonical isomorphisms

$$Z_G(\varphi_0^{-1}(\varkappa_C^0)) \cong Z_{G_0}(\varkappa_C^0) \cong \mathrm{Im}(V \rightarrow V^\vee)$$

from [Tho13, Corollary 2.9]. By Proposition 2.8.10 we have that  $\mathrm{Im}(V \rightarrow V^\vee) \cong J_x[2]$ . Thus there is an injection

$$G(k) \backslash X_x(k) \hookrightarrow \mathrm{H}^1(k, Z_G(\varphi_0^{-1}(\varkappa_C^0))) \cong \mathrm{H}^1(k, J_x[2]).$$

The map in the statement of Theorem 4.1.4 is defined by sending  $A \in J_x(k)/2$  to the orbit  $G(k) \cdot \varphi_B^{-1}(\varkappa_C^B)$ . We have shown that the coboundary map  $\delta: J_x(k)/2 \hookrightarrow \mathrm{H}^1(k, J_x[2])$  factors through  $G(k) \backslash X_x(k)$ , so we see that the mapping  $A \mapsto G(k) \cdot \varphi_B^{-1}(\varkappa_C^B)$  is injective. This finishes the proof in the  $E_8$  case. The  $\epsilon_8$  case is obtained similarly.  $\square$

## 4.5 Future directions

We believe that Theorem 4.1.3 and Theorem 4.1.4 can be generalized to consider arbitrary uniquely trigonal genus 4 curves  $(C, P) \in \mathcal{T}_4^{\text{ram}}(k)$ . To prove analogous statements of Theorem 4.1.3 and Theorem 4.1.4 for  $(C, P) \in \mathcal{T}_4^{\text{ram}}(k)$  we require a key technical detail; namely, given a  $(C, P) \in \mathcal{T}_4^{\text{ram}}(k)$  and a theta group of  $J_C[2]$ , that the involution obtained from Lurie's construction in Lemma 4.4.2 is split. In [Tho16, Theorem 3.5 and Theorem 3.6], the affine algebraic group obtained from Lurie's construction is always split. In our case, the form of the affine algebraic group of type  $E_8$  possibly depends on the curve  $C$ .

**Question 4.5.1.** *Let  $(C, P) \in \mathcal{T}_4^{\text{ram}}(k)$  and let  $\Theta$  be a theta group of  $J_C[2]$ . Is the involution arising from Lurie's construction split?*

We hope to consider this topic in a future article.

# Bibliography

- [AC55] N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math. **5** (1955), 321–324.
- [Bha13] Manjul Bhargava, *Most hyperelliptic curves over  $\mathbb{Q}$  have no rational points*, 2013. arXiv preprint arxiv:1308.0395.
- [BG13] Manjul Bhargava and Benedict H. Gross, *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, Automorphic representations and  $L$ -functions, Tata Inst. Fundam. Res. Stud. Math., vol. 22, Tata Inst. Fund. Res., Mumbai, 2013, pp. 23–91.
- [BG14] ———, *Arithmetic invariant theory*, Symmetry: representation theory and its applications, Progr. Math., vol. 257, Birkhäuser/Springer, New York, 2014, pp. 33–54, DOI 10.1007/978-1-4939-1590-3\_3.
- [BGW17] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang, *A positive proportion of locally soluble hyperelliptic curves over  $\mathbb{Q}$  have no point over any odd degree extension*, J. Amer. Math. Soc. **30** (2017), no. 2, 451–493. With an appendix by Tim Dokchitser and Vladimir Dokchitser.
- [BS15] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242, DOI 10.4007/annals.2015.181.1.3.
- [BS17] M. Bhargava and A. Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, 2017. arXiv preprint arxiv:1312.7859.
- [BG16] Yuri Bilu and Jean Gillibert, *Chevalley-Weil theorem and subgroups of class groups*, arXiv preprint arxiv:1606.03128 (2016).
- [BG18] ———, *Chevalley-Weil theorem and subgroups of class groups*, Israel J. Math. **226** (2018), no. 2, 927–956, DOI 10.1007/s11856-018-1718-9.
- [BL05] Yuri F. Bilu and Florian Luca, *Divisibility of class numbers: enumerative approach*, J. Reine Angew. Math. **578** (2005), 79–91.
- [BL04] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004.
- [BG06] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).
- [Bou68] N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*, Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968 (French).
- [Bou75] ———, *Éléments de mathématique. Fasc. XXXVIII: Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées*, Actualités Scientifiques et Industrielles, No. 1364. Hermann, Paris, 1975 (French).
- [BFT14] Nils Bruin, E. Victor Flynn, and Damiano Testa, *Descent via  $(3, 3)$ -isogeny on Jacobians of genus 2 curves*, Acta Arith. **165** (2014), no. 3, 201–223, DOI 10.4064/aa165-3-1.
- [BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, DOI 10.1090/S0025-5718-09-02255-8.
- [CF07] G. Casnati and C. Fontanari, *On the rationality of moduli spaces of pointed curves*, J. Lond. Math. Soc. (2) **75** (2007), no. 3, 582–596, DOI 10.1112/jlms/jdm011.
- [Çel18] Türkü Özlüm Çelik, *Propriétés géométriques et arithmétiques explicites des courbes*, Université de Rennes 1, IRMAR, 2018.
- [Cla04] Pete Clark, *The period-index problem in WC-groups II: abelian varieties*, 2004. arXiv preprint arxiv:math/0406135.
- [CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), 1984, pp. 33–62.
- [Con02] Brian Conrad, *A modern proof of Chevalley’s theorem on algebraic groups*, J. Ramanujan Math. Soc. **17** (2002), no. 1, 1–18.
- [Con07] ———, *Deligne’s notes on Nagata compactifications*, J. Ramanujan Math. Soc. **22** (2007), no. 3, 205–257.
- [CFO<sup>+</sup>08] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon, and M. Stoll, *Explicit  $n$ -descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155, DOI 10.1515/CRELLE.2008.012.
- [DO88] Igor Dolgachev and David Ortland, *Point sets in projective spaces and theta functions*, Astérisque **165** (1988), 210 pp. (1989) (English, with French summary).
- [Dol12] Igor V. Dolgachev, *Classical algebraic geometry*, Cambridge University Press, Cambridge, 2012. A modern view.
- [DZ94] R. Dvornicich and U. Zannier, *Fields containing values of algebraic functions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **21** (1994), no. 3, 421–443.

- [FH91] William Fulton and Joe Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991. A first course; Readings in Mathematics.
- [Gau66] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, Translated into English by Arthur A. Clarke, S. J., Yale University Press, New Haven, Conn.-London, 1966.
- [GL12] Jean Gillibert and Aaron Levin, *Pulling back torsion line bundles to ideal classes*, Math. Res. Lett. **19** (2012), no. 6, 1171–1184.
- [RLYG12] Mark Reeder, Paul Levy, Jiu-Kang Yu, and Benedict H. Gross, *Gradings of positive rank on simple Lie algebras*, Transform. Groups **17** (2012), no. 4, 1123–1190, DOI 10.1007/s00031-012-9196-3.
- [HM98] Joe Harris and Ian Morrison, *Moduli of curves*, Graduate Texts in Mathematics, vol. 187, Springer-Verlag, New York, 1998.
- [Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.
- [HS00] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. An introduction.
- [Hon68] Taira Honda, *On real quadratic fields whose class numbers are multiples of 3*, J. Reine Angew. Math. **233** (1968), 101–102.
- [Kul16] Avinash Kulkarni, *Magma script accompanying [Kul18a]*, 2016. Available at <http://www.sfu.ca/~akulkarn/delPezzoBranchCurve.m>.
- [Kul17] ———, *An arithmetic invariant theory of curves from  $E_8$* , 2017. arXiv preprint arxiv:1711.08843.
- [Kul18a] ———, *An explicit family of cubic number fields with large 2-rank of the class group*, Acta Arith. **182** (2018), no. 2, 117–132, DOI 10.4064/aa8669-10-2017.
- [Kul18b] ———, *Magma script accompanying this thesis.*, 2018. Available at <http://www.sfu.ca/~akulkarn/q245/>.
- [Kul18c] ———, *Magma script accompanying this thesis.*, 2018. Available at <http://www.sfu.ca/~akulkarn/section44/regular-nilpotent.m>.
- [Loo93] Eduard Looijenga, *Cohomology of  $\mathcal{M}_3$  and  $\mathcal{M}_3^1$* , Mapping class groups and moduli spaces of Riemann surfaces (Göttingen, 1991/Seattle, WA, 1991), Contemp. Math., vol. 150, Amer. Math. Soc., Providence, RI, 1993, pp. 205–228, DOI 10.1090/conm/150/01292.
- [Lur01] Jacob Lurie, *On simply laced Lie algebras and their minuscule representations*, Comment. Math. Helv. **76** (2001), no. 3, 515–575.
- [Mes83] Jean-Francois Mestre, *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, J. Reine Angew. Math. **343** (1983), 23–35.
- [Mil86a] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

- [Mil86b] ———, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.
- [Mil13] James S. Milne, *Lie Algebras, Algebraic Groups, and Lie Groups*, 2013. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).
- [Mum66] D. Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1** (1966), 287–354, DOI 10.1007/BF01389737.
- [Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970.
- [MFK94] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], vol. 34, Springer-Verlag, Berlin, 1994.
- [Mur99] M. Ram Murty, *Exponents of class groups of quadratic fields*, Topics in number theory (University Park, PA, 1997), 1999, pp. 229–239.
- [Nag22] Trygve Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **1** (1922), no. 1, 140–150.
- [Nak86] Shin Nakano, *On the construction of pure number fields of odd degrees with large 2-class groups*, Proc. Japan Acad. Ser. A Math. Sci. **62** (1986), no. 2, 61–64.
- [Nak88] ———, *Construction of pure cubic fields with large 2-class groups*, Osaka J. Math. **25** (1988), no. 1, 161–170.
- [Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; With a foreword by G. Harder.
- [PS14] Bjorn Poonen and Michael Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), no. 3, 1137–1166, DOI 10.4007/annals.2014.180.3.7.
- [AC55] N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*, Pacific J. Math. **5** (1955), 321–324.
- [Bha13] Manjul Bhargava, *Most hyperelliptic curves over  $Q$  have no rational points*, 2013. arXiv preprint arxiv:1308.0395.
- [BG13] Manjul Bhargava and Benedict H. Gross, *The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point*, Automorphic representations and  $L$ -functions, Tata Inst. Fundam. Res. Stud. Math., vol. 22, Tata Inst. Fund. Res., Mumbai, 2013, pp. 23–91.
- [BG14] ———, *Arithmetic invariant theory*, Symmetry: representation theory and its applications, Progr. Math., vol. 257, Birkhäuser/Springer, New York, 2014, pp. 33–54, DOI 10.1007/978-1-4939-1590-3\_3.

- [BGW17] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang, *A positive proportion of locally soluble hyperelliptic curves over  $\mathbb{Q}$  have no point over any odd degree extension*, J. Amer. Math. Soc. **30** (2017), no. 2, 451–493. With an appendix by Tim Dokchitser and Vladimir Dokchitser.
- [BS15] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242, DOI 10.4007/annals.2015.181.1.3.
- [BS17] M. Bhargava and A. Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, 2017. arXiv preprint arxiv:1312.7859.
- [BG16] Yuri Bilu and Jean Gillibert, *Chevalley-Weil theorem and subgroups of class groups*, arXiv preprint arxiv:1606.03128 (2016).
- [BL05] Yuri F. Bilu and Florian Luca, *Divisibility of class numbers: enumerative approach*, J. Reine Angew. Math. **578** (2005), 79–91.
- [BL04] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004.
- [BG06] Enrico Bombieri and Walter Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.
- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993).
- [Bou68] N. Bourbaki, *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*, Actualités Scientifiques et Industrielles, No. 1337, Hermann, Paris, 1968 (French).
- [Bou75] ———, *Éléments de mathématique. Fasc. XXXVIII: Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées*, Actualités Scientifiques et Industrielles, No. 1364. Hermann, Paris, 1975 (French).
- [BFT14] Nils Bruin, E. Victor Flynn, and Damiano Testa, *Descent via  $(3, 3)$ -isogeny on Jacobians of genus 2 curves*, Acta Arith. **165** (2014), no. 3, 201–223, DOI 10.4064/aa165-3-1.
- [BS09] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, Math. Comp. **78** (2009), no. 268, 2347–2370, DOI 10.1090/S0025-5718-09-02255-8.
- [CF07] G. Casnati and C. Fontanari, *On the rationality of moduli spaces of pointed curves*, J. Lond. Math. Soc. (2) **75** (2007), no. 3, 582–596, DOI 10.1112/jlms/jdm011.
- [Çel18] Türkü Özlüm Çelik, *Propriétés géométriques et arithmétiques explicites des courbes*, Université de Rennes 1, IRMAR, 2018.

- [Cla04] Pete Clark, *The period-index problem in WC-groups II: abelian varieties*, 2004. arXiv preprint arxiv:math/0406135.
- [CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), 1984, pp. 33–62.
- [Con02] Brian Conrad, *A modern proof of Chevalley’s theorem on algebraic groups*, J. Ramanujan Math. Soc. **17** (2002), no. 1, 1–18.
- [Con07] ———, *Deligne’s notes on Nagata compactifications*, J. Ramanujan Math. Soc. **22** (2007), no. 3, 205–257.
- [CFO<sup>+</sup>08] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon, and M. Stoll, *Explicit  $n$ -descent on elliptic curves. I. Algebra*, J. Reine Angew. Math. **615** (2008), 121–155, DOI 10.1515/CRELLE.2008.012.
- [DO88] Igor Dolgachev and David Ortland, *Point sets in projective spaces and theta functions*, Astérisque **165** (1988), 210 pp. (1989) (English, with French summary).
- [Dol12] Igor V. Dolgachev, *Classical algebraic geometry*, Cambridge University Press, Cambridge, 2012. A modern view.
- [DZ94] R. Dvornicich and U. Zannier, *Fields containing values of algebraic functions*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **21** (1994), no. 3, 421–443.
- [FH91] William Fulton and Joe Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991. A first course; Readings in Mathematics.
- [Gau66] Carl Friedrich Gauss, *Disquisitiones arithmeticae*, Translated into English by Arthur A. Clarke, S. J, Yale University Press, New Haven, Conn.-London, 1966.
- [GL12] Jean Gillibert and Aaron Levin, *Pulling back torsion line bundles to ideal classes*, Math. Res. Lett. **19** (2012), no. 6, 1171–1184.
- [RLYG12] Mark Reeder, Paul Levy, Jiu-Kang Yu, and Benedict H. Gross, *Gradings of positive rank on simple Lie algebras*, Transform. Groups **17** (2012), no. 4, 1123–1190, DOI 10.1007/s00031-012-9196-3.
- [HM98] Joe Harris and Ian Morrison, *Moduli of curves*, Graduate Texts in Mathematics, vol. 187, Springer-Verlag, New York, 1998.
- [Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.
- [HS00] Marc Hindry and Joseph H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. An introduction.
- [Hon68] Taira Honda, *On real quadratic fields whose class numbers are multiples of 3*, J. Reine Angew. Math. **233** (1968), 101–102.
- [Kul16a] Avinash Kulkarni, *An explicit family of cubic number fields with large 2-rank of the class group*, 2016.

- [Kul16b] ———, *Magma script accompanying [Kul18a]*, 2016. Available at <http://www.sfu.ca/~akulkarn/delPezzoBranchCurve.m>.
- [Kul17] ———, *An arithmetic invariant theory of curves from  $E_8$* , 2017. arXiv preprint arxiv:1711.08843.
- [Kul18a] ———, *Magma script accompanying this thesis.*, 2018. Available at <http://www.sfu.ca/~akulkarn/q245/>.
- [Kul18b] ———, *Magma script accompanying this thesis.*, 2018. Available at <http://www.sfu.ca/~akulkarn/section44/regular-nilpotent.m>.
- [Loo93] Eduard Looijenga, *Cohomology of  $\mathcal{M}_3$  and  $\mathcal{M}_3^1$* , Mapping class groups and moduli spaces of Riemann surfaces (Göttingen, 1991/Seattle, WA, 1991), Contemp. Math., vol. 150, Amer. Math. Soc., Providence, RI, 1993, pp. 205–228, DOI 10.1090/conm/150/01292.
- [Lur01] Jacob Lurie, *On simply laced Lie algebras and their minuscule representations*, Comment. Math. Helv. **76** (2001), no. 3, 515–575.
- [Mes83] Jean-Francois Mestre, *Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques*, J. Reine Angew. Math. **343** (1983), 23–35.
- [Mil86a] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.
- [Mil86b] ———, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.
- [Mil13] James S. Milne, *Lie Algebras, Algebraic Groups, and Lie Groups*, 2013. Available at [www.jmilne.org/math/](http://www.jmilne.org/math/).
- [Mum66] D. Mumford, *On the equations defining abelian varieties. I*, Invent. Math. **1** (1966), 287–354, DOI 10.1007/BF01389737.
- [Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970.
- [MFK94] D. Mumford, J. Fogarty, and F. Kirwan, *Geometric invariant theory*, 3rd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (2) [Results in Mathematics and Related Areas (2)], vol. 34, Springer-Verlag, Berlin, 1994.
- [Mur99] M. Ram Murty, *Exponents of class groups of quadratic fields*, Topics in number theory (University Park, PA, 1997), 1999, pp. 229–239.
- [Nag22] Trygve Nagell, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **1** (1922), no. 1, 140–150.
- [Nak86] Shin Nakano, *On the construction of pure number fields of odd degrees with large 2-class groups*, Proc. Japan Acad. Ser. A Math. Sci. **62** (1986), no. 2, 61–64.

- [Nak88] ———, *Construction of pure cubic fields with large 2-class groups*, Osaka J. Math. **25** (1988), no. 1, 161–170.
- [Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; With a foreword by G. Harder.
- [PS14] Bjorn Poonen and Michael Stoll, *Most odd degree hyperelliptic curves have only one rational point*, Ann. of Math. (2) **180** (2014), no. 3, 1137–1166, DOI 10.4007/annals.2014.180.3.7.
- [Poo17] Bjorn Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017.
- [RS17] E. M. Rains and S. V. Sam, *Invariant theory of  $\wedge^3(9)$  and genus 2 curves*, 2017. arXiv preprint arxiv:1702.04840.
- [Ree10] Mark Reeder, *Torsion automorphisms of simple Lie algebras*, Enseign. Math. (2) **56** (2010), no. 1-2, 3–47, DOI 10.4171/LEM/56-1-1.
- [Ric82] R. W. Richardson, *Orbits, invariants, and representations associated to involutions of reductive groups*, Invent. Math. **66** (1982), no. 2, 287–312, DOI 10.1007/BF01389396.
- [RT17] Beth Romano and Jack Thorne, *On the arithmetic of simple singularities of type E*, 2017. arXiv preprint arxiv:1707.04355.
- [Sch98] Edward F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310** (1998), no. 3, 447–471.
- [SS04] Edward F. Schaefer and Michael Stoll, *How to do a  $p$ -descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231.
- [Ser02] Jean-Pierre Serre, *Galois cohomology*, Corrected reprint of the 1997 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. Translated from the French by Patrick Ion and revised by the author.
- [Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
- [SP] The Stacks project authors, *The Stacks project* (2018), <https://stacks.math.columbia.edu>.
- [TY05] Patrice Tauvel and Rupert W. T. Yu, *Lie algebras and algebraic groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005.
- [Tho13] Jack A. Thorne, *Vinberg’s representations and arithmetic invariant theory*, Algebra Number Theory **7** (2013), no. 9, 2331–2368, DOI 10.2140/ant.2013.7.2331.
- [Tho16] ———, *Arithmetic invariant theory and 2-descent for plane quartic curves*, Algebra Number Theory **10** (2016), no. 7, 1373–1413, DOI 10.2140/ant.2016.10.1373. With an appendix by Tasho Kaletha.

- [Tit66] J. Tits, *Classification of algebraic semisimple groups*, Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), Amer. Math. Soc., Providence, R.I., 1966, 1966, pp. 33–62.
- [Wan13] Xiaoheng Wang, *Pencils of quadrics and Jacobians of hyperelliptic curves*, ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)—Harvard University.
- [Vak01] Ravi Vakil, *Twelve points on the projective line, branched covers, and rational elliptic fibrations*, Math. Ann. **320** (2001), no. 1, 33–54, DOI 10.1007/PL00004469.
- [Vin76] È. B. Vinberg, *The Weyl group of a graded Lie algebra*, Izv. Akad. Nauk SSSR Ser. Mat. **40** (1976), no. 3, 488–526, 709 (Russian).
- [Wei73] P. J. Weinberger, *Real quadratic fields with class numbers divisible by  $n$* , J. Number Theory **5** (1973), 237–241.
- [Yam70] Yoshihiko Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.
- [Zar08] Yu. G. Zarhin, *Del Pezzo surfaces of degree 1 and Jacobians*, Math. Ann. **340** (2008), no. 2, 407–435, DOI 10.1007/s00208-007-0157-4.

# Appendix A

## Some results on theta groups

We provide some commentary on the technical details in the proof of Proposition 2.7.5(a,b). The results are well-known, but we found it difficult to find a preexisting reference in the literature. Throughout, we let  $C/k$  be a smooth curve of genus  $g > 1$ , and  $J_C$  its Jacobian variety. The results in this section are true for  $g = 1$  by [CFO<sup>+</sup>08]. The proofs in the genus 1 case carry over almost directly.

We recall the definition of an (abstract) theta group from Section 2.7.

**Definition A.0.1.** A *theta group* of  $J_C[2]$  is a central extension of  $k$ -groups

$$0 \longrightarrow \mathbb{G}_m \xrightarrow{\eta} \Theta \xrightarrow{\pi} J_C[2] \longrightarrow 0$$

such that the commutator pairing on  $\Theta$  descends to the Weil pairing on  $J_C[2]$ . A *morphism of theta groups* is a morphism such that the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Theta_1 & \longrightarrow & J_C[2] \longrightarrow 0 \\ & & \parallel & & \downarrow \psi & & \parallel \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Theta_2 & \longrightarrow & J_C[2] \longrightarrow 0 \end{array}$$

commutes.

We point out that Mumford [Mum70, Section 23] has also introduced the closely related concept of the theta group of a line bundle. We will not need this notion and our focus will be on theta groups as in the definition above.

**Lemma A.0.2.** Let  $\Theta$  be a theta group of  $J_C[2]$  and let  $x, y \in \Theta$ . Then

$$xyx^{-1}y^{-1} = \eta(e_2(\pi x, \pi y))$$

where  $e_2: J_C[2] \times J_C[2] \rightarrow \mathbb{G}_m$  is the Weil pairing on  $J_C[2]$ .

*Proof.* See [Mum70, Section 23]. □

## A.1 Part (a): $k$ -isomorphism classes of theta groups

We prove that the  $k$ -isomorphism classes of theta groups are in bijection with elements of  $H^1(k, J_C[2])$ . We let

$$F := \mathbb{G}_m(k^{\text{sep}}) \times \langle a_1, \dots, a_g, b_1, \dots, b_g \rangle$$

where  $\langle \dots \rangle$  denotes the free group on the symbols  $a_1, \dots, b_g$ . Note that the centre of  $F$  is canonically identified with  $\mathbb{G}_m(k^{\text{sep}})$  by definition; we abbreviate the element  $(\lambda, x)$  by  $\lambda x$  and we abbreviate  $(-1, x)$  by  $-x$  (note that  $-x$  is not necessarily  $x^{-1}$ ). We let  $R$  be the set of relations generated by

$$\{a_i^2 = b_i^2 = 1, a_i b_j = -b_j a_i, b_i b_j = b_j b_i, a_i a_j = a_j a_i\}$$

and we define  $H := F/R$ .

**Lemma A.1.1.** *Let  $\Theta$  be a theta group of  $J_C[2]$ . Then as a group  $\Theta(k^{\text{sep}})$  is isomorphic to  $H$ . In particular, any two abstract theta groups of  $J_C[2]$  are isomorphic over  $k^{\text{sep}}$ .*

*Proof.* Let  $a_1, \dots, a_g, b_1, \dots, b_g$  be a symplectic basis for  $J_C[2](k^{\text{sep}})$  with respect to the Weil pairing. Since  $\mathbb{G}_m(k^{\text{sep}})$  is divisible, we may choose lifts of the  $a_i, b_i$  to  $\Theta$  such that  $a_i^2 = b_i^2 = 1$ . Since the commutator of  $a_i, b_j$  is  $e_2(\pi(a_i), \pi(b_j))$ , we have that the  $a_i, b_j$  satisfy the same relations as the generators in the definition of  $H$ , so by identifying the generators of  $H$  with the elements  $a_i, b_j \in \Theta(k^{\text{sep}})$  we define a morphism

$$\rho: H \rightarrow \Theta(k^{\text{sep}})$$

such that  $\rho(\mathbb{G}_m(k^{\text{sep}})) = \mathbb{G}_m(k^{\text{sep}})$  and such that  $\rho$  induces the identity on  $\mathbb{G}_m(k^{\text{sep}})$ . We claim that  $\rho$  is an isomorphism. For injectivity, let  $x \in \ker \rho$ . Up to the defining relations we may assume that  $x$  is of the form

$$x = \lambda a_1^{c_1} \dots a_g^{c_g} b_1^{c_{g+1}} \dots b_g^{c_{2g}} \quad \text{for } c_i \in \{0, 1\} \text{ and } \lambda \in \mathbb{G}_m(k^{\text{sep}}).$$

Since  $\rho(x)$  is trivial, we have that  $\pi(\rho(x))$  is also trivial. As the  $a_i, b_i$  were chosen to be a basis for  $J_C[2](k^{\text{sep}})$ , it follows that each  $c_i = 0$ . It follows that  $\lambda = 1$  as well.

For surjectivity, we have for any  $y \in \Theta$  that

$$\pi(y) = c_1 a_1 + \dots + c_g a_g + c_{g+1} b_1 + \dots + c_{2g} b_g \quad \text{for some } c_i \in \{0, 1\}$$

where we write  $J_C[2](k^{\text{sep}})$  as an additive group. Set  $x := a_1^{c_1} \dots a_g^{c_g} b_1^{c_{g+1}} \dots b_g^{c_{2g}}$ . It follows that  $\rho(\pi(x)) = \pi(y)$ , so  $\rho(x)$  and  $y$  differ by an element of  $\mathbb{G}_m(k^{\text{sep}})$ .  $\square$

**Proposition A.1.2.** *There is a bijection between  $k$ -isomorphism classes of theta groups of  $J_C[2]$  and elements of  $H^1(k, J_C[2])$ .*

*Proof.* Since  $\mathbb{G}_m(k^{\text{sep}})$  is exactly the centre of  $\Theta(k^{\text{sep}})$ , we have that the inner automorphism group of  $\Theta(k^{\text{sep}})$  is isomorphic to  $J_C[2](k^{\text{sep}})$ , and that every inner automorphism fixes  $\mathbb{G}_m$  and induces the identity on  $\Theta/\mathbb{G}_m = J_C[2]$ . That is, we have that the automorphism group of the central extension  $(\mathbb{G}_m(k^{\text{sep}}) \rightarrow \Theta(k^{\text{sep}}) \rightarrow J_C[2](k^{\text{sep}}))$  is isomorphic to  $J_C[2](k^{\text{sep}})$ . Since any two theta groups of  $J_C[2]$  are isomorphic over  $k^{\text{sep}}$ , the result follows from the twisting principle.  $\square$

## A.2 Part (b): Representations of theta groups

We prove that every theta group admits a natural embedding into  $\mathrm{GL}_{2g}$  as  $k$ -groups. We will need to use some terminology from [CFO<sup>+</sup>08]. If  $X/k$  is a variety, a *twist* of  $X/k$  is a variety  $Y/k$  such that  $X_{k^{\mathrm{al}}} \cong Y_{k^{\mathrm{al}}}$ .

**Definition A.2.1.** A *Brauer-Severi variety* is a variety  $S/k$  such that  $S_{k^{\mathrm{al}}} \cong \mathbb{P}_{k^{\mathrm{al}}}^n$  for some  $n \geq 1$ .

If  $X/k$  is a projective variety and the functor  $R \mapsto \mathrm{Aut}_R(X \times_k R)$  from  $\mathbf{k}\text{-alg}$  to  $\mathbf{Set}$  is representable by a scheme, we denote the  $k$ -group representing this functor by  $\underline{\mathrm{Aut}}(X)$ . Note that the functor  $R \mapsto \mathrm{Aut}_R(\mathbb{P}_k^n \times_k R)$  is representable by the  $k$ -group  $\mathrm{PGL}_{n+1}$ . By definition every Brauer-Severi variety  $S$  of dimension  $n$  is a twist of  $\mathbb{P}^n$ , so we have that the automorphisms of  $S$  have the structure of a  $k$ -group. If  $S(k) \neq \emptyset$ , then we have that  $S \cong \mathbb{P}^n$  and  $\underline{\mathrm{Aut}}(S) \cong \underline{\mathrm{Aut}}(\mathbb{P}^n)$ .

**Definition A.2.2.** Let  $X/k$  be a torsor of  $J_C$ . A *diagram*  $[X \rightarrow S]$  is a morphism from  $X$  to  $S$  defined over  $k$ . An *isomorphism of diagrams*  $f: [X_1 \rightarrow S_1] \rightarrow [X_2 \rightarrow S_2]$  is a pair of isomorphisms  $(f: X_1 \rightarrow X_2, g: S_1 \rightarrow S_2)$  over  $k$  such that the square

$$\begin{array}{ccc} X_1 & \longrightarrow & S_1 \\ \downarrow f & & \downarrow g \\ X_2 & \longrightarrow & S_2 \end{array}$$

commutes.

If  $\mathcal{L}_0$  is the distinguished line bundle on  $J_C$  from Section 2.7, then the global sections of  $\mathcal{L}_0$  define a morphism  $\varphi_{\mathcal{L}_0}: J_C \rightarrow |\mathcal{L}_0|^\vee \cong \mathbb{P}^{2g-1}$ . This is the natural analogue of the morphism given by the linear system  $|2O_E|$  of an elliptic curve  $E$  with identity point  $O_E$ .

**Definition A.2.3.** A *Brauer-Severi diagram* is a twist of the diagram  $[\varphi_{\mathcal{L}_0}: J_C \rightarrow \mathbb{P}^{2g-1}]$ . In other words, a Brauer-Severi diagram is a diagram  $[X \rightarrow S]$  such that there is an isomorphism of diagrams  $f: [\varphi_{\mathcal{L}_0}: J_C \rightarrow \mathbb{P}^{2g-1}] \rightarrow [X \rightarrow S]$  over  $k^{\mathrm{sep}}$ .

The automorphisms  $\sigma$  of  $J_C$  such that  $\sigma^* \mathcal{L}_0 \cong \mathcal{L}_0$  are exactly the translation morphisms  $\tau_x$  with  $x \in J_C[2](k^{\mathrm{sep}})$ . In particular, each  $\tau_x$  acts on the global sections of  $\mathcal{L}_0$  and hence defines a linear automorphism of  $|\mathcal{L}_0|^\vee$ . We formulate this as a lemma.

**Lemma A.2.4.** *Let  $x \in J_C[2](k^{\mathrm{sep}})$  and let  $\tau_x: J_C \rightarrow J_C$  be the translation by  $x$ . Then  $\tau_x^* \mathcal{L}_0 \cong \mathcal{L}_0$ , and  $\tau_x^*$  induces a linear action on  $|\mathcal{L}_0|^\vee$ . There is an injective morphism  $\rho: J_C[2] \rightarrow \mathrm{PGL}_{2g}$  of  $k$ -groups such that*

$$\begin{array}{ccc} J_C & \xrightarrow{\tau_x} & J_C \\ \downarrow & & \downarrow \\ |\mathcal{L}_0|^\vee & \xrightarrow{\rho(x)} & |\mathcal{L}_0|^\vee \end{array}$$

*commutes for all  $x \in J_C[2](k^{\mathrm{sep}})$ . Furthermore, the mapping above defines a Galois-equivariant isomorphism  $J_C[2](k^{\mathrm{sep}}) \cong \mathrm{Aut}_{k^{\mathrm{sep}}}[J_C \rightarrow \mathbb{P}^{2g-1}]$  of groups.*

By the lemma above, we may view the automorphisms of the diagram  $[J_C \rightarrow \mathbb{P}^{2g-1}]$  as a  $k$ -group isomorphic to  $J_C[2]$ . We denote this  $k$ -group by  $\underline{\text{Aut}}[J_C \rightarrow \mathbb{P}^{2g-1}]$ . Let  $\rho: J_C[2] \rightarrow \text{PGL}_{2g}$  be the representation in the lemma above and consider the exact sequence of  $k$ -groups

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \text{GL}_{2g} \xrightarrow{\alpha} \text{PGL}_{2g} \longrightarrow 0.$$

We define  $\Theta_{J_C} := \alpha^{-1}\rho(J_C[2])$ . By definition, we have that there is an injective morphism  $\rho_0: \Theta_{J_C} \rightarrow \text{GL}_{2g}$  of  $k$ -groups.

**Lemma A.2.5.** *The group  $\Theta_{J_C}$  is a theta group of  $J_C[2]$ .*

*Proof.* The definition of  $\Theta_{J_C}$  is a concrete description of the Heisenberg group  $\tilde{H}_{\mathcal{L}_0}$ . More precisely, the natural action of  $\tilde{H}_{\mathcal{L}_0}$  on  $H^0(J_C, \mathcal{L}_0)$  defines a representation whose image is  $\Theta_{J_C}$ .  $\square$

If  $[X \rightarrow S]$  is a Brauer-Severi diagram, then there are isomorphisms of  $k$ -groups  $\underline{\text{Aut}}[X \rightarrow S] \cong \underline{\text{Aut}}[J_C \rightarrow \mathbb{P}^{2g-1}] \cong J_C[2]$ . The action of  $J_C[2]$  on the torsor  $X$  induces an automorphism of the diagram  $[X \rightarrow S]$ , so there is an injective morphism  $\rho_X: J_C[2] \rightarrow \underline{\text{Aut}}(S)$  of  $k$ -groups. Note however that the images of  $\rho$  and  $\rho_X$  in  $\text{PGL}_{2g}$  are not necessarily conjugate over  $k$ . As before, we may define  $\Theta_X := \alpha^{-1}(\rho_X(J_C[2]))$  and obtain an injective morphism of  $k$ -groups  $\rho_X: \Theta_X \rightarrow \text{GL}_{2g}$ .

We now summarize some results on theta groups from [CFO<sup>+</sup>08] as adapted to Jacobian varieties.

**Proposition A.2.6.** *Let  $C/k$  be a curve of genus  $g > 0$ . The mapping*

$$\{\text{Brauer-Severi diagrams } [X \rightarrow S]\} \rightarrow \{\text{theta groups } \Theta_X \text{ of } J_C[2]\}$$

*given by*

$$[X \rightarrow S] \mapsto \alpha^{-1}(\rho_X(J_C[2]))$$

*is a bijection. We have that  $[X_1 \rightarrow S_1]$  and  $[X_2 \rightarrow S_2]$  are isomorphic over  $k$  if and only if the corresponding theta groups are isomorphic over  $k$ . In particular, if  $C(k) \neq \emptyset$ , then for any  $\Theta$  a theta group of  $J_C[2]$  there is an injective homomorphism of  $k$ -groups  $\rho: \Theta \hookrightarrow \text{GL}_{2g}$ .*

*Proof.* See [CFO<sup>+</sup>08, Proposition 1.31], as well as the following discussion.  $\square$