Vinberg Representations and 2-Descent on Jacobians of Curves

by

Jiayu Liang

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2022

Doctoral Committee:

Professor Wei Ho, Chair
Professor Victoria Booth
Professor Yuan Liu
Professor Andrew Snowden

Jiayu Liang
liangji@umich.edu
ORCID iD: 0000-0002-5920-8522

To the future

ACKNOWLEDGEMENTS

I would like to thank Lena Ji, David Schwein, and Nawaz Sultani for helpful discussions about algebraic geometry and representation theory.

I would also like to thank my advisor, Wei Ho, for her effort and countless hours of time during the past six years, and for the detailed comments she made on this dissertation.

Lastly, I would like my doctoral committee, and especially Yuan Liu for providing thorough feedback on this dissertation.

TABLE OF CONTENTS

ABSTRACT

This dissertation applies Vinberg theory to the problem of constructing 2-descent maps on the Jacobians of hyperelliptic curves. In the first part, we construct, given a hyperelliptic curve C with certain marked points P and tangent vectors t, a smooth, complete surface S. Using the Picard group of S, we obtain a 2-graded simple adjoint Lie group (H, θ) of Dynkin type A_n, where n depends on the genus of C and the nature of the marked points. Assuming that H is split, we show that there exists an injective 2-descent map from the Jacobian of C into the orbit spaces of the local and global Vinberg representations associated to (H, θ). The approach is based on previous work of Thorne which addresses the cases where H is of Dynkin type E_6 or E_7.

In the second part, we construct, given a polynomial $f(x)$ of odd degree n and satisfying certain properties, an explicit map ψ from $J(C)$ into the orbit space of $G = \mathrm{SO}(V) \times \mathrm{SO}(V)$ acting on $\mathrm{End}(V)$, where C is the smooth, complete curve satisfying the equation $y^2 = f(x)$, and V is an orthogonal space of dimension n with maximal index of isotropy and discriminant 1. The pair (G, V) is exactly the degree 2 Vinberg representation of Dynkin type D_n. The map ψ extends a previous construction of Thorne which gives an explicit descent map for the degree 2 Vinberg representation of Dynkin type A_n.

In both parts, we work over an arbitrary field K of characteristic 0.

CHAPTER I
Introduction

I.1: Rational Points on Abelian Varieties and Descent

Let K be a number field and A an abelian variety defined over K. The group $A(K)$ of K-rational points has a theoretically simple structure.

Theorem I.1 (Mordell-Weil, [Wei29]). *The group $A(K)$ is a finitely-generated abelian group, i.e., there exists non-negative integers $r_0, r_1, ..., r_m$ and positive integers $n_1, ..., n_m$ such that*

$$A(K) \cong \mathbb{Z}^{r_0} \oplus \bigoplus_{i=1}^{m} (\mathbb{Z}/n_i\mathbb{Z})^{r_i}.$$

At the same time, there are no known effective proofs of this theorem, i.e., there exists no known method for obtaining the generators in general, and the question of even determining the r_j and n_k also remains unsolved. The size of the torsion part, i.e., the subgroup $A_{tors}(K) := \bigoplus_{i=1}^{m} (\mathbb{Z}/n_i\mathbb{Z})^{r_i}$, is conjectured to be controlled by the dimension of A and the degree of K over $\mathbb{Q}$.

Conjecture I.2 (Torsion Conjecture, see [CT13] for background). *Let d be the dimension of A and δ be the degree of K over $\mathbb{Q}$. There exists some $N = N(d, \delta)$ such that for all A, we have*

$$A_{tors}(K) \subset A[N](\bar{\mathbb{Q}}),$$

where the inclusion is of subgroups.

Understanding the rank is even more difficult. Even in the elliptic curve case $d = 1$, where the torsion part is well understood and computable, it is not known if the rank is even bounded, or which integers occur as the rank (see [RS02] for background on studying the rank of elliptic curves).

One approach to addressing these questions is *descent*, which generally refers to computing the group $A/pA(K)$ for some (usually) prime p. This computation is often easier than

computing the group $A(K)$ in general. By the Mordell-Weil Theorem, the group $A/pA(K)$ has the structure $A/pA(K) \cong (\mathbb{Z}/p\mathbb{Z})^{r_0+j}$, where j is determined by the structure of the torsion part. If we have a good understanding of the torsion part of A, which is plausible in many cases, we can determine the rank r_0 given the size of the group $A/pA(K)$.

We are often interested in understanding these questions in the case where A is the Jacobian variety $J(C)$ of some algebraic curve C defined over K. In this case, an understanding of the arithmetic of $J(C)$ leads to an understanding of arithmetic on C as well (see [Maz86] for a useful survey). This thesis provides approaches to 2-descent for certain curves C based on orbit parameterizations of representations arising in Vinberg theory; the following sections give explicit details.

I.2: Vinberg Theory and Curves

One way to study a variety X is to construct an injection $i : X \to G\backslash Y$, where $G\backslash Y$ is the orbit space, or set of orbits, of some algebraic group G acting on some variety Y. In many cases, $G\backslash Y$ will have the structure of an algebraic variety, and the map i will be an isomorphism of varieties. The variety Y will ideally be one with a thoroughly understood structure and even a coordinate system; for example, Y may be a linear representation of G. In this way, Y can be used to give an explicit parameterization of X. If we want to answer arithmetic questions about X, we will stipulate that all the objects are defined over K, and that the embedding is functorial with respect to base change.

The group actions we work with come from *Vinberg theory*. The setting is the following: let H be a simple, adjoint split Lie group defined over K with simply-laced Dynkin type. Let θ be a stable degree 2 involution of H, and $d\theta$ the induced involution on the Lie algebra $\mathfrak{h}$ of H. Define G to be the connected component of the subgroup H^θ, Y to be the connected component of the inverted set of points $h \in H$ such that $\theta(h) = h^{-1}$, and V to be the (-1)-eigenspace of $d\theta$, or equivalently the tangent space to Y at the identity. We can show that V is stable under conjugation by G, and this group action is called the *Vinberg representation associated to the grading* θ. One of the fundamental results of Vinberg theory states that the invariant ring $K[V]^G$ is free of finite rank; therefore the categorical quotient $B := V/\!/G = \mathrm{Spec}(K[V]^G)$ is an affine space. Further there is a (G-invariant) polynomial function Δ on V such that a vector $v \in V$ is stable (in the sense of geometric invariant theory) if any only if $\Delta(v)$ is non-zero.

The (non-unique) map $\pi : G\backslash V \to B$ given by sending each point v to the vector $(f_1(v), ..., f_n(v))$, where the f_j are free, homogenous generators of $K[V]^G$, is in general not bijective, even if K is algebraically closed. In particular, there can be distinct orbits on

which the f_j all take the same value. Let B^s be the set of points in B where Δ does not vanish, and V^s the set of points in V where Δ doesn't vanish. If K is algebraically closed (but crucially, not in general), the restricted map $G\backslash V^s \to B^s$ is a bijection; in other words, each orbit in V^s is completely determined by the values of the invariant polynomials.

A connection to curves was studied by Thorne in [Tho13]. Specifically, Thorne shows that there exists some subvariety $X \subset V$ such that the restricted map $\pi : X \to B$ is a flat family of reduced, affine curves. Further, if X^s is the pre-image in X of B^s, then $\pi : X^s \to B^s$ is a flat family of smooth affine curves. In addition, Thorne shows that there exists a natural $\mathbb{G}_m$ action on X and on B such that π is $\mathbb{G}_m$-equivariant, and that we may pick coordinates on X and B homogeneous with respect to this action such that each family $\pi : X \to B$ has a simple equation, given below in Table 1.1; with respect to these equations, each fiber X_b can naturally be seen as a curve in $\mathbb{A}^2$. We see directly from these equations that every X_b has the same number of marked K-points at infinity (although we note that some families have other marked points not at infinity), and that there exists a compactification $\pi : Y \to B$ such that (i) Y is a flat family of projective curves, each curve smooth over an open subset B^s of B, (ii) for $b \in B^s$, the fiber Y_b is the unique smooth completion of X_b, and (iii) the components of $Y\backslash X$ are disjoint, each isomorphic to B, and their number is the same as the number of marked points at infinity.

The preceding discussion is summarized in the following two tables. Our Table I.1, which gives the equation of the families, is largely identical to the table in [Tho13, Theorem 3.8] and to Table 1 in Jef Laga's thesis [Lag22]. The coordinates $(p_{d_1}, ..., p_{d_r})$ are homogeneous generators of the invariant ring $K[V]^G$, and in each case r is equal to the rank of H; this can be shown using Vinberg theory. In addition, the coordinates $(p_{d_1}, ..., p_{d_{r-1}}, x, y)$ are $\mathbb{G}_m$ homogeneous coordinates on X. The marked points correspond to special points on the smooth curves X_b; we hope our descriptions will be understandable given the type of curve. Explicit descriptions of the Vinberg representations can be found in Table 2 in [Lag22].

Dynkin Type	Genus	Equation of Family	Marked Points at Infinity
A_{2g}	g	$y^2 = x^{2g+1} + p_2x^{2g-1} + ... + p_{2g+1}$	1 (Weier.)
A_{2g+1}	g	$y^2 = x^{2g+2} + p_2x^{2g} + ... + p_{2g+2}$	2 (same fiber)
D_{2g+1}	g	$y(xy + p_{2g+1}) = x^{2g} + p_2x^{2g-1} + ... + p_{4g}$	2 (both Weier.)
D_{2g+2}	g	$y(xy + p_{2g+2}) = x^{2g+1} + p_2x^{2g} + ... + p_{4g+2}$	3 (1 Weier., 2 same fiber)
E_6	3	$y^3 = x^4 + (p_2x^2 + p_5x + p_8)y + (p_6x^2 + p_9x + p_{12})$	1 (hyperflex)
E_7	3	$y^3 = x^3y + p_{10}x^2 + x(p_2y^2 + p_8y + p_{14}) + p_6y^2 + p_{12}y + p_{18}$	1 (flex + pt. on its tan.)
E_8	4	$y^3 = x^5 + y(p_2x^3 + p_8x^2 + p_{14}x + p_{20}) + p_{12}x^3 + p_{18}x^2 + p_{24}x + p_{30}$	1 (simply-ram. pt.)

Table I.1: Equations of families

For a given b in B^s, let V_b denote the set of vectors in V which map to b under the map π. Over some separable closure of K, the set V_b consists of a single G orbit. The problem, as stated in [Tho13, Conjecture 4.16], is the following.

Problem I.3. *Construct a map*

$$i_b : J(Y_b)(K)/2J(Y_b)(K) \to G\backslash V_b(K),$$

where $G\backslash V_b(K)$ is the set of all orbits which map to b. We want the construction to be functorial with respect to base change, and to be "uniform" over b. Given the latter condition, we can hope to study the images of the descent maps i_b inside the total orbit space $G\backslash V$ in order to understand something (for example, the size of the Selmer groups) about how the Jacobians $J(Y_b)$ vary across the family.

In this thesis, we provide two different approaches to addressing this problem. To put these approaches into context, we first review some previous work that has been done on Problem I.3.

I.3: Previous Work

One set of approaches to Problem I.3 in the non-exceptional case uses the geometry of the hyperelliptic curves involved, notably their connection to pencils of quadric surfaces, to construct the descent maps i_b. This was carried out by Bhargava-Gross in [BG13] for the case where H is of Dynkin type A_{2g}, by Shankar-Wang in [SW18] for the A_{2g+1} case, and by Shankar in [Sha19] for the case where H is of Dynkin type D_{2g+1}. In all these works, the image of the descent maps i_b is sufficiently understood to prove facts about the distribution of the sizes of the Selmer groups of the Jacobians.

In addition, Thorne in [Tho14] provides an alternate construction of a 2-descent map in the case A_{2g} using the *Mumford representation* of a line bundle on a hyperelliptic curve. He shows that the map he constructs is equivalent to the one constructed in [BG13]. An advantage of the approach in [Tho14] is that given a genus g hyperelliptic curve C and a degree 0 line bundle $\mathcal{L}$ on C, one can actually write down a matrix corresponding to the image of $\mathcal{L}$ under the descent map.

In the exceptional cases E_6 and E_7, Thorne in [Tho16] approaches Problem I.3 by associating to the corresponding curves C_b a complete surface S_b. He shows that the Picard lattice S contains a lattice Λ of the desired Dynkin type. Further he shows that given some additional data on the curve, we can recover the split Lie group H as well as obtain a descent map

$$i_b : J(C_b)/2J(C_b)(K) \to G\backslash V_b(K).$$

This construction is interesting because it is a partial converse to the scenario in the previous section; given the curve and some geometric data, we obtain a 2-graded split Lie group H.

In addition, the surfaces S_b are completions of the so-called *Slodowy surfaces* of type E_6 and E_7, thus partially completing the circle of ideas which inspired [Tho13] (see [Tho13, Section 1]). Further, Thorne also constructs descent maps

$$i_b : J(C_b)/2J(C_b)(K) \to G\backslash Y_b(K),$$

where Y is a non-linear variety on which G acts; this is a "global" analogue of the "local" Vinberg representation V. Unlike the works in the previous paragraph, the article [Tho16] does not study use the descent maps constructed to study the Selmer groups of the Jacobians. Kulkarni in [Kul17] has used the approach discussed in this paragraph to construct 2-descent maps in the E_8 case.

Recently, Jef Laga in his thesis [Lag22] has developed an approach which addresses all the simply-laced Dynkin types uniformly. To explain his approach, we first recall a theorem of Galois cohomology (see [BG14, Proposition 1] for proof; the statement there is given when X is a vector space, but the theorem applies equally well when X is a variety).

Theorem I.4. *Let G be an algebraic group and V an algebraic variety, both defined over some number field K. Given $x \in X$, let G_x be the stabilizer group of x, and let V_x be the points of V which become G-equivalent to x over $\bar{\mathbb{Q}}$. There is a bijection*

$$\phi : G\backslash V_x(K) \to \ker(\gamma : H^1(K, G_x) \to H^1(K, G)).$$

The bijection ϕ sends $x \in V_x$ to the trivial cocycle in $H^1(K, G_x)$.

For each $b \in B$, we can choose a distinguished element in the pre-image V_b, namely the point κ_b given by the intersection of V_b and the so-called *Kostant section* $\kappa \subset V$. The connection to Jacobians arises due to the fact, proved by Thorne, that there exists an isomorphism $G_{\kappa_b} \to J(Y_b)[2]$, and due to existence of the map

$$\psi : J(Y_b)/2J(Y_b)(K) \to H^1(K, J(Y_b)[2])$$

obtained from a certain long-exact sequence on Galois cohomology. Thus if one can show that the image of ψ lies in the kernel of the map γ, we will have a 2-descent map $i_b : J(Y_b)/2J(Y_b)(K) \to G\backslash V_{\kappa_b}(K)$. Laga proves this by studying a compactification of the relative Jacobian of the family $Y \to B$. He is able to use his descent map to prove bounds on the size of the 2-Selmer groups of the Jacobians in the family.

I.4: Statement and Outline of Results

In Chapter II, we survey some of the necessary background on Lie theory and Vinberg theory. In Chapter III, we generalize the approach of [Tho16] to the case where the group H is of type A_n. Specifically, for each n, we define a category $\mathcal{S}_n$ of equivalence classes of curves C with marked points P and tangent vectors t at P. The category $\mathcal{S}_n$ contains a subcategory (to be defined in Chapter 3) S_n^0. We prove the following theorem.

Theorem I.5. *For every $v = [(C, P, t)] \in \mathcal{S}_n(K)$, we define*

1. *A complete surface S defined over K equipped with an involution ι such that C is embedded into S as the fixed locus of ι,*
2. *a simply-laced root sublattice Λ of $\mathrm{Pic}(S)(K^s)$ defined over K and of type A_n,*
3. *and for each class $A \in J(C)(K)$, a central extension $\tilde{V}_A$ of $V = \Lambda/2\Lambda$.*

Given this data, we obtain a simple adjoint group H with Dynkin type A_n defined over K. Assuming that H is split, we also obtain

1. *a stable involution θ on H defined over K,*
2. *a split maximal torus T on which θ acts by inversion,*
3. *marked points $\kappa_C \in V$ and $\mu_C \in Y$, where V and Y are the local and global Vinberg representations of the 2-graded Lie group H,*
4. *and for each $A \in J(C)$, an element $i_C(A)$ in $V_{\kappa_C}(K)$.*

Then the assignment $A \to i_C(A)$ descends to an injection.

$$i_C : J(C)/2J(C)(K) \to G\backslash V_{\kappa_C}(K).$$

Further, if v is in $\mathcal{S}_n^0(K)$, there exists a similar injection

$$I_C : J(C)/2J(C)(K) \to G\backslash Y_{\mu_C}(K).$$

Our theorem is an analog of [Tho16, Theorem 3.6], which addresses the cases when H is of types E_6 or E_7.

In Chapter IV, we extend the approach of [Tho14] to the case where H is type D_n, n odd. More precisely, we prove the following theorem.

Theorem I.6. *For $n \geq 3$ odd and a hyperelliptic curve C of genus $\frac{n-1}{2}$ given by an equation of the form,*

$$y^2 = x^{n+1} + ... + c^2,$$

where c is some constant in K, there is a canonical injection

$$\psi : J(C)/2J(C)(K) \to G\backslash \mathrm{End}(V),$$

where V is an orthogonal space of dimension n, maximal index of isotropy, and discriminant 1 and $G = \mathrm{SO}(V) \times \mathrm{SO}(V)$ acts on $\mathrm{End}(V)$ by $(a, b) \cdot T = aTb^*$.

This theorem is an extension of [Tho14, Theorem 4.6], which is used as an intermediate step in constructing the injection ψ.

As mentioned in the previous section, the articles [Tho16] and [Tho14] contain distinct approaches to Problem I.3 which are each geometrically interesting; we hope that our work will help generalize these approaches uniformly to all simply-laced Dynkin types.

CHAPTER II
Background

In this chapter, we describe background information on Vinberg theory that forms the basic technical material used in this thesis. Vinberg theory studies representations arising from Lie algebras with a graded structure; these representations can be seen as generalizations of the adjoint representation of a Lie group on its Lie algebra (this can be seen as the case of a degree 1 grading). We begin by recalling some facts about the adjoint representation; these give some intuition about the basic properties of Vinberg representations. Next, we state some basic definitions related to graded Lie algebras and facts about Vinberg representations. Finally, we end the chapter by describing the connections between Vinberg theory and the arithmetic of curves.

Throughout this chapter, we fix a ground field K of characteristic 0, with a separable closure K^s. We assume knowledge of Lie algebras and their representations, as contained in [Hum72], with the caveat that this source does not cover the arithmetic aspects of the theory. We will work with split Lie groups, which the unfamiliar reader may assume behave similarly to Lie groups over algebraically closed fields.

II.1: The Adjoint Representation

For the rest of this chapter, we assume that G is a split, connected, reductive Lie group defined over K with Lie algebra $\mathfrak{g}$. The results in this section are well-known and given without proof.

Definition II.1. *The adjoint representation is the representation of the group G acting on the vector space $\mathfrak{g}$ by conjugation.*

As with any other representation, we naturally want to understand the invariant ring of the adjoint representation. To do so, we may restrict to a linear representation of a finite group on a simple subspace of $\mathfrak{g}$.

Definition II.2. *Let $\mathfrak{c} \subset \mathfrak{g}$ be a split Cartan subalgebra. We define $N_{\mathfrak{c}} \subset G$ to be the normalizer of $\mathfrak{c}$ and $Z_{\mathfrak{c}} \subset G$ to be the stabilizer of of $\mathfrak{c}$. The Weyl group $W_{\mathfrak{c}}$ is the quotient group $N_{\mathfrak{c}}/Z_{\mathfrak{c}}$.*

The group $W_{\mathfrak{c}}$ acts faithfully on $\mathfrak{c}$ by conjugation. Suppose that $f \in K[\mathfrak{g}]^G$ is a G-invariant polynomial. Then the restriction of f to $\mathfrak{c}$ is a W-invariant polynomial, so that we have a restriction map $r : K[\mathfrak{g}]^G \to K[\mathfrak{c}]^W$.

Theorem II.3 (Chevalley Restriction Theorem)**.** *The restriction map $r : K[\mathfrak{g}]^G \to K[\mathfrak{c}]^{W_{\mathfrak{c}}}$ is an isomorphism.*

Proof. See [Hum72, p.127] for a proof. □

Since the Weyl group $W_{\mathfrak{c}}$ is a finite reflection group, the ring $K[\mathfrak{c}]^{W_{\mathfrak{c}}}$ is a free polynomial ring with $\dim \mathfrak{c} = \operatorname{rk} G$ homogeneous generators (see [Che55] for a proof of this fact). The Chevalley restriction theorem thus says that $K[\mathfrak{g}]^G$ is freely generated by homogeneous generators, and in many cases, we can use the theorem to help us compute these generators.

Example II.4. *Let $G = \mathfrak{sl}_2(K)$. Then $\mathfrak{g} = \mathfrak{sl}_2(K)$ is the space of traceless, 2-by-2 matrices, and we may choose $\mathfrak{c}$ to be space of matrices of the form $\left[\begin{smallmatrix} \lambda & 0 \\ 0 & -\lambda \end{smallmatrix}\right]$. By direct computation, we can see that $N_{\mathfrak{c}}$ consists of the subgroup of diagonal and off-diagonal matrices of determinant 1, and $Z_{\mathfrak{c}}$ consists of the the subgroup of diagonal matrices of determinant 1. Therefore $W_{\mathfrak{c}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ and acts on $\mathfrak{c}$ by swapping λ and $-\lambda$. Identifying $K[\mathfrak{c}]$ with $K[\lambda]$, $W_{\mathfrak{c}}$ acts $K[\lambda]$ by sending $f(\lambda)$ to $f(-\lambda)$, so that $K[\lambda]^{W_{\mathfrak{c}}}$ is generated by the restriction of the determinant function on $K[\mathfrak{g}]^G$. By the Chevalley restriction theorem, the determinant function generates $K[\mathfrak{g}]^G$.*

II.2: Vinberg Representations

The material in this section can be found in [Pan05], and the statements of most results are given here without proof.

II.2.1: Basic Notions

Definition II.5. *An m-graded Lie algebra is a pair $(\mathfrak{g}, \theta)$ where $\mathfrak{g}$ is the split, semisimple Lie algebra of some split, adjoint simple Lie group G over K and θ is an automorphism of $\mathfrak{g}$ of pure degree m. We usually assume θ is clear by context, and also assume that K contains a primitive m-th root of unity.*

Example II.6. *Let $\mathfrak{g} = \mathfrak{sl}_2(K)$ be the Lie algebra of traceless 2-by-2 matrices. For a matrix $x \in g$, let x^* denote reflection over the antidiagonal. Let $\theta : \mathfrak{g} \to \mathfrak{g}$ be defined by $\theta(x) = -x^*$. Then $(\mathfrak{g}, \theta)$ is a 2-graded Lie algebra.*

After defining an m-graded structure on $\mathfrak{g}$, we often simply write $\mathfrak{g}$ instead of $(\mathfrak{g}, \theta)$ to refer to the graded Lie algebra.

Lemma II.7. *Suppose that K contains a primitive m-th root of unity ζ. Given an m-graded Lie algebra $\mathfrak{g}$, define*

$$\mathfrak{g}_i := \{x \in \mathfrak{g} \mid \theta(x) = \zeta^i x\}.$$

We have the direct sum decomposition

$$\mathfrak{g} = \oplus_{i=0}^{m-1} \mathfrak{g}_i.$$

Proof. Since θ is a linear transformation, $\mathfrak{g}$ is the direct sum of the generalized eigenspaces of θ. Since $\theta^m = I$, we can further deduce that $\mathfrak{g}$ is the sum of the eigenspaces of θ. □

Lemma II.8. *For any $1 \leq i, j \leq m-1$, we have*

$$[\mathfrak{g}_i, \mathfrak{g}_j] \subset \mathfrak{g}_{i+j}.$$

Proof. If x and y satisfy $\theta(x) = \zeta^i x$ and $\theta(y) = \zeta^j y$, then we have

$$\theta[x, y] = [\theta(x), \theta(y)] = [\zeta^i x, \zeta^j y] = \zeta^{i+j}[x, y],$$

which finishes the proof. □

Example II.9. *The only primitive second root of unity is -1. In the preceding example, we have that $\mathfrak{g}_0$ consists of the matrices such that $x = -x^*$ and $\mathfrak{g}_1$ consists of the matrices such that $x = x^*$. In this case, the lemma restates the familiar fact that every (traceless) matrix an be written as the sum of a (traceless) skew-adjoint matrix and a (traceless) self-adjoint matrix.*

Definition II.10. *Let $(\mathfrak{g}, \theta)$ be an m-graded Lie algebra. Let G_0 be the connected component of the fixed subgroup G^θ (observe that $\mathfrak{g}_0$ is the Lie algebra of G_0 Since $[\mathfrak{g}_0, \mathfrak{g}_1] \subset \mathfrak{g}_1$, the adjoint action of G_0 is a vector space automorphism of $\mathfrak{g}_1$. The Vinberg representation associated to $(\mathfrak{g}, \theta)$ is the representation* $\mathrm{Ad} : G_0 \to \mathrm{Aut}(\mathfrak{g}_1)$.

Example II.11. *In the $\mathfrak{g} = \mathfrak{sl}_2(K)$ example, we have that G_0 is the space $\mathrm{SO}_2(K)$ of 2x2 matrices X of determinant 1 such that $XX^* = I$ and $\mathfrak{g}_1$ is the space $\mathfrak{so}_2(K)$ of traceless*

self-adjoint transformations. The Vinberg representation is thus $\mathrm{SO}_2(K)$ *acting on* $\mathfrak{so}_2(K)$ *by conjugation.*

Explicitly, a general element of G_0 *can be written* $X = \left(\begin{smallmatrix} a & 0 \\ 0 & \frac{1}{a} \end{smallmatrix}\right)$ *with* $a \neq 0$ *and a general element of* $\mathfrak{g}_1$ *can be written* $x = \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$*. The action of* X *on* x *sends* x *to* $\left(\begin{smallmatrix} 0 & a^2 \cdot b \\ \frac{c}{a^2} & 0 \end{smallmatrix}\right)$.

II.2.2: Stable Involutions

In order to obtain representations whose properties (e.g. invariant ring, sections) we can understand, we restrict ourselves to a class of gradings which satisfy certain stability conditions. In order to discuss these conditions, we first recall some terminology.

Definition II.12. *For* $x \in \mathfrak{g}$*, define the centralizer of* x *in* $\mathfrak{g}$*, which we denote by* $Z_{\mathfrak{g}}(x)$*, to be the subalgebra of all* $y \in \mathfrak{g}$ *such that* $[x, y] = 0$.

It can be shown that $\dim Z_{\mathfrak{g}}$ *is at least* $\operatorname{rk} \mathfrak{g}$*. If* $\dim Z_{\mathfrak{g}}(x) = \operatorname{rk} \mathfrak{g}$*, we say that* x *is regular.*

If $\dim Z_{\mathfrak{g}}(x) = \operatorname{rk} \mathfrak{g} + 2$*, we say that* x *is subregular*

If $\operatorname{ad}(x)^m = 0$ *as a linear transformation on* $\mathfrak{g}$ *for some* m*,* x *is nilpotent.*

If $\operatorname{ad}(x)$ *is diagonalizable as a linear transformation on* $\mathfrak{g}$*, then* x *is semisimple*

Example II.13. *In the* $\mathfrak{g} = \mathfrak{sl}_2(K)$ *example, the element* 0 *is not regular, since all of* $\mathfrak{g}$ *is in the centralizer of* 0*, but it is nilpotent and semisimple.*

The vector $x_0 = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$ *in* $\mathfrak{g}_1$ *is regular; its centralizer consists of all the multiples of* x_0 *and is thus one-dimensional. It is also nilpotent, since* $\operatorname{ad}(x_0)^2 = 0$*. We can check directly by choosing a basis of* $\mathfrak{g}$ *that* $\operatorname{ad}(x_0)$ *is not diagonalizable, so that* x_0 *is not semisimple.*

Similarly, we can see that the vector $x_1 = \left[\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right]$ *in* $\mathfrak{g}_1$ *is regular and semisimple, but not nilpotent.*

Lemma II.14 (Graded Jordan Decomposition)**.** *Let* $x = x_s + x_n$ *be the Jordan decomposition, i.e.,* x_s *is semisimple and* x_n *is nilpotent. If* x *is in* $\mathfrak{g}_i$ *for some* i*, then* x_s *and* x_n *are in* $\mathfrak{g}_i$ *as well.*

Proof. See the discussion in Section 1.4 of [Vin76]. □

Example II.15. *In the* $\mathfrak{g} = \mathfrak{sl}_2(K)$ *example, if* x *is in* $\mathfrak{g}_0$ *or* $\mathfrak{g}_1$*, then* x *is nilpotent if it is not semisimple, so the preceding lemma holds (note that this is a very special case, and in general the elements of* $\mathfrak{g}_i$ *are neither nilpotent nor semisimple.*

Definition II.16. *Let* $(\mathfrak{g}, \theta)$ *be an* m*-graded Lie algebra, and suppose that* K *contains a primitive* m*-th root of unity* ζ*. We say that a vector* $x \in \mathfrak{g}_1$ *is stable if the orbit* $G_0(K^s) \cdot x$ *is closed in* $\mathfrak{g}_1(K^s)$ *and the stabilizer subgroup* $Z_{G_0(K^s)}(x)$ *of* x *in* G_0 *is finite. (Note that this*

follows the general definition of a stable element of a representation of an algebraic group on a variety.)

Example II.17. *In the $\mathfrak{g} = \mathfrak{sl}_2(K)$ example, the vector 0 in $\mathfrak{g}_1$ is not stable since every element of G_0 stabilizes 0, so the stabilizer subgroup is infinite.*

The vector $x_0 = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ in $\mathfrak{g}_1$ is is not stable. A group element $X = \left(\begin{smallmatrix} a & 0 \\ 0 & \frac{1}{a} \end{smallmatrix}\right)$ acts on x_0 by conjugation and sends x_0 to $\left(\begin{smallmatrix} 0 & a^2 \\ 0 & 0 \end{smallmatrix}\right)$, with $a \neq 0$. Therefore the orbit $G_0 \cdot x_0$ does not contain 0 but does contain 0 in its closure, so it is not closed.

The vector $x_1 = \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right)$ in $\mathfrak{g}_1$ is stable. A group element $X = \left(\begin{smallmatrix} a & 0 \\ 0 & \frac{1}{a} \end{smallmatrix}\right)$ sends x_1 to $\left(\begin{smallmatrix} 0 & a^2 \\ \frac{2}{a^2} & 0 \end{smallmatrix}\right)$ with $a \neq 0$. Therefore the stabilizer group $Z_{G_0}(x_1)$ has exactly two elements, corresponding to $a = \pm 1$. In addition, the orbit $G_0 \cdot x_1$ is closed in $\mathfrak{g}_1$; it is the subvariety $bc = 2$.

Of the three vectors, x_1 is the only stable vector. Recall that x_1 is also the only vector which is both regular and semisimple; we will see later that this is no coincidence.

Definition II.18. *The automorphism θ is called stable if $\mathfrak{g}_1$ contains stable elements. We are specifically interested in stable involutions, i.e., degree 2 stable automorphisms.*

Example II.19. *As we say in the previous example, the involution $\theta(x) = -x^*$ on $\mathfrak{sl}_2(K)$ is stable.*

Suppose that G is a split adjoint group of simply-laced Dynkin type. By [Tho13, Corollary 2.15] and the discussion preceding it, there is a unique class of stable involutions with nice properties.

Lemma II.20 (Lemma 2.7 of [Tho13] and Proposition 1.9 of [Tho16])**.** *If G is a split adjoint group of simply-laced Dynkin type, there is a unique $G(K)$-conjugacy class of stable involutions θ on G satisfying the following:*

1. $\mathrm{tr}(d\theta : \mathfrak{g} \to \mathfrak{g}) = -\mathrm{rk}(G)$,
2. *G_0 is split, and*
3. *$\mathfrak{g}_1$ contains a regular nilpotent element.*

Further, the first two conditions imply the third, and the first and third conditions imply the second.

Lemma II.21. *If G is a split adjoint group of simply-laced Dynkin type, there is a unique $G(K)$-conjugacy class of stable involutions θ on G satisfying the following:*

1. $\mathrm{tr}(d\theta : \mathfrak{g} \to \mathfrak{g}) = -\mathrm{rk}(G)$,

2. *G_0 is split, and*

3. *$\mathfrak{g}_1$ contains a regular semisimple element.*

Further, the first two conditions imply the third, and the first and third conditions imply the second.

Proof. This follows from the preceding lemma and the fact that when θ is an involution, the presence of a regular semisimple element in $\mathfrak{g}_1$ implies and is implied by the presence of a regular nilpotent elment (see the remark about the equivlance of S-regularity and N-regularity in [Pan05, p.656]). □

For the rest of the chapter, we assume that G and θ satisfy the properties listed in the previous lemma.

We have the following helpful characterization of a stable vector.

Lemma II.22 (Theorem 1.10 of [Tho16])**.** *There exists a G_0-invariant polynomial Δ such that for all x in $\mathfrak{g}_1$, the following are equivalent:*

1. *x is regular semisimple,*

2. *x is stable,*

3. *$\Delta(x)$ is non-zero.*

In addition, it is possible to compute the dimensions of the given spaces $\mathfrak{g}_i$

Definition II.23. *For a graded, semisimple Lie algebra $\mathfrak{g}$ of rank l, the exponents $d_1, ..., d_l$ are the degrees of the fundamental invariants of $\mathfrak{g}$, ordered to be non-decreasing. Given a natural number m, we define for any integer j*

$$k_j = \#\{r \mid d_r - 1 \equiv j \mod m\}.$$

Lemma II.24. *We have the equality*

$$\dim \mathfrak{g}_1 - \dim \mathfrak{g}_0 = k_1 - k_0.$$

Proof. See Theorem 3.3 of [Pan05]. □

Using the preceding lemma and the fact that $\dim \mathfrak{g}_0 + \dim \mathfrak{g}_1 = \dim \mathfrak{g}$, we can compute the dimensions of all the $\mathfrak{g}_i$.

Example II.25. *The $\mathfrak{g} = \mathfrak{sl}_2(K)$ example, our involution θ is in fact of the type given above. In that case, we have $k_0 = 0$ and $k_1 = 1$. Applying the preceding lemma, we get the equation*

$$\dim \mathfrak{g}_1 - \dim \mathfrak{g}_0 = k_1 - k_0 = 1.$$

In addition, we have the equation

$$\dim \mathfrak{g}_1 + \dim \mathfrak{g}_0 = \dim \mathfrak{g} = 3.$$

Solving these two equations, we obtain

$$\dim \mathfrak{g}_0 = 1, \dim \mathfrak{g}_1 = 2,$$

which we can verify directly.

Next, we move on to discussing the invariant theory of the Vinberg representation induced by θ. As in the case of the adjoint representation, this theory is simplified by passing to a subspace of $\mathfrak{g}_1$.

Definition II.26. *A Cartan subspace is a maximal abelian, semisimple subspace of $\mathfrak{g}_1$.*

Example II.27. *In the $\mathfrak{g} = \mathfrak{sl}_2(K)$ example, the subspace $\left[\begin{smallmatrix} 0 & b \\ b & 0 \end{smallmatrix}\right]$ of $\mathfrak{g}_1$ is a Cartan subspace. We can compute directly that this subspace is abelian and semisimple and no vector outside this subspace commutes with it.*

Definition II.28. *Suppose that $\mathfrak{c}$ a Cartan subspace. Define $N_{G_0}(\mathfrak{c})$ to be the subgroup of G_0 which normalizes $\mathfrak{c}$ and $Z_{G_0}(\mathfrak{c})$ to be the subgroup of G_0 which stabilizes $\mathfrak{c}$. Define the little Weyl group of $\mathfrak{c}$ to be the group*

$$W(\mathfrak{c}, \theta) := N_{G_0}(\mathfrak{c})/Z_{G_0}(\mathfrak{c}).$$

Example II.29. *In the $\mathfrak{g} = \mathfrak{sl}_2(K)$ example, we can see directly by our previous computations that the normalizer subgroup $N_{G_0}(\mathfrak{c})$ of our chosen Cartan subpsace $\mathfrak{c}$, which is given by matrices of the form $\left[\begin{smallmatrix} 0 & b \\ b & 0 \end{smallmatrix}\right]$, is the group $\left[\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right]$. Further, we can check directly that this entire group acts trivially on $\mathfrak{c}$. Therefore $N_{G_0}(\mathfrak{c}) = Z_{G_0}(\mathfrak{c})$, and the Weyl group $W(\mathfrak{c}, \theta)$ is trivial.*

Theorem II.30 (Little Chevalley Theorem, Theorem 7 of [Vin76])**.** *If $K = K^s$, the restriction map $r : K[\mathfrak{g}_1]^{G_0} \to K[\mathfrak{c}]^{W(\mathfrak{c},\theta)}$ is an isomorphism.*

Note that the "Little" Chevalley Theorem is not true in general if K is not algebraically closed.

As before, $W(\mathfrak{c}, \theta)$ is a finite reflection group, so that $K[\mathfrak{c}]^{W(\mathfrak{c},\theta)}$ is free with k_1 homogeneous generators. In practice, if we know the invariants $K[\mathfrak{g}]^G$ of the adjoint representation, we can often compute the invariants $K[\mathfrak{g}_1]^{G_0}$ of the Vinberg representation. To do this, we need introduce some terminology.

Definition II.31. *Let $(\mathfrak{g}, \theta)$ be an m-graded Lie algebra. Let $F_1, ..., F_l$ be homogeneous, algebraically independent generators of $K[\mathfrak{g}]^G$. Recall*

1. *the integers $d_i = \deg(F_i)$ are the degrees of $\mathfrak{g}$, and*
2. *the integers $m_i = d_i - 1$ are the exponents of $\mathfrak{g}$.*

The F_i may be chosen so that $\theta(F_i) = \epsilon_i F_i$ for some m-th root of unity ϵ_i. The ϵ_i are called the factors of θ.

Theorem II.32 (Theorem 3.5 of [Pan05])**.** *There is a restriction homomorphism*

$$s : K[\mathfrak{g}]^G \to K[\mathfrak{g}_1]^{G_0}.$$

The map s is onto, and $K[\mathfrak{g}_1]^{G_0}$ is freely generated by the restriction of the homogeneous generators F_j of $K[\mathfrak{g}]^G$ satisfying $\zeta^{d_j}\epsilon_j = 1$.

Example II.33. *We use the preceding material to calculate the invariant ring of the Vinberg representation in our $\mathfrak{g} = \mathfrak{sl}_2(K)$ example. We have previously seen that we may choose $K[\mathfrak{g}]^G$ to be generated by the determinant function F_1, and thus θ acts trivially on F_1, so that $d_1 = 2$ and $\epsilon_1 = 1$. Since the degree is 2, we have $\zeta = -1$, so that $\zeta^{d_1}\epsilon_1 = (-1)^2 \cdot 1 = 1$. Therefore $K[\mathfrak{g}_1]^{G_0}$ is freely generated by the restriction of the determinant function.*

II.3: Connections to Curves

In this section, we describe associate to each stable 2-grading of a split, simple adjoint group of simply-laced Dynkin type a family of curves. The material in this section comes from [Tho13], to which we refer for proofs. Before proceeding, we recall that Lemma II.20 states our choice of grading is unique up to a $G(K)$-change of coordinates.

In order to explain how the families arise, we will define a refinement of an $\mathfrak{sl}_2$-triple.

Definition II.34. *An $\mathfrak{sl}_2$-triple (e, h, f) is called θ-adjusted if e is in $\mathfrak{g}_1$, h is in $\mathfrak{g}_0$, and f is in $\mathfrak{g}_{-1}$. It is called (sub)regular/nilpotent if e is (sub)regular/nilpotent.*

Lemma II.35 (Weighted Jacobson-Morozov)**.** *Every nilpotent e in $\mathfrak{g}_1$ is contained in some θ-adjusted $\mathfrak{sl}_2$-triple.*

Proof. See Lemma 2.17 of [Tho13]. □

Next, we will define the Kostant section, as well as our families of curves. It is natural to introduce the Kostant section here, since the construction is similar to that of the families of curves; the Kostant section gives a natural choice of K-orbit among each stable K^s-orbit. Our construction of the Kostant section as well as of our families involves the choice of some (sub)regular element; the next lemma describes how well this choice is determined.

Lemma II.36 (Lemma 2.17 and Proposition 2.29 of [Tho13])**.** *Given θ, there is a unique $G^\theta(K)$-conjugacy class of regular nilpotent elements E in $\mathfrak{g}_1$ (recall that G_0 is the connected component of G^θ).*

1. *If G is of type D_r or E_r, there is a unique $G^\theta(K)$-conjugacy class of subregular nilpotent elements in $\mathfrak{g}_1$.*
2. *If G is of type A_{2r}, the $G_0(K)$-conjugacy classes of subregular nilpotent elements in $\mathfrak{g}_1$ are in bijection with $K^\times/(K^\times)^2$.*
3. *If G is of type A_{2r+1}, there is a unique $G_0(K)$-conjugacy class of subregular nilpotent elements in $\mathfrak{g}_1$.*

Further, given E, a θ-adjusted $\mathfrak{sl}_2$-triple containing E is determined up to $Z_{G_0}(E)(K)$-conjugacy.

Definition II.37. *For a graded Lie algebra $\mathfrak{g}$, we define*

$$\mathfrak{g}_1//G_0 := \mathrm{Spec}(K[\mathfrak{g}_1]^{G_0}).$$

Definition II.38. *An affine subspace $\kappa \subset \mathfrak{g}_1$ is called a Kostant section if*

1. *the restriction of $\pi : \mathfrak{g}_1 \to \mathfrak{g}_1//G_0$ to κ induces an isomorphism of κ and $\mathfrak{g}_1//G_0$ and*
2. *over $K = K^s$, κ meets every regular semisimple orbit exactly once.*

Lemma II.39 (Lemma 3.5 of [Tho13])**.** *Let (e, h, f) be a θ-adjusted, regular nilpotent $\mathfrak{sl}_2(K)$-triple. Let $Z_{\mathfrak{g}}(f)_1$ denote the intersection of the centralizer of f in $\mathfrak{g}$ with $\mathfrak{g}_1$. Then $\kappa = e + Z_{\mathfrak{g}}(f)_1$ is a Kostant section.*

Theorem II.40 (Theorem 3.8, Lemma 4.9, and Corollary 4.12 of [Tho13])**.** *Let (e, h, f) be a θ-adjusted, subregular nilpotent $\mathfrak{sl}_2(K)$-triple. Then $X = e + Z_{\mathfrak{g}}(f)_1$ satisfies the following:*

1. *the map* $\pi : X \to \mathfrak{g}_1 /\!/ G_0$ *is a flat family of reduced, affine curves,*

2. *the fibers over the stable locus* $(\mathfrak{g}_1 /\!/ G_0)^s$ *are smooth curves, and*

3. $X_0 = \pi^{-1}(0) \subset X$ *has a simple singularity of the same Dynkin type as* G*.*

Further, there exists a compactification $\pi : Y \to \mathfrak{g}_1 /\!/ G_0$ *satsifying the following:*

1. Y *is a flat family of projective curves,*

2. *the fibers over the stable locus* $(\mathfrak{g}_1 /\!/ G_0)^s$ *are smooth curves,*

3. *the components of* Y/X *are disjoint, each isomorphic to* $B = \mathfrak{g}_1 /\!/ G_0$*, and*

4. *for each* $b \in B^s$ *and* x_b *in the fiber over* b*, there is a canonical isomorphism*

$$(G_0)_{x_b} \to J(Y_b)[2].$$

We recall an explicit description of the families of curves given a choice of coordinates is given in Table I.1 of our Introduction.

We note that there is a global, non-linear analog of the representations described in this chapter, namely the action of the group G_0 on the connected component Y of the subvariety of elements g in G such that $\theta(g) = g^{-1}$. These "global" Vinberg representations are studied in [Ric82], but our impression is that as of this writing, their properties are not as well-understood as those of the "local" Vinberg representations we just described. A helpful task would be to prove results for the global representations analogous to those we have stated for the local representations. The global Vinberg representations appear in our Chapter III, although we use little more than their definition.

CHAPTER III
Surfaces and the Orbit Problem for A_n

III.1: Introduction

Let K be a field of characteristic 0 with separable closure K^s. Suppose that C is a hyperelliptic curve of genus g with a marked points and tangent vectors. Our goal is to construct functorially, given certain types of data (C, P, t), where P is a point on C and t a tangent vector at P, a split, simple adjoint Lie group H of type A_n equipped with a stable involution θ such that

1. if $G = H_0$ acting on $V = \mathfrak{h}_1$ is the local Vinberg representation associated to (H, θ), if $B = V/\!/G := \mathrm{Spec}(K[V]^G)$, and if $\pi : X \to B$ is the family of curves in Theorem II.40, then C is isomorphic to X_b for some $b \in B$, and the marked points on C correspond to the points at infinity of X_b, and

2. if Y is the global Vinberg representation associated to (H, θ), then there are injections $\phi : J(C)/2J(C)(K) \to G\backslash V(K)$ and $\Phi : J(C)/2J(C)(K) \to G\backslash Y(K)$.

Recall that (2) is the 2-*Descent Problem*. The goal of this chapter is to prove Theorem I.5, which provides an approach to this problem when H is of type A_n.

Proposition III.1 (see [BG14], Proposition 1)**.** *Using the preceding notation, given an orbit v with invariant set f, there is a bijection between the orbit set $G\backslash V_f(k)$ and the kernel of the map*

$$\gamma : H^1(k, G_x) \to H^1(k, G).$$

As stated in the Introduction, the work in this chapter is based on work by Romano and Thorne in the E_n case as outlined in the papers [RT21], [Rom21], and especially [Tho16]. It differs from other work addressing the 2-Descent Problem in the A_n case in that we study both the local and global Vinberg representations, whereas previous works focus on the local representation. In addition, we address not only the descent step (2), but also step (1); that is, we do not assume that (H, θ) is given, but rather construct the group H and the automorphism θ from the data (C, P, t).

III.2: Constructing the Surface S

Let C be a hyperelliptic curve of genus g defined over K. There exists a degree $2g+2$ polynomial $f(x)$ such that we can write C as the unique smooth completion of the affine curve $\mathcal{C}$ given by

$$y^2 = f(x).$$

The choice of f can vary up to a projective change of coordinates in x; later in this chapter, we discuss the implications of this choice. We will also see that given marked points and tangent vectors on C, we may conclude properties of the form of f.

Given $f(x)$, we also obtain an affine surface $\mathcal{S}$ in $\mathbb{A}^3$ given by the equation

$$y^2 - z^2 = f(x).$$

One smooth, complete model S for $\mathcal{S}$ is a conic bundle over $\mathbb{P}^1_K$ with $2g+2$ nodal fibers. We begin by defining S and note that a different choice of f induced by a projective change of coordinates in x yields an isomorphism between surfaces via a map changing x and fixing all other coordinates. From our definition, it will be clear that S has a map to $\mathbb{P}^1_K$ such that the fibers of this map are generically smooth genus zero curves.

We construct S by gluing together two surfaces defined over $\mathbb{A}^1_k$. Let $m = g+1$. Define the surface S_1 in $\mathbb{P}^2_k \times \mathbb{A}^1_k$, with coordinates $[w : y : z] \times u$ by the equation

$$y^2 - z^2 = w^2 F(u, 1),$$

where $F(u, v)$ is a degree $2m$ homogeneous polynomial such that $F(u, 1) = f(u)$. Define the surface S_2 in $\mathbb{P}^2_k \times \mathbb{A}^1_k$, with coordinates $[w' : y' : z'] \times v$ by the equation

$$y'^2 - z'^2 = w'^2 F(1, v).$$

We can check by directly computing the Jacobians of their defining equations that S_1 and S_2 are smooth, that the fibers above each point of $\mathbb{A}^1_k$ are conics, and that the singular fibers lie above the $2m$ roots of F and are (over K^s) unions of lines intersecting transversely.

We may identify the open subsets $U_1 \subset S_1$ and $U_2 \subset S_2$ where u and v, respectively, are non-zero, via the isomorphism $\phi : U_1 \to U_2$ given by

$$\phi([y : z : w] \times u) \to [y, z, u^m w] \times \frac{1}{u}.$$

Let S be the surface obtained from gluing the S_i along the U_i.

Remark III.2. Note that S comes equipped with an involution $\theta : S \to S$ given on each chart by sending z to $-z$ and fixing all other coordinates.

In summary, we have constructed, given the polynomial $f(x)$, a conic bundle S above $\mathbb{P}^1$ with $2g+2$ reducible nodal fibers.

As seen in Table I.1, to each Dynkin type A_n, we have associated a family of hyperelliptic curves, each with a certain number of marked points. In what follows, we show that we may use the Picard group of S to construct in a functorial way a Lie algebra of type A_n, with n depending on the genus of our hyperelliptic curve C and the marked rational points on C.

III.3: Picard Group of S

In order to describe the Picard group of S, we provide an alternate description of S as a Hirzebruch surface.

Lemma III.3 (Classical, see 1.2.3 of [Dol82])**.** *The Hirzebruch surface $\mathbb{F}_m$ is isomorphic to the blowup of the weighted projective space $\mathbb{P}(1,m,1)$ at its singular point.*

Theorem III.4. *Suppose that f is a degree $2m$ polynomial defined over K with distinct roots in K^s, and let S be the completion of the affine surface*

$$y^2 - z^2 = f(x)$$

constructed in the previous section. Let $u_1, ..., u_{2m}$ be the roots of f, let $[u : v : w]$ be coordinates on $\mathbb{P}(1,m,1)$, let $\mathbb{F}_m = \mathrm{Bl}_{[0:1:0]}\mathbb{P}(1,m,1)$, and let P_i be the the point $[u_i, 0, 1]$ in $\mathbb{P}(1,m,1) \subset \mathbb{F}_m$. Then S is isomorphic over K to $\mathrm{Bl}_{P_1,...,P_{2m}}\mathbb{F}_m$ (note that $\mathrm{Bl}_{P_1,...,P_{2m}}\mathbb{F}_m$ is defined over K since the Galois action permutes the P_i).

Proof. We prove this theorem by explicitly constructing an isomorphism ϕ from $X = \mathrm{Bl}_{P_1,...,P_{2m}}\mathbb{F}_m$ to S. To do this, we recall that Lemma III.3 states that $\mathbb{F}_m$ is the Bl of $\mathbb{P}(1,m,1)$ at $[0:1:0]$.

On the open subset $[a : b : 1]$ of $\mathbb{P}(1,m,1)$ where $a \neq 0$, we set

$$\phi([a:1:b]) = [-2 : -(b + F(\frac{b}{a}, 1)) : b - F(\frac{b}{a}, 1)] \times \frac{b}{a} \in S_1,$$

where S_1 is open subsurface of S defined in the preceding section. Geometrically, on each line L_λ given by the equation $b = \lambda a$, this map is the classical isomorphism, sending the point $[a : 1 : b]$ to the intersection of the line of slope b through $[1 : 1 : 0]$ and the conic S_λ in S lying over $x = \lambda$, between L_λ and S_λ. From this description, one can readily deduce that ϕ extends to a morphism on all of X and is an isomorphism. □

Next, we record some facts about the Picard group of S.

Lemma III.5. *Let the P_i be given as above, and let $S = \mathrm{Bl}_{P_1,\ldots,P_{2m}}\mathbb{F}_m$. Let F be the exceptional curve over $[0:1:0]$. Let D be the curve $u - u_0 w = 0$, where u_0 is not equal to any of the u_i for $1 \leq i \leq 2m$. Let E_i' be the strict transform of the curve $u - u_i w = 0$. Let E_i be the exceptional curve over P_i. Let F' be the strict transform of $v = 0$.*

1. *If θ is the involution of S in Remark III.2, then we have $\theta(F) = F'$ and $\theta(E_i) = E_i'$.*
2. *The group $\mathrm{Pic}(S)(K^s)$ is freely generated by F, D, and the E_i for $1 \leq i \leq 2m$ (note that D corresponds to a fiber of the conic bundle). The intersection numbers are given by the following:*

$$F^2 = -m,\ D^2 = 0,\ E_i^2 = -1,$$

$$F.D = 1,\ F.E_i = 0,$$

$$D.E_i = 0,\ E_i.E_j = 0$$

for $i \neq j$.

3. *The anticanonical class of S is given by*

$$-K_S = 2F + (m+2)D - E_1 - E_2 - \ldots - E_{2m}.$$

(Note that the Galois action fixes F and D permutes the E_i, so that K_S is defined over K.)

Proof. (1) This follows from the isomorphism between $\mathrm{Bl}_{P_1,\ldots,P_{2m}}\mathbb{F}_m$ and S given in proof of the preceding theorem and the explicit formula for θ given in Section 3.2.

(2) By [Bea96, IV.1], the Picard group of $\mathbb{F}_m$ is $\mathbb{Z}F \oplus \mathbb{Z}D$ with intersection matrix

$$\begin{bmatrix} -m & 1 \\ 1 & 0 \end{bmatrix}.$$

The rest follows from the fact that the P_i lie on neither F nor D.

(3) By the remark after 2.7 in [Rei97], the anticanonical class of $\mathbb{F}_m$ is given by $2F + (m+2)D$. Again, the rest follows from the fact that the P_i lie on neither F nor D. □

Now we record some facts about root lattices contained in $\mathrm{Pic}(S)(K^s)$.

Lemma III.6. *1. The orthogonal complement of $-K_S$ in $\mathrm{Pic}(S)(K^s)$ is generated by*

$$e_{-1} = F + (m-1)D - E_1 - E_2 - \ldots - E_{2m}, e_0 = D - E_1 - E_2,$$

$$e_1 = E_1 - E_2, ..., e_{2m-1} = E_{2m-1} - E_{2m}.$$

2. *The orthogonal complement of $-K_S$ and D is generated by e_j for $0 \leq j \leq 2m-1$. The intersection matrix of these e_j is*

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

so that the e_j generate a D_{2m} root lattice.

Proof. (1) Suppose that L in $\mathrm{Pic}(S)(K^s)$ is given by $L = aF + bD + \sum_{i=1}^{2} mc_iE_i$. By Lemma III.5, we have

$$-K_S.L = (2-m)a + 2b + \sum_{i=1}^{2m} c_i.$$

From this equation and the formula for the e_j, we see that for $-1 \leq j \leq 2m-1$, we have $e_j.K_s = 0$ For

$$L = aF + bD + \sum_{i=1}^{2m} c_iE_i$$

in $K_S^{\perp}$, we have that

$$L = ae_{-1} + (b - (m-1))e_0 + \sum_{k=1}^{2m-1} d_ke_k,$$

where the d_k are undetermined coefficients which can be solved given the equality $(2-m)a + 2b + \sum_{i=1}^{2m} c_i = 0$

(2) This follows from part (1) and the fact that if $L = aF + bD + \sum_{i=1}^{2m} c_iE_i$ is perpendicular to K_S and D, then $a = 0$. The intersection numbers can be directly computed using the presentation of the Picard group of S given in Lemma III.5. □

Later, we will use two important anti-canonical curves in S whose properties are described in the following lemmas.

Lemma III.7. *Let S, F, and F' be as above, and let D_1 and D_2 be the strict transforms of the lines $a_1u - b_1w = 0$ and $a_2u - b_2w = 0$, respectively, which do not intersect any of the exceptional loci. Let C' be the union of F, F', D_1, and D_2. Then*

1. *C' is an anticanonical divisor,*

2. $\mathrm{Pic}(C') = \mathbb{G}_m^4$ *(where the first two factors correspond to D_1 and D_2, respectively, and the second two factors correspond to F and F', respectively), and*

3. *the subgroup of elements of* $\mathrm{Pic}(C')$ *negated by the involution θ of Remark III.2 is isomorphic to $\mathbb{G}_m$.*

Proof. (1) Write $C' = aF + bD + \sum_{i=1}^{2} mc_iE_i$. Then we have

$$C'.D = 2,\ C'.F = -m + 2,\ C'.E_i = 1.$$

From this and Lemma III.5, we obtain $a = 2$, $b = m + 2$, and $c_i = -1$. Therefore C' is anticanonical.

(2) This follows from Chapter 9 of [BLR90].

(3) The explicit isomorphism between S and $\mathrm{Bl}_{P_1,\ldots,P_{2m}}\mathbb{F}_m$ given in the proof of Theorem III.4 shows that θ acts on $\mathrm{Pic}(C')$ by the identity on the first two $\mathbb{G}_m$ factors and swaps the second two $\mathbb{G}_m$ factors. Therefore the subgroup negated by θ is isomorphic to $\mathbb{G}_m$. □

Lemma III.8. *Let S, F, and F' be as above, and let D' be the strict transform of the line $au - bw = 0$, chosen to not intersect any of the exceptional loci. Let C'' be the union of F, F',and D'. Then*

1. *C'' is an anticanonical divisor,*

2. $\mathrm{Pic}(C'') = \mathbb{G}_a^2$ *(where the two factors correspond to F and F', respectively), and*

3. *the subgroup of elements of* $\mathrm{Pic}(C'')$ *negated by the involution θ of Remark III.2 is isomorphic to $\mathbb{G}_a$.*

Proof. The proof is similar to that of the previous lemma. □

III.4: Summary of Special Sublattices

We have seen that orthogonal complement of K_S and D, which are both defined over K, in the Picard lattice is a D_{2g+2} lattice Λ_g, which has a K-structure. This has a unique A_{2g+1} sublattice with a K-structure, which we call Λ'_g. Using the notation above, this A_{2g+1} sublattice is generated by the e_i for $1 \leq i \leq 2g+1$ and is given by the orthogonal complement of K_S, D, and F. In the case that we have a marked reducible fiber $E_1 \cup E'_1$ defined over K, we obtain an A_{2g} sublattice with a K-structure, which we call Λ''_g. Using the intersection

matrix in the previous section, we see that the lattice Λ_g'' is the complement of $E_1 - E_1'$ in Λ_g'. The Galois action sends $E_1 - E_1'$ to $E_1' - E_1$, so this complement is defined over K. Using the notation above, the lattice Λ_g'' is generated by the e_i for $2 \leq i \leq 2g+1$.

We note in particular that given a hyperelliptic curve C of genus g and a marked Weierstrass point P, we may choose and equation $f(x)$ with a root at $x = 0$, which leads to a marked reducible fiber defined over K. Thus we may obtain an A_{2g} sublattice. Without the marked Weierstrass point, we can always obtain a D_{2g+2} lattice and an A_{2g+1} lattice with K-structures.

III.5: Lie Groups with Involutions and Extensions of Root Lattices

In order to perform our construction of a Lie group plus additional data, we use a result of Lurie extended by Thorne and Kaletha in [Tho16] which connects Lie groups with stable involutions to extensions of root lattices. To describe this result, it is helpful to first define two categories.

Definition III.9. *Let $\mathcal{L}$ be the category consisting of tuples (H, θ, T, π), where*

1. *H is a simple adjoint Lie group defined over K,*
2. *θ is a stable involution of H with trace $-\mathrm{rk}(H)$, T is a maximal torus of H on which θ acts by inversion,*
3. *and $\pi : \mathfrak{g} = \mathfrak{h}^\theta \to \mathfrak{gl}(W)$ is a representation defined over K.*

A morphism from (H, θ, T, π) to (H', θ', T', ϕ') consists of

1. *an isomorphism $\rho : H \to H'$ sending T to T' such that $\theta' \circ \rho = \rho \circ \theta$*
2. *and a K-vector space isomorphism $\phi : W \to W'$ such that if $\Phi : \mathfrak{gl}(W) \to \mathfrak{gl}(W')$ is defined by $\Phi(m) = \phi \circ m \circ \phi^{-1}$, then $\Phi \circ \pi = \pi' \circ d\rho$.*

Definition III.10. *Let $\mathcal{R}$ be the category consisting of tuples $(\Lambda, \psi, \tilde{V}, \mu, \gamma)$, where*

1. *Λ is a simply laced root lattice defined over K^s with associated quadratic form q and $V := \Lambda/2\Lambda$ (we will also use q to denote the $\mathbb{F}_2$-valued quadratic form on V),*
2. *$\psi : \Gamma_K \to W(\Lambda)$ is a continuous homomorphism from the absolute Galois group Γ_K of K^s/K to the Weyl group of Λ,*

3. *$\tilde{V}$ is a central extension*

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

such that $\tilde{v}^2 = (-1)^{q(v)}$ for any $\tilde{v} \in \tilde{V}$ lying above v in V.

4. *$\mu : \Gamma_K \to \mathrm{Aut}(\tilde{V})$ is a continuous homomorphism such that $\mu(\Gamma_K)$ leaves the subgroup $\{\pm 1\}$ of $\tilde{V}$ invariant and that the maps*

$$\Gamma_K \xrightarrow{\psi} W(\Lambda) \subset \mathrm{Aut}(\Lambda) \longrightarrow \mathrm{Aut}(V)$$

and

$$\Gamma_K \xrightarrow{\mu} \mathrm{Aut}(\tilde{V}) \longrightarrow \mathrm{Aut}(V)$$

coincide,

5. *and $\gamma : \tilde{V} \to \mathrm{GL}(W \otimes K^s)$ is a Γ_K-invariant group homomorphism from $\tilde{V}$ into the automorphisms of some K-vector space W such that $\gamma(-1) = -\mathrm{id}_W$.*

A morphism from $(\Lambda, \psi, \tilde{V}, \mu, \gamma)$ to $(\Lambda', \psi', \tilde{V}', \mu', \gamma')$ is

1. *an isomorphism $\rho : \Lambda \to \Lambda'$ of simply laced root lattices which commutes with the actions of ψ and μ*

2. *an K-vector space isomorphism $\phi : W \to W'$ which agrees with the maps γ and γ'.*

Theorem III.11 (Section 2 and Appendix of [Tho16])**.** *There is a functor $F : \mathcal{R} \to \mathcal{L}$ which induces an equivalence of of categories.*

Definition III.12. *An object of $\mathcal{L}$ such that $\mathfrak{h}$ and $\mathfrak{h}^{d\theta}$ are both split is called a split object.*

Finally, we will use the following results on involutions of split Lie algebras.

Theorem III.13. *Suppose that H and H_0 are split, simple adjoint Lie groups over K of Dynkin type A_n equipped with involutions θ and θ_0, respectively. There exists an isomorphism $\psi : H \to H_0$ satisfying*

$$\theta_0 \circ \psi = \psi \circ \theta,$$

and ψ is unique up to $H^\theta(K)$-conjugacy and multiplication by θ in the sense that if an isomorphism $\psi' : H \to H_0$ has the same property, then $\psi^{-1} \circ \psi'$ is of the form $\theta \circ C_h$, where $C_h : H \to H$ is conjugation by some element h of H^θ.

Let V_0 be the standard representation of $\mathfrak{h}_0 \cong \mathfrak{sl}(n+1)$. We may choose ψ so that $\psi^*(V_0)$ is the standard representation of of $\mathfrak{h}$, and with this assumption, the map ψ is unique up to H^θ-conjugacy.

Let W_0 be the standard representation of $\mathfrak{g}_0 = \mathfrak{h}_0^\theta = \mathfrak{so}(n+1)$. We may choose ψ so that in addition, $\psi^*(W_0)$ is the standard representation of $\mathfrak{g} = \mathfrak{h}^\theta$, and with this additional assumption, the map ψ is unique up to $(H^\theta)^\circ$-conjugacy.

The proof of this theorem utilizes the following lemma.

Lemma III.14 (Proposition 1.9, [Tho16])**.** *Let H be a simple, adjoint split Lie group defined over K of type A_n. The class of involutions θ satisfying*

1. $\mathrm{tr}(d\theta : \mathfrak{h} \to \mathfrak{h}) = -\mathrm{rk}H$ *and*
2. *the identity component $(H^\theta)^\circ$ of H^θ is split*

is unique up to $H(K)$-conjugacy.

Proof of Theorem III.13. Since H and H_0 are simple, adjoint, split Lie groups over K with the same Dynkin type, there exists some isomorphism $\psi : H \to H_0$. We can check that $\psi^{-1} \circ \theta_0 \circ \psi$ is an involution on H satisfying the conditions in Lemma III.14. Therefore there exists some h in H such that

$$(\psi \circ L_h)^{-1} \circ \theta_0 \circ (\psi \circ L_h) = \theta,$$

where $L_h : H \to H$ is left multiplication by h. Replacing ψ with $\psi \circ L_h$, we have shown the existence of an isomorphism ψ such that $\theta_0 \circ \psi = \psi \circ \theta$.

To show uniqueness, it suffices to show that the commutator of θ in $\mathrm{Aut}(H)$ is given by elements of the form $\theta \circ C_h$, where h is in H^θ; indeed, when H is of type A_n, then $\mathrm{Aut}(H)$ is a semidirect product of the inner automorphisms with the cyclic group generated by θ, as shown in the description of θ given in [Tho13, Lemma 2.13]. It is clear that θ commutes with itself, so we need to show that if C_h commutes with θ, then h is fixed by θ. If C_h commutes with θ, then for all $g \in H$, we have

$$\theta(h) g \theta(h)^{-1} = hgh^{-1}.$$

Since H is adjoint, this implies $\theta(h) = h$, so that h is in H^θ.

By the classification of representations of $\mathfrak{sl}(n+1)$, as in [Tit66, pp. 54–58], we have that $\psi^*(V_0)$ is either isomorphic to the standard representation or its dual. Since $\theta^*(V_0)$ is

the dual to the standard representation, if $\psi^*(V_0)$ is isomorphic to the dual of the standard representation, we replace ψ by $\theta \circ \psi$. Then ψ is unique up to H^θ-conjugacy.

If n is even, then H^θ is connected, and we are done. If n is odd, then H^θ has two components and conjugating by an element of the non-identity component sends $\psi^*(W_0)$ to its dual while leaving $\psi^*(V_0)$ fixed. Therefore if $\psi^*(W_0)$ is isomorphic to the dual of the standard representation of $\mathfrak{so}(n)$, we conjugate ψ by an element of H^θ not in the identity component. Then ψ is unique up to $(H^\theta)^\circ$-conjugacy.

□

III.6: Heisenberg Groups

We recall some well-known material on Heisenberg groups of abelian varieties, which we will use to construct our central extensions. For references and proofs where needed, we refer to [BL04].

Definition III.15. *Let X be an abelian variety defined over an algebraically closed field of characteristic 0. Let L be a very ample line bundle on X.*

The group $K(X, L)$ is the subgroup of elements x in X such that $t_x^*(L)$ is isomorphic to L.

The Heisenberg group $\mathcal{H}(X, L)$ is the group of pairs (x, ϕ), where $t_x^*(L)$ is isomorphic to L and such that the diagram

$$\begin{array}{ccc} L & \xrightarrow{\phi} & L \\ \downarrow & & \downarrow \\ X & \xrightarrow{t_x^*} & X \end{array}$$

is Cartesian.

The product $(x, \phi).(y, \psi)$ is equal to $(x + y, \phi \circ \psi)$.

Lemma III.16. *The map $\pi : \mathcal{H}(X, L) \to K(X, L)$ given by forgetting ϕ canonically identifies $\mathcal{H}(X, L)$ with a central extension of $K(X, L)$ by $\mathbb{G}_m$.*

Proof. The map π is clearly surjective, and the kernel of π is simply the isomorphism group of L, which is canonically isomorphic to $\mathbb{G}_m$. □

We are specifically interested in the Heisenberg groups of line bundles related to theta divisors on Jacobians. We recall the definition of a theta divisor.

Definition III.17. *A divisor Θ which defines a principal polarization on $J(C)$ is called a* theta divisor *(see [BL04, p.323] for further details). A divisor on $J(C)$ is called* symmetric *if it is fixed by the pullback map $(-1)^*$ on $\mathrm{Pic}(J(C))$.*

We will use the following result in our computations.

Lemma III.18. *Suppose that C is a curve of genus g defined over K. Let Θ be a symmetric theta divisor, and for a point $B \in J(C)$, let Θ_B be equal to $t_B^*(\Theta)$. The following are true. For any $d > 0$, we have*

1. $h^0(J(C), d\Theta_B) := \dim H^0(J(C), d\Theta_B) = d^g$ *and*
2. $K(J(C), d\Theta_B) = J(C)[d]$.

Proof. 1. This follows from [BL04, 3.2.8] along with the fact that Θ, by definition, defines a principal polarization on $J(C)$.

2. This follows from [BL04, 11.3.4]. □

Lemma III.19. *For any $h = (x, \phi)$ in $\mathcal{H}(J(C), 2\Theta_B)$, we that h^2 lies in $\mathbb{G}_m$. Therefore there is a well-defined map*

$$\chi : \mathcal{H}(J(C), 2\Theta_B) \to \mathbb{G}_m$$

sending h to $(-1)^{q(x)}h^2$, where q is the quadratic form on $J(C)[2]$ induced by the Weil pairing.

Proof. For $h = (x, \phi)$, in $\mathcal{H}(J(C), 2\Theta_B)$, by Lemma III.18 we have that x lives in $K(J(C), 2\Theta_B) = J(C)[2]$. Therefore $h^2 = (x + x, \phi \circ \phi) = (0, \phi \circ \phi)$. □

Definition III.20. *Suppose that $\omega \in H^0(X, L)$ is a global section of L. For any element (x, ϕ) in $\mathcal{H}(X, L)$, the element $\phi \circ \omega \circ t_x^{-1}$ is also a global section. Thus (x, ϕ) acts on $H^0(X, L)$, and this action defines the canonical representation $\rho : \mathcal{H}(X, L) \to \mathrm{GL}(H^0(X, L))$.*

Lemma III.21. . *The canonical representation is irreducible. In the specific case of $\mathcal{H}(J(C), 2\Theta_B)$, we have that the restriction of ρ to the subgroup $\ker(\chi)$ is an irreducible representation of $\ker(\chi)$ as well.*

In addition, we have that $\rho(-1) = -1$, where here -1 denotes the element

$$(0, -1) \in \mathbb{G}_m \subset \mathcal{H}(X, L).$$

Proof. The first sentence is [BL04, 6.4.3]; the proof given there shows, in addition, that given any non-zero vector v in $H^0(J(C), 2\Theta_B)$, there exist elements $g_1, ..., g_m$ in $\mathcal{H}(J(C), 2\Theta_B)$, such that $g_1.v, ..., g_m.v$ is a basis of $H^0(J(C), 2\Theta_B)$. By scaling, we may assume that $g_1, ..., g_m$ lie in $\ker(\chi)$. This shows that there are no non-trivial subrepresentations of ρ on $\ker(\chi)$, so that ρ is irreducible on $\ker(\chi)$.

The second sentence follows immediately from the definition of ρ; namely, given a section $\omega \in H^0(X, L)$, we have that

$$\rho(-1).(\omega) = (0, -1).\omega = (-1) \circ \omega = -\omega,$$

which finishes the proof. □

In addition, we will need to show that various line bundles have a K-structure, even when we work in part over its algebraic closure K^s.

Lemma III.22. *Suppose that C is a curve of genus g defined over a field K (not necessarily algebraically closed) of characteristic 0. If Θ is a symmetric theta divisor defined over K and B in $J(C)$ is such that $2B$ is defined over K, then $2\Theta_B$ is also defined over k.*

Proof. This follows from applying [BL04, 11.3.4] with (in the notation of that book) $\kappa = \omega + B$, where ω is any theta divisor on C defined over K^s. □

III.7: Marked Data and Equations

In this section, we show that given additional marked data on the curve C, we can make assumptions about the form of f in the defining equation of our surface S. These assumptions will be useful in the following sections.

Lemma III.23. *Given a hyperelliptic curve C of genus g defined over K and marked rational points P_1 and P_2 defined over K such that $[P_1 + P_2]$ is the hyperelliptic class, there is a polynomial $f(x)$ of degree $2g + 2$ such that*

1. *f is monic,*
2. *the coefficient of x^{2g+1} in f is zero,*
3. *C is the unique smooth completion of the affine curve*

$$y^2 = f(x), \text{ and}$$

4. *if $F(x, z)$ is the homogenization of f, then there is an isomorphism from C to the curve*

$$Y^2 = F(X, Z)$$

in $\mathbb{P}(1, g + 1, 1)$ sending P_1 to $[1 : 1 : 0]$.

Further, f is unique up to a change in the equation induced by the change in variables $x \to \lambda x$, $y \to \lambda^{g+1} y$, where λ is a non-zero constant.

Before beginning the proof, we recall note that for $n = 2g + 1$, the curves in the family $\pi : X \to B$ corresponding to the degree-2 Vinberg representation of type A_n are exactly those of the form

$$y^2 = f(x),$$

where f satisfies conditions 1-4.

Proof. It is a classical fact (see for example [Sha13, 6.5]) that there exists a polynomial f satisfying properties 1, 3, and 4. After possibly translating x, we can assume that 2 is satisfied. By conditions 3 and 4, x must be a rational function on C in the Riemann-Roch space $\mathcal{L}(P_1 + P_2)$, and y must be a rational function in the Riemann-Roch space $\mathcal{L}((g + 1)(P_1 + P_2))$. In order to preserve conditions 1–4, the only other possible choices of x and y are $x \to \lambda x$, $y \to \lambda^{g+1} y$, where λ is a non-zero constant. □

Lemma III.24. *Given a hyperelliptic curve C of genus g defined over K, a marked Weierstrass point P defined over K, and a non-zero tangent vector t in the tangent space at P defined over K, there is a unique polynomial $f(x)$ of degree $2g + 2$ such that*

1. *f is monic,*
2. *the coefficient of x^{2g+1} in f is zero,*
3. *C is the unique smooth completion of the affine curve*

$$y^2 = f(x),$$

4. *if $F(x, z)$ is the homogenization of f, then there is an isomorphism from C to the curve*

$$Y^2 = F(X, Z)$$

   in $\mathbb{P}(1, g + 1, 1)$ sending P_1 to $[1 : 1 : 0]$, and

5. *the differential $d(\frac{Z}{X})$ sends t to 1.*

Before beginning the proof of this lemma, we note that the choice of coordinates for the family $\pi : X \to B$ described in the text preceding Table I.1 in the Introduction gives a canonical choice of tangent vector for the marked point(s) at infinity.

Proof. We have already shown a polynomial $f(x)$ exists satisfying 1-4 unique up to a change in the equation induced by the change in variables $x \to \lambda x$, $y \to \lambda^{g+1} y$, where λ is a non-zero constant.

We now show that we may choose $f(x)$ satisfying 5. By 4., on the affine coordinates $a = \frac{Z}{X}, b = \frac{Y}{X^{g+1}}$, the tangent space to P_1 can be identified with the subspace $b = 1$. Since t is non-zero, $d(\frac{Z}{X}) = da$ sends t to some non-zero scalar k. We set $\lambda = k$, and this fixes our choice of λ. □

The proofs of the following two lemmas are similar.

Lemma III.25. *Given a hyperelliptic curve C of genus g defined over K and a marked rational Weierstrass point P defined over K, there is a polynomial $f(x)$ of degree $2g+2$ such that*

1. *the constant term in f is 0,*
2. *the coefficient of x in f is 1,*
3. *the coefficient of x^2 in f is 1,*
4. *C is the unique smooth completion of the affine curve*

$$y^2 = f(x), \text{ and}$$

5. *if $F(x, z)$ is the homogenization of f, then there is an isomorphism from C to the curve*

$$Y^2 = F(X, Z)$$

in $\mathbb{P}(1, g + 1, 1)$ sending P to $[0 : 0 : 1]$.

Further, f is unique up to a change in the equation induced by the change in variables $x \to \lambda x$, $y \to \lambda^{g+1} y$, where λ is a non-zero constant.

We note that Table I.1 shows that for $n = 2g$, the curves in the family $\pi : X \to B$ corresponding to the degree-2 Vinberg representation of type A_n are exactly those of the form

$$y^2 = h(x),$$

where h is of degree $2g + 1$ and satisfies conditions 1-3 in Lemma III.23. This curve is birational via a transformation of the form $x \to \frac{1}{x-a}$, $y \to \frac{y}{x^{g+1}}$ to an affine curve of the form

$$y^2 = f(x),$$

where f satisfies conditions 1-5 in Lemma III.25.

Proof. It is a classical fact that there exists a polynomial f of degree $2g+1$ satisfying conditions 1-4 in Lemma III.23. After a birational transformation of the kind in the remarks preceding this proof, we may assume f is of degree $2g+2$ and satisfies conditions 1-4 in Lemma III.25. The rest of the proof proceeds similarly to that of Lemma III.23. □

Lemma III.26. *Given a hyperelliptic curve C of genus g defined over K, a marked Weierstrass point P defined over K, and a non-zero tangent vector t in the tangent space at P defined over K, there is a unique polynomial $f(x)$ of degree $2g+2$ such that*

1. *the constant term in f is 0,*
2. *the coefficient of x in f is 1,*
3. *the coefficient of x^2 in f is 1,*
4. *C is the unique smooth completion of the affine curve*

$$y^2 = f(x),$$

5. *if $F(x,z)$ is the homogenization of f, then there is an isomorphism from C to the curve*

$$Y^2 = F(X,Z)$$

   in $\mathbb{P}(1,g+1,1)$ sending P to $[0:0:1]$, and

6. *the differential $d(\frac{Y}{X})$ sends t to 1.*

Proof. The proof is similar to that of Lemma III.24. □

III.8: Connections to Jacobians of Curves

Recall that C naturally lives inside S as the locus (on each affine piece S_i) $z=0$. Let $i : C \to S$ be the inclusion. Then i induces a map $i^* : \mathrm{Pic}(S) \to \mathrm{Pic}(C)$. Let Λ be one of the sublattices Λ_g, Λ'_g, or Λ''_g defined in Section III.4. The map i^* descends to a *restriction map* $r : \Lambda \to \mathrm{Pic}(C)$. We will show that r induces a surjection from $V := \Lambda_\theta = \Lambda/2\Lambda$ onto $\mathrm{Pic}(C)[2] = J(C)[2]$, and that it preserves natural bilinear $\mathbb{F}_2$-forms that we define on each group. In this section, we will switch freely between the description of S given via equations and the description as a blowup of a Hirzebruch surface.

Definition III.27. *The Weil pairing $\langle \cdot, \cdot \rangle_{J(C)[2]}$ is the non-degenerate bilinear $\mathbb{F}_2$-form on $J(C)[2]$ given by taking the usual Weil pairing $J(C)[2] \times J(C)[2] \to \mu_2$ and identifying μ_2 with $\mathbb{F}_2$.*

Definition III.28. *The form $\langle \cdot, \cdot \rangle_V$ is defined to be the non-degenerate bilinear $\mathbb{F}_2$-form on $V = \Lambda/2\Lambda$ given by taking the intersection number, modulo 2. (The non-degeneracy can be checked directly using the intersection matrix in Lemma III.6.)*

Lemma III.29. *The restriction map $r : \Lambda \to \mathrm{Pic}(C)$ is surjective onto $\mathrm{Pic}(C)[2]$, contains 2Λ in its kernel, and preserves the non-degenerate $\mathbb{F}_2$-forms on each vector space. In the case $\Lambda = \Lambda_g''$, this restriction map induces an isomorphism between $\Lambda/2\Lambda$ and $\mathrm{Pic}(C)[2]$.*

The proof is by direct computation. Before beginning the proof, it is helpful to remember how to compute the Weil pairing. The following lemma is classical.

Lemma III.30. *Let $(\cdot, \cdot)$ denote the usual μ_2-valued Weil pairing on $J(C)[2]$. Suppose that $[D]$ and $[E]$ are 2-torsion divisor classes, i.e., $2[D] = 2[E] = [0]$. Choose rational functions f and g such that $\mathrm{div}(f) = D$ and $\mathrm{div}(g) = E$. Then*

$$([D], [E]) = \prod_{P \in C} \frac{g^{\mathrm{ord}_P(D)}}{f^{\mathrm{ord}_P(E)}}(P).$$

Proof. See Exercise 3.16 of [Sil86] for an equivalent formulation. □

In addition, we recall the structure of $J(C)[2]$ when C is hyperelliptic of genus g.

Lemma III.31. *Suppose that $P_1, ..., P_{2g+1}$ are $2g+1$ distinct Weierstrass points of C. The divisor classes*

$$[D_1] = [P_2 - P_1], ..., [D_{2g}] = [P_{2g+1} - P_1]$$

form a basis of $J(C)[2]$.

Proof. Using the intersection matrix given in Lemma III.6, we can compute

$$\langle [D_i], [D_i] \rangle_{J(C)[2]} = 0, \ \langle [D_i], [D_j] \rangle_{J(C)[2]} = 1, \ i \neq j$$

A fact from linear algebra (see for example [Zar08, Lemma 2.8]) implies that given these intersection numbers, the $[D_i]$ are linearly independent. Since $J(C)[2]$ is $2g$-dimensional as an $\mathbb{F}_2$ vector space, the $[D_i]$ form a basis. □

Proof of Lemma III.29. Let $P_1, ..., P_{n+1}$ be the affine Weierstrass points of C, and a_i be the x-coordinate of P_i. The divisor E_i defined in Section 3.3 lives in the fiber above a_i, and $i^*([E_i]) = [P_i]$. Using the notation of Lemma III.6, we then have $r([e_i]) = [P_i - P_{i+1}]$ for $1 \leq i \leq 2g+1$.

We can see directly that the divisor classes $[D_i] = [P_{i+1} - P_1]$ for $1 \leq i \leq 2g$ lie in the image of r, so that r is surjective by Lemma III.31. In the case $\Lambda = \Lambda_g''$, the lattice Λ is

generated by e_i for $2 \leq i \leq 2g+1$, so it contains the $2g$ divisor classes $[D_i'] = [P_{i+1} - P_2]$. Since $V = \Lambda/2\Lambda$ and $J(C)[2]$ are both $2g$-dimensional as $\mathbb{F}_2$ vector spaces, r induces an isomorphism between V and $J(C)[2]$.

□

III.9: Canonical Orbits

In this section, we associate to each appropriate tuple (C, P, t) a Lie group G and a canonical element κ_C (or μ_C) of the vector space V (respectively, variety Y) on which G acts. The element κ_C (or μ_C) will correspond to the image of $0 \in J(C)$ under the descent map as well as index the orbit space in which the image of $J(C)$ lies. First, we make a definition in order to better discuss our tuples.

Definition III.32. *For $n = 2m$, let $\mathcal{S}_n(K)$ be the set of equivalence classes of pairs (C, P, t), where C is a smooth, genus m hyperelliptic curve defined over K, P is a marked Weierstrass K-point on C, and t is a tangent vector at P. For $n = 2m+1$, let $\mathcal{S}_n(K)$ be the set of equivalence classes of pairs (C, P, t), where C is a smooth, genus m hyperelliptic curve, P is a marked non-Weierstrass K-point on C, and t is a tangent vector at P.*

By Lemmas III.24 and III.26, each object in $\mathcal{S}_n(K)$ determines a unique polynomial $f(x)$. Let $\mathcal{S}_n^0(K)$ be the objects such that the constant term of $f(x)$ is non-zero.

Suppose that we are given a tuple v in $\mathcal{S}_n(K)$ for some n. Let C be the curve in v. Let $B \in J(C)(K^s)$ be a line bundle such that $2B$ is defined over K.

We will construct an object ρ_B in the category $\mathcal{R}$. Let S be the completion of the affine surface $y^2 - z^2 = f(x)$, where $f(x)$ is the unique polynomial corresponding to v from Lemmas III.24 and III.26.

To give an object of $\mathcal{R}$, we must specify a tuple $(\Lambda_B, \psi_B, \tilde{V}_B, \mu_B, \gamma_B)$. We define Λ_B to be the lattice Λ_g' if n is even and Λ_g'' if n is odd. We can check by the explicit generators given for Λ_B that the Galois group Γ_K acts via automorphisms in the Weyl group, which specifies the map ψ_B.

The most involved part is defining the central extension $\tilde{V}_B$. Recall that by definition, $V_B = \Lambda_B/2\Lambda_B$. By Lemma III.18, we have a central extension $\mathcal{H}(J(C), 2\Theta_B)$ of $K(J(C), 2\Theta_B) = J(C)[2]$ by $\mathbb{G}_m$. We push this out by the (Galois invariant) surjection $r : V \to J(C)[2]$ of Lemma III.29 to obtain a central extension $\tilde{E}_B$ of V_B by $\mathbb{G}_m$. The extension $\tilde{E}_B$ has the property that for any $\tilde{e} \in \tilde{E}_B$ lying above e in V_B, we have that $\tilde{e}^2$ is in $\mathbb{G}_m$ (since the extension $\mathcal{H}(J(C), 2\Theta_B)$ has this property by Lemma III.19). Therefore we may define a map $\chi_B : \tilde{E}_B \to \mathbb{G}_m$ by $\chi_B(\tilde{e}) = (-1)^{q(e)}\tilde{e}^2$. Define $\tilde{V}_B := \ker \chi_B$. Then $\tilde{V}_B$ is a

central extension of V_B by $\{\pm 1\}$, and $\chi_B(\tilde{v}) = (-1)^{q(v)}\tilde{v}^2 = 1$, so $\tilde{v}^2 = (-1)^{q(v)}$ for any $\tilde{v}$ in $\tilde{V}_B$.

The map μ_B comes from pushing out the analogous map by the extension $\mathcal{H}(J(C), 2\Theta_B)$ (and its properties are checked the same way).

Similarly, γ_B comes from pushing out the canonical representation on $\mathcal{H}(J(C), 2\Theta_B)$.

Definition III.33. *Having constructed an object ρ_B of $\mathcal{R}$, we define λ_B in $\mathcal{L}$ to be $\lambda_B := F(\rho_B)$, where F is the equivalence of categories in Theorem III.11.*

The most canonical choice of tuple in $\mathcal{L}$ associated to $v = (C, P, t)$ is of course the object $\lambda_0 = (H_0, \theta_0, T_0, \pi_0)$ corresponding to the trivial bundle $0 \in J(C)$ as in Theorem III.35. We construct canonical elements in the orbit spaces $W_0\backslash\mathfrak{t}_0$ and $W_0\backslash T_0$. The idea is that for any given invariant set $\mathbf{f}$, an orbit in the torus with invariant set $\mathbf{f}$ is the most "obvious" choice (although we note that if K is not algebraically closed, there can be multiple orbits in the torus with a given invariant set).

We recall that for a smooth hyperelliptic curve C, the polynomial f in the equation $y^2 = f(x)$ corresponding to C has distinct roots. In terms of the Vinberg representation, this means C corresponds to the set of invariants of a regular semistable orbit. Therefore, we want to show that we may associate to each curve C a point in T_0^{rss}.

Lemma III.34. *Given a datum $v = [(C, P, t)] \in \mathcal{S}_n(K)$, and a point B in $J(C)(K)$ such that $2B$ is defined over K, there is a canonical choice of*

1. *a point $\kappa_{C,B} \in \mathfrak{t}_B^{rss}(K)$, where T_B is the maximal torus corresponding to λ_B, as in Theorem III.35, and $\mathfrak{t}_B$ its Lie algebra, and*

2. *if v is in $\mathcal{S}_n^0(K)$, a point $\mu_{C,B}$ in $T_B^{rss}(K)$.*

Proof. For 1., let C'' be the anticanonical curve in Lemma III.8 with D chosen to be the curve $w = 0$. Since θ acts on $\mathrm{Pic}(S)(K^s)$ by negation, the image of the restriction map $r : \Lambda = \Lambda_B \to \mathrm{Pic}(C'')$ lies inside the subgroup A of $\mathrm{Pic}(C')$ negated by θ, which is isomorphic to $\mathbb{G}_a$, but not canonically. We choose an isomorphism as follows. Each element of A can be uniquely represented as $P_1 - P_2$, where P_1 and P_2 are effective divisors whose support is on the regular points of F', or in this case the set of points $[u : 0 : 1]$ (since D was chosen to be the curve $w = 0$). We obtain an isomorphism $A \cong \mathbb{G}_a$ sending $[u : 0 : 1]$ to u and extending linearly. Therefore we obtain a map $\Lambda_B \to A \subset \mathrm{Pic}(C'') \to \mathbb{G}_a$, which corresponds to an element $\kappa_{C,B}$ of the the Cartan subspace $\mathfrak{t}_B \cong \mathrm{Hom}(\Lambda_B, \mathbb{G}_a)$. To show that $\kappa_{C,B}$ lies in the regular semisimple locus $\mathfrak{t}_B$, we must show that $\kappa_{C,B}$ doesn't send any roots to 0.This can be checked explicitly using the description of the divisors E_i and E_i'.

For 2., let C' be the anticanonical curve in Lemma III.7 with D_1 chosen to be the curve $u = 0$ and D_2 chosen to be the curve $w = 0$ (this is possible since 0 is assumed not to be a root of $f(x)$). The rest of the proof proceeds similarly to that of 1. □

Theorem III.35. *Let λ_B be the object $\mathcal{L}$ from definition III.33. Assuming that H_B is split, we have that λ_B is split.*

Proof. By Lemma III.34, we have that $(\mathfrak{g}_B)_1$ contains a regular semisimple element. By Lemma II.21, G_B is split. □

From now on, we use κ_C to denote $\kappa_{C,0}$ and μ_C to denote $\mu_{C,0}$.

Theorem III.36. *The map assigning $v = [(C, P, t)]$ to κ_C induces a map Φ from $\mathcal{S}_n(k)$ into $W_0\backslash\mathfrak{t}_0^{rss}$. If K is algebraically closed, this map is a bijection.*

Proof. The proof of Lemma III.34 shows that κ_C is canoincally determined by v, so that the orbit $[\kappa_C]$ is well-defined. To show that Φ is a bijection if K is algebraically closed, we construct an inverse Ψ following the argument in the proof of Proposition 1.8 of [Loo93]. Suppose that χ is a character on $\mathfrak{t}_0^{rss}$, i.e., $\chi(E_i - E_j) \neq 0$ for any $i \neq j$. Choose an arbitrary point P_1 in $\mathbb{G}_a = A^1_K$. For $P_2, ..., P_n$, let $P_{i+1} = \chi(E_{i+1} - E_i)P_i$. Since χ is in $\mathfrak{t}_0^{rss}$, the P_j are distinct for all $1 \leq j \leq n$. Let $g(x)$ be the degree n monic polynomial in x with roots at the P_j, and let $f(x)$ be the shift of g so that the equation has zero as the coefficient of x^{n-1} (then g depends on the initial choice of P_1, but not f).

The action of W on χ simply permutes the roots of f and thus does not alter f. Therefore each orbit in $W_0\backslash\mathfrak{t}_0^{rss}$ yields a well-defined class v, namely the curve C with marked point(s) at infinity and canonical choice of tangent vector given by the affine equation $y^2 = f(x)$. Define $\Psi([\chi])$ to be the class $[(C, P, t)]$. Then Ψ is the inverse of Φ. □

The following lemma relates the elements $\kappa_{C,B}$ to the canonical element $\kappa_C = \kappa_{C,0}$.

Lemma III.37. *Let $(H_0, \theta_0, T_0, \pi_0)$ and $(H_B, \theta_B, T_B, \pi_B)$ be the split objects of $\mathcal{L}$ of Theorem III.35. and $\psi : H_0 \to H_B$ an isomorphism satsifying all the assumptions in Theorem III.13. Then $\psi^{-1}(\kappa_{C,B})$ lies in the same G_0-orbit as $\kappa_C = \kappa_{C,0}$ over K^s.*

Proof. Over K^s, the tuples $(H_0, \theta_0, T_0, \pi_0)$ and $(H_B, \theta_B, T_B, \pi_B)$ are isomorphic objects of $\mathcal{L}$, so there exists an isomorphism $\mathcal{F}_B$ between them defined over K^s. In particular, we have a map $\mathcal{F}_B : H_0 \to H_B$ which by definition sends T_0 to T_B, identifies Λ_B with Λ_0, and thus sends $\kappa_{C,0}$ to $\kappa_{C,B}$, and which also commutes with the involutions. By the proof of Theorem III.13, we may further assume after modifying $\mathcal{F}_B$ by conjugation by elements of $H_0^\theta(K)$ that $\mathcal{F}_B$ preserves the standard representations of $\mathfrak{h}_0$ and $\mathfrak{g}_0$. (Of relevance to later work is that

this modification does not change the cocycle class $\mathcal{F}_B^{-1\sigma}\mathcal{F}_B$ where σ is an element of the absolute Galois group.)

Thus $\psi^{-1} \circ \mathcal{F}_B$ is an automorphism of H_0 defined over K^s satsifying all the assumptions in Theorem III.13, so it is equal to conjugation by some element of $G_0(K^s)$. At the same time, we have $\psi^{-1} \circ \mathcal{F}_B(\kappa_{C,0}) = \psi^{-1}(\kappa_{C,B})$, thus completing the proof of the lemma. □

III.10: Descriptions of the Stabilizer Group

In order to construct our descent maps, we will pass between several equivalent descriptions of the stabilizer subgroup $(G_0)_{\kappa_C}$ of κ_C in G_0. This section is dedicated to proving the following theorem.

Theorem III.38. *There is an isomorphism $\delta : (G_0)_{\kappa_C} \to J(C)[2]$ such that the isomorphism ϕ, given in Theorem I.4, between $G_0\backslash V_{\kappa_C}$ and*

$$\ker(\gamma : H^1(K, (G_0)_{\kappa_C}) \to H^1(K, G_0))$$

which sends κ_C to the zero cocycle sends the orbit of $\psi^{-1}(\kappa_{C,B})$, where ψ is the map in Lemma III.37, to the coycle $\sigma \to B^\sigma - B$ under the isomorphism induced by δ between $H^1(K, (G_0)_{\kappa_C})$ and $H^1(K, J(C)[2])$.

The same claim is true if we replace κ_C by μ_C.

This is theorem is the assertion implicitly underlying the argument in the 4th paragraph of the proof of Theorem 3.6 in [Tho16]. For clarity, we provide a proof of this theorem. In order to construct the isomorphism δ and verify its properties, we need a series of intermediate lemmas.

Lemma III.39. *Using the notation above, we have*

$$(G_0)_{\kappa_C} = (G_0)_{\mu_C} = (T \cap G_0)[2].$$

(Note that this is an actual equality, not merely an isomorphism.)

Proof. By definition, we have that $(G_0)_{\mu_C}$ consists of the elements of G_0 which commute with μ_C. Since μ_C is regular semisimple and lives in T, its commutator in H_0 is exactly T, so that $(G_0)_{\mu_C} = T \cap G_0$. Since θ acts on T by inversion and θ acts trivially on G_0, for any g in $T \cap G_0$, we have $\theta(g) = g = g^{-1}$, so that g is 2-torsion. Therefore we have

$$(G_0)_{\mu_C} = T \cap G_0 = (T \cap G_0)[2].$$

For the case of $(G_0)_{\kappa_C}$ we may apply the same argument, along with the statements and proofs in [Tho13, 2.8-2.10]. □

Definition III.40. *Let*

$$0 \longrightarrow A \longrightarrow B \xrightarrow{\phi} C \longrightarrow 0$$

be a central extension of groups. We define the group $\mathrm{Aut}(B; C)$ *to be the group of automorphisms* f *of* B *such that* f *leaves* A *fixed and* $f \circ \phi = \phi$.

Lemma III.41 (Lemma 1.7 of [Tho16])**.** *The map*

$$\alpha : J(C)[2] \to \mathrm{Aut}(\mathcal{H}(J(C), 2\Theta_B); J(C)[2])$$

given by

$$\nu \to ((\omega, \psi) \to (\omega, (-1)^{\langle \nu, \omega \rangle}\psi))$$

is an isomorphism of groups.

Lemma III.42 (Lemma 1.8 of [Tho16])**.** *Let* σ *be an element of the absolute Galois group* Γ_K*, and suppose that* $B \in J(C)(K^s)$ *satisfies* $2B = A$*, where* A *is in* $J(C)(K)$*. Then* $B^\sigma - B$ *lies in* $J(C)[2](K^s)$ *and*

$$\alpha(B^\sigma - B) = F_B^{-1\sigma} F_B,$$

where $F_B : \mathcal{H}(J(C), 2\Theta) \to \mathcal{H}(J(C), 2\Theta_B)$ *is the isomorphism from the remarks preceding Lemma 1.8 of [Tho16].*

Lemma III.43 (Lemma 2.4 of [Tho16])**.** *Let* $\tilde{V}_B$ *be the central extension defined in the proof of Theorem III.*35*. The map*

$$\beta : V_B^\vee \to \mathrm{Aut}(\tilde{V}_B; V_B)$$

given by

$$f \to (\tilde{v} \to (-1)^{f(v)}\tilde{v}),$$

where $\tilde{v}$ *in* $\tilde{V}_B$ *lies above* v *in* V_B*, is an isomorphism of groups.*

Lemma III.44. *Let* $(H_0, \theta_0, T_0, \pi_0)$ *be object of* $\mathcal{L}$ *associated to the trivial bundle* $0 \in J(C)$ *as in Theorem III.35. There is a* Γ_K*-equivariant isomorphism* $\epsilon : V_0^\vee \to T_0[2]$ *satisfying:*

1. *the restriction of of* ϵ *to the image* N_{V_0} *of* V_0 *in* $V_0^\vee$ *induces an isomorphism between* N_{V_0} *and* $(T \cap G)[2]$ *and*

2. *for $f \in V_0^\vee$, let $s = \epsilon(f)$ be the image of f in $T_0[2]$. Via the correspondence in Theorem III.11, the automorphism $\beta(f) \in \mathrm{Aut}(\tilde{V}_B; V_B)$ induces an automorphism F of the triple (H_0, θ_0, T_0) defined over K^s. F is equal to conjugation by s and thus either fixes π_0 or takes π_0 to its dual.*

Proof. 1. This follows from the remarks after the proof of Proposition 2.2 in [Tho16].

2. This is the second part of Lemma 2.4 in [Tho16]. □

Remark III.45. Recall that the divisor classes $D_i = P_{i+1} - P_1$ for $1 \leq i \leq 2g$ form an $\mathbb{F}_2$-basis for $J(C)[2]$. Since the Weil pairing turns $J(C)[2]$ into a symplectic space of dimension $2g$ over $\mathbb{F}_2$, for each D_i there exists a D_i' such that the D_i' form an $\mathbb{F}_2$-basis of $J(C)[2]$ and

$$\langle D_i, D_j' \rangle_{J(C)[2]} = \delta_{i,j}.$$

Lemma III.46. *Define a map $\eta : V_0^\vee \to J(C)[2]$ by*

$$\eta(f) = \sum_{i=1}^{2g} f(E_{i+1} - E_1) D_i'.$$

Then η induces an isomorphism between N_{V_0} and $J(C)[2]$.

Proof. Whether $\Lambda_0 = \Lambda_g'$ or $\Lambda_0 = \Lambda_g''$, we have that N_{V_0} is freely generated by the images $e_j^\vee$ of $e_j = E_j - E_{j+1}$ in $V_0^\vee$ for $2 \leq j \leq 2g+1$. By direct computation, we have that

$$e_j^\vee(E_i - E_1) = \delta_{j+1,i} - \delta j, i.$$

By the formula given in the statement of the lemma, we have

$$\eta(e_2^\vee) = -D_1' + D_2',\ \eta(e_3^\vee) = -D_2' + D_3', ...,\ \eta(e_{2g+1}^\vee) = -D_{2g}'.$$

Therefore the image of the $e_j^\vee$ spans $J(C)[2]$. Since N_{V_0} and $J(C)[2]$ both have 2^{2g} elements, η induces an isomorphism between them. □

Definition III.47. *Let*

$$0 \longrightarrow A \longrightarrow B \xrightarrow{\phi} C \longrightarrow 0$$

be a central extension of groups, let $\psi : C' \to C$ be a surjection, and consider the central extension $\psi^*(B) \cong C' \times_C B$ of C' by A. Given an automorphism f in $\mathrm{Aut}(B; C)$, we define an automorphism $\psi^*(f)$ in $\mathrm{Aut}(\psi^*(B); C')$ by $\psi^*(f)(c', b) = (c', f(b))$. This assignment defines

the pullback map

$$\psi^* : \mathrm{Aut}(B; C) \to \mathrm{Aut}(\psi^*(B); C').$$

Remark III.48. By Lemma III.29, there is a surjection $r : V_B \to J(C)[2]$. This induces a pullback map

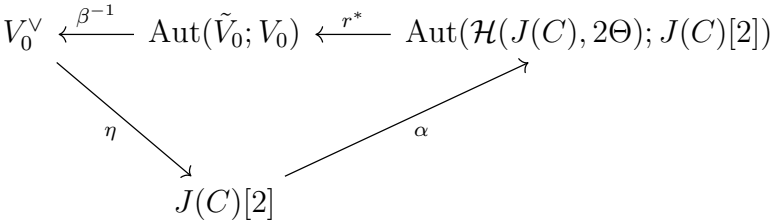
$$r^* : \mathrm{Aut}(\mathcal{H}(J(C), 2\Theta_B); J(C)[2]) \to \mathrm{Aut}(\tilde{E}_B; V_B),$$

where $\tilde{E}_B$ is the central extension of V_B by $\mathbb{G}_m$ defined in the proof of Theorem III.35. Since $\tilde{V}_B$ is by definition the kernel of χ_B in $\tilde{E}_B$, one can check that any automorphism in $\mathrm{Aut}(\tilde{E}_B; V_B)$ restricts to an automorphism in $\mathrm{Aut}(\tilde{V}_B; V_B)$. Therefore r^* yields, by restriction, a map

$$\mathrm{Aut}(\mathcal{H}(J(C), 2\Theta_B); J(C)[2]) \to \mathrm{Aut}(\tilde{V}_B; V_B),$$

which by abuse of notation we also call r^* in what follows.

Lemma III.49. *Going around the diagram*



induces the identity on $J(C)[2]$.

Proof. Suppose that we have an element ν in $J(C)[2]$. For an element $(\omega, \psi) \in \mathcal{H}(J(C), 2\Theta)$, we have by definition

$$\alpha(\nu).(\omega, \psi) = (\omega, (-1)^{\langle \nu, \omega \rangle} \psi).$$

For $(v, (\omega, \psi)) \in \tilde{V}_0 \subset r^*(\mathcal{H}(J(C), 2\Theta))$, we also have by definition

$$r^*(\alpha(\nu)).(v, (\omega, \psi)) = (v, \alpha(\nu).(\omega, \psi)) = (v, (\omega, (-1)^{\langle \nu, \omega \rangle} \psi)).$$

Note by the definition of $r^*(\mathcal{H}(J(C), 2\Theta))$ that we have $r(v) = \omega$. Thus by the definition of β, we have that $b^{-1}(r^*(\alpha(\nu)))$ in $V_0^\vee$ is the linear functional f_ν on V_0 which sends $v \in V_0$ to $\langle r(v), \nu \rangle$. Now by the definition of η, we have

$$\eta(b^{-1}(r^*(\alpha(\nu)))) = \eta(f_\nu) = \sum_{i=1}^{2g} f_\nu(E_{i+1} - E_1) D_i'$$

$$= \sum_{i=1}^{2g} \langle r(E_{i+1} - E_1), \nu \rangle D_i' = \sum_{i=1}^{2g} \langle D_i, \nu \rangle D_i' = \nu,$$

and this completes the proof. □

Definition III.50. *Let $\epsilon : V_0^\vee \to T_0[2]$ and $\eta : V_0^\vee \to J(C)[2]$ be as in the statement of Lemmas III.44 and III.46.*

We define a map δ from $Z_{G_0} \subset T_0[2]$ to $J(C)$ by

$$\delta := \eta \circ \epsilon^{-1}.$$

Lemma III.51. *The map δ is an isomorphism.*

Proof. By Lemma III.44, the map ϵ maps N_{V_0} isomorphically onto Z_{G_0}. By Lemma III.46, the map η maps N_{V_0} isomorphically onto $J(C)[2]$. □

Proof of Theorem III.38. We start by proving the claim for κ_C.

The isomorphism

$$\phi : G_0 \backslash V_{\kappa_C} \to \ker(\gamma : H^1(K, (G_0)_{\kappa_C}) \to H^1(K, G_0))$$

which sends κ_C to the zero cocycle sends $\psi^{-1}(\kappa_{C,B})$ to $s^{-1\sigma}s$, where $\psi^{-1} \circ \mathcal{F}_B$ is equal to conjugation by s, as in the proof of Lemma III.37.

By Lemma III.41, we have that $\alpha(B^\sigma - B) = F_B^{-1\sigma} \circ F_B$. Note that $\mathcal{F}_B^{-1\sigma} \circ \mathcal{F}_B$ is exactly the automorphism of H_0 induced by $r^*(\alpha(B^\sigma - B)) = r^*(F_B^{-1\sigma} \circ F_B)$, and that since ψ is defined over K, we have

$$(\psi^{-1} \circ \mathcal{F}_B)^{-1\sigma} \circ (\psi^{-1} \circ \mathcal{F}_B) = \mathcal{F}_B^{-1\sigma} \circ \mathcal{F}_B.$$

By this last equality, we have that $\mathcal{F}_B^{-1\sigma} \circ \mathcal{F}_B$ is equal to conjugation by $s^{-1\sigma}s$.

By Lemma III.44, we have that $s^{-1\sigma}s = \epsilon(r^*(\alpha(B^\sigma - B))$, and by the proof of Lemma III.37, s lies in G_0. By Lemma III.49, we have that $\eta(r^*(\alpha(B^\sigma - B))) = B^\sigma - B$.

Finally, we have that

$$\delta(s^{-1\sigma}s) = \eta(\epsilon^{-1}(s^{-1\sigma}s)) = \eta(r^*(\alpha(B^\sigma - B))) = B^\sigma - B,$$

which completes the proof.

The same argument works for μ_C since the stabilizer subgroups of κ_C and of μ_C in G_0 are equal by Lemma III.39. □

III.11: Construction of Descent Maps

In this section, we construct 2-descent maps from the Jacobians $J(C)$ over our curves C into the orbit spaces of the local and global Vinberg representations arising from our surfaces S and prove Theorem I.5.

Theorem III.52. *Suppose that $v = (C, P, t)$ is a point in $\mathcal{S}_n(K)$. The map $v \to \kappa_C$ can be extended to an injective map*

$$i_C : J(C)/2J(C)(K) \to G_0\backslash V_{0,\kappa_C}(K)$$

sending 0 to κ_C. If v is in $\mathcal{S}_n^0(K)$, the map $v \to \mu_C$ can be extended to an injective map

$$I_C : J(C)/2J(C)(K) \to G_0\backslash Y_{0,\mu_C}(K),$$

sending 0 to μ_C.

Here V_0 is the -1 eigenspace of $d\theta$ in $\mathfrak{g}_0$ and Y_0 is the identity component of the subvariety $\theta(g) = g^{-1}$ in G_0, and where for a K-variety X on which a group G acts X_p denotes the set of points of X which lie in the same $G(K^s)$-orbit as $p \in X$.

Proof of Theorem III.52. First, we construct i_c.

Given a rational point $A \in J(C)(K)$, choose a point $B \in J(C)(K^s)$ such that $2B = A$. We define $i_C(A) \in X_0$ to be $\psi^{-1}(\kappa_{C,B})$, where $\psi : H_0 \to H_B$ is the map of Lemma IV.7; then $i_C(A)$ is well-defined up to G_0-conjugacy.

By Lemma III.37, this is in the G_0 orbit of κ_C over K^s. By Theorem III.38, this is the orbit corresponding to the cocycle $\sigma \to B^\sigma - B$. Since this coycle is the image of A in the injection $J(C)/2J(C) \to H^1(K, J(C)[2])$, it depends only on A and not the choice of B and further is an injection.

To construct I_C, we simply replace κ_C by μ_C in the preceding argument. □

Proof of Theorem I.5. The data referenced in the Theorem are defined throughout the chapter. Their properties are proved in Theorem III.52. □

CHAPTER IV
Decomposable Transformations and the Orbit Problem for D_n

IV.1: Introduction

Let K be a field of characteristic 0 with separable closure K^s. For a simple, split adjoint Lie algebra of type D_n, where n is odd, the local Vinberg representation of degree 2 is the group $G = \mathrm{SO}(V) \times \mathrm{SO}(V)$, where V is an orthogonal space of dimension $n = 2m + 1$ with index of isotropy $i(V) = 2m$ and discriminant 1, acting on the space $\mathrm{End}(V)$ with the action $(a, b) \cdot T = aTb^*$.

The invariant polynomials of this action are the degree 1 through $n-1$ coefficients f_{2j} of the characteristic polynomial of $T \circ T^*$, where T^* is the adjoint of T, plus the determinant g_n of T. Let $\mathbf{f}_T = (f_2, ..., f_{2(n-1)}, g_n)$ be the vector of invariants of T. When K is algebraically closed (but not in general), these invariants completely determine the orbit of T, assuming T is stable. The orbit of T is associated to a hyperelliptic curve $C_{\mathbf{f}_T}$, namely the projective completion of the affine plane curve

$$y(xy + g_n) = x^{n-1} + f_2 x^{n-2} + ... + f_{2(n-1)}. \tag{IV.1.1}$$

This curve is isomorphic to the projective completion of the affine plane curve

$$y^2 = x^n + f_2 x^{n-1} + ... + f_{2(n-1)} x + g_n^2. \tag{IV.1.2}$$

The curve has a marked Weierstrass point lying above $x = \infty$ and a marked non-Weierstrass point, which corresponds to the point $(0, g_n)$.

The goal of this chapter is to prove Theorem I.6, i.e., construct an injective map from the set $J(C_{\mathbf{f}_T})/2J(C_{\mathbf{f}_T})$ into the set of K-orbits $[T']$ of G acting on V satisfying the condition $\mathbf{f}_{T'} = \mathbf{f}_T$. This yields a kind of explicit 2-descent on $J(C_{\mathbf{f}_T})$.

Various constructions used in the A_n case and found in [Tho14] can also be applied in

our D_n case. We recall some relevant facts, which are found in that article. The relevant terminology is also reviewed in the next section. Let C be a hyperelliptic curve given by the equation

$$y^2 = x^n + c_1 x^{n-1} + ... + c_n = f(x). \tag{IV.1.3}$$

Let $\mathcal{W}$ be the sublocus of C given by the non-infinite ramification points of C. To each degree zero line bundle $\mathcal{L}$ on C we associate the m-dimensional vector space $\mathcal{V} = H^0(\mathcal{W}, \mathcal{L})$. There exists a symmetric bilinear form $\langle \cdot, \cdot \rangle$ on $\mathcal{V}$ with respect to which $\mathcal{V}$ is a split orthogonal space of discriminant 1 and maximal index of isotropy and multiplication by x is a self-adjoint linear transformation, denoted by T_x.

We will prove the following theorem.

Theorem IV.1 (Decomposition Theorem)**.** *Using the notation above, in the case where the constant term of $f(x)$ is a non-zero square c^2 in K, there exists a linear transformation S_x of $\mathcal{V}$ defined over K such that T_x has the decomposition*

$$T_x = S_x \circ S_x^*.$$

For a given x, the set of all such S_x's breaks into two $\mathrm{SO}(\mathcal{V}) \times \mathrm{SO}(\mathcal{V})$ orbits, one with determinant c and the other with determinant $-c$.

The assumption that c^2 is non-zero does not change the moduli objects parameterized; the constant term can always be made non-zero by a shift in x, and this simply changes the coordinate of one of the marked points.

After proving the Decomposition Theorem, we use it to give a proof of Theorem I.5. Note that Decomposition Theorem is true regardless of the parity of n but Theorem I.5 assumes that n is odd; we will say more about this assumption later in the chapter.

IV.2: Preliminary Notions

We first define some preliminary notions and notations, starting with some generalities on orthogonal spaces.

Definition IV.2. *An* orthogonal space *is a k-vector space V of dimension n together with a non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$. We often treat the form as implicitly and simply state that V is an orthogonal space.*

Example IV.3. *The space $V = \mathbb{R}^n$ endowed with the Euclidean inner product is an orthogonal space over $\mathbb{R}$.*

Definition IV.4. *Let V be an orthogonal space and T a linear transformation on V. T is called* decomposable *if there exists a linear transformation S defined over K such that $T = S \circ S^*$.*

From this definition, it follows that a decomposable transformation T must be self-adjoint, and its determinant must be a square in K. At the same time, not every linear transformation with these properties is decomposable, as the following example shows.

Example IV.5. *Consider the orthogonal space $\mathbb{Q}^2$ endowed with the standard inner product $\langle e_i, e_j \rangle = \delta_{ij}$. The transformation represented by the matrix $\left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ has determinant 1 and is self-adjoint (which in this case is the same as the matrix being symmetric), but it is not decomposeable since any matrix of the form $\mathbf{M}\mathbf{M}^T$ has non-negative entries on its diagonal.*

The following two lemmas state fundamental properties of decompsable transformations.

Lemma IV.6. *An invertible transformation T has a decomposition $T = P \circ P^*$ if and only if there exists a transformation R such that $R \circ T \circ R^* = I$.*

Proof. Simply set $R = P^{-1}$ (since T and I are invertible, P and R must be invertible as well). □

Lemma IV.7. *Let T be an invertible transformation. Suppose the transformation A satisfies $A \circ A^* = T$. Then B satisfies $T = B \circ B^*$ and has the same determinant as A if and only if A and B are in the same orbit of $\mathrm{SO}(V)$ acting on the right.*

Proof. The "if" direction follows directly from the relevant definitions. We now address the "only if" direction.

By Lemma IV.6, there exists a transformation R such that $R \circ T \circ R^* = I$. Then we have $(RA)(RA)^* = I = (RB)(RB)^*$. This shows that RA and RB are both in $O(V)$. Since A and B have the same determinant, RA and RB either both have determinant 1 or determinant -1, so they are in the same $\mathrm{SO}(V)$-right orbit. □

As stated earlier, we aim to prove decomposability for a certain class of transformations. We now study decomposability on split orthogonal spaces of discriminant 1, a category which the spaces we are interested in belong to.

Definition IV.8. *Let V be an orthogonal space. We define the* determinant *of V to be the class $\det(V)$ in $K^\times/(K^\times)^2$ given by the determinant of any matrix $\mathbf{M}$ which represents the form $\langle \cdot, \cdot \rangle$, i.e., such that $\mathbf{M}_{ij} = \langle e_i, e_j \rangle$ for some basis $\{e_k\}$ of V. We define the* discriminant *of V to be the class $\mathrm{disc}(V)$ in $K^\times/(K^\times)^2$ given by $(-1)^{\frac{n(n-1)}{2}} \det(V)$.*

Example IV.9. *Let $V = \mathbb{Q}^2$ be endowed with the basis $\mathcal{B} = \{(1,0),(0,1)\}$. Let $\langle \cdot, \cdot \rangle$ be the bilinear form which is represented relative to $\mathcal{B}$ by the matrix*

$$\begin{bmatrix} 7 & 1 \\ 2 & 3 \end{bmatrix}.$$

The determinant and discriminant of V in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ are, respectively, 19 *and* $[-19]$.

Definition IV.10. *Let V be an orthogonal space of dimension $n = 2m$. We say that V is* split *if it has an isotropic subspace of dimension m.*

Definition IV.11. *An orthogonal space V is* anisotropic *if there are no non-zero vectors v satisfying $\langle v, v \rangle = 0$.*

Example IV.12. *The Euclidean space $\mathcal{V} = \mathbb{R}^6$ is anisotropic and is not split; there are no non-zero isotropic vectors.*

The following theorem is a summary of the results in Chapter 3, Section 1 of [MH73].

Theorem IV.13. *Suppose that V is an orthogonal space. There exists an orthogonal decomposition*

$$V = S \oplus A,$$

where S is split and A is anisotropic. The dimension of S satisfies

$$\dim(S) = 2i(V),$$

where $i(V)$ is the index of isotropy of V, i.e., the dimension of the largest isotropic subspace of V. Note that the index of isotropy is thus at most $\frac{\dim V}{2}$.

We will be interested in split orthogonal spaces. The following lemma shows that split orthogonal spaces of discriminant 1 have a very simple structure.

Lemma IV.14. *Every orthogonal space V of dimension $n = 2m + 1$ with index of isotropy $2m$ and discriminant 1 has a basis $\{e_1, ..., e_k, g, f_k, ..., f_1\}$ satisfying $\langle e_i, f_i \rangle = 1$, $\langle g, g \rangle = 1$, and all other products of basis elements equal to 0.*

Every split orthogonal space V of dimension $n = 2m$ and discriminant 1 has a basis $\{e_1, ..., f_1\}$ satisfying $\langle e_i, f_i \rangle = 1$ and all other products of basis elements equal to 0.

Proof. The case $n = 2m$ follows directly from [MH73, CH. 1, 6.3] (note that this shows something even stronger - that every split orthogonal space has discriminant 1). The case $n = 2m + 1$ follows from applying, in addition, [MH73, CH. 3, 1.1]. □

Definition IV.15. *If V is an orthogonal space with maximal index of isotropy and discriminant* 1*, we call a basis of V satisfying the properties given in the preceding lemma a* standard split basis.

If T is a linear transformation on V and $\mathbf{M}_T$ is its matrix with respect to a standard split basis, then the matrix $\mathbf{M}_{T^*}$ is given by reflecting the entries of $\mathbf{M}_T$ over the antidiagonal.

There is an alternate way of giving matrix representations of symmetric bilinear forms that is more suitable when studying split spaces; it is formalized in the following definition and lemma.

Definition IV.16. *Suppose that V is an orthogonal space. Two linear transformations T and S on V are* similar *if there exists an invertible linear transformation P on V such that $T = P^*SP$.*

Remark IV.17. The order of P and P^* can be reversed in the preceding definition, but the one we use corresponds to the way bilinear forms transform under a change of basis.

Lemma IV.18. *Let V be a K-vector space of dimension $n = 2m$ and $B : V \times V \to k$ be a bilinear form on V. Let $\mathcal{B} = \{b_1, ..., b_m, c_m, ..., c_1\}$ be a basis for V, and consider the matrix*

$$\mathbf{M} = \begin{bmatrix} B(c_1,b_1) & ... & B(c_1,b_m) & B(c_1,c_m) & ... & B(c_1,c_1) \\ ... & ... & ... & ... & ... & ... \\ B(c_m,b_1) & ... & B(c_m,b_m) & B(c_m,c_m) & ... & B(c_m,c_1) \\ B(b_m,b_1) & ... & B(b_m,b_m) & B(b_m,c_m) & ... & B(b_m,c_1) \\ ... & ... & ... & ... & ... & ... \\ B(b_1,b_1) & ... & B(b_1,b_m) & B(b_1,c_m) & ... & B(b_1,c_1) \end{bmatrix}$$

We say that $\mathbf{M}$ represents B in the split sense relative to $\mathcal{B}$. If $\mathcal{B}' = \{b'_1, ..., c'_1\}$ is another basis for V and $\mathbf{M}'$ represents B relative to $\mathcal{B}'$, then we have the equality

$$\mathbf{M}' = \mathbf{P}^*\mathbf{M}\mathbf{P},$$

where $\mathbf{P}$ is the change of basis matrix from $\mathcal{B}'$ to $\mathcal{B}$ and $\mathbf{P}^*$ is obtained from $\mathbf{P}$ by reflection across the antidiagonal.

An analogous statement is true when the dimension $n = 2m + 1$ is odd.

Proof. The proof is by direct computation of the matrices $\mathbf{M}$ and $\mathbf{M}'$ (see the example below). □

Example IV.19. *Let $V = \mathbb{Q}^2$, and consider the quadratic form given by $Q((x, y)) = x^2 + y^2$. The matrix representing Q in the split sense relative to $\{(1, 0), (0, 1)\}$ is $\left[\begin{smallmatrix} 0 & 2 \\ 2 & 0 \end{smallmatrix}\right]$. Define the*

vectors $b_1 = (1, 7)$ *and* $c_1 = (1, 2)$*, and let* $\mathcal{B}$ *be the basis* $\mathcal{B} = \{b_1, c_1\}$*. The following identities come from direct computation*

$$B(b_1, c_1) = 30, B(b_1, b_1) = 100, B(c_1, c_1) = 10.$$

In addition, we can verify directly the equation

$$\begin{bmatrix} 30 & 10 \\ 100 & 30 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 7 & 1 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 7 & 2 \end{bmatrix}.$$

Lemma IV.20. *Let* $(V, \langle \cdot, \cdot \rangle)$ *be an orthogonal space. We have that*

$$\operatorname{disc}(V) = \det(\mathbf{M}),$$

where $\mathbf{M}$ *is any matrix which represents* $\langle \cdot, \cdot \rangle$ *in the split sense.*

Proof. The proof is by direct computation. □

Next we move on to developing a decomposability criteria for invertible, self-adjoint transformations T on orthogonal spaces with maximal index of isotropy and discriminant 1. We will find it helpful to think of these transformations as symmetric bilinear forms, in the vein of the next lemma.

Lemma IV.21. *Let* $(V, \langle \cdot, \cdot \rangle)$ *be an orthogonal space, and let* T *be an invertible self-adjoint transformation on* V*. Let* $\mathcal{T} = (\cdot, \cdot)$ *be the bilinear form on* V *given by* $(v, w) = \langle v, Tw \rangle$*. Then* $(V, \mathcal{T})$ *is an orthogonal space.*

Further, suppose V *has maximal index of isotropy and* $\mathcal{B}$ *is a standard split basis of* V*. Let* $\mathbf{M}_T$ *be the matrix representing* T *with respect to* $\mathcal{B}$ *and* $\mathbf{M}_{\mathcal{T}}$ *be the matrix representing the form* $\mathcal{T}$ *with respect to* $\mathcal{B}$*. Then* $\mathbf{M}_T = \mathbf{M}_{\mathcal{T}}$*.*

Proof. The form $\mathcal{T}$ is symmetric since T is self-adjoint with respect to $\langle \cdot, \cdot \rangle$ and it is non-degenerate since T is invertible. The claim in the second paragraph follows directly by writing down both matrices. □

Lemma IV.22 ([MH73])**.** *Let* $(V, \langle \cdot, \cdot \rangle)$ *be an orthogonal space of dimension* $n = 2m$ *or* $n = 2m + 1$ *which contains a split subspace of dimension* $2m$*, and let* $\mathcal{B}$ *be a standard split basis of* V*. Suppose* T *is an invertible self-adjoint transformation on* V *such that*

1. *the symmetric form* $\mathcal{T} = (\cdot, \cdot) = \langle \cdot, T(\cdot) \rangle$ *turns* V *into an orthogonal space of dimension* n *which contains a split subspace of dimension* $2m$ *and*

2. the discriminant of $\mathcal{T}$ is 1.

Let $\mathbf{M}_T$ be the matrix representing T in the split sense with respect to $\mathcal{B}$. Recall by the previous Lemma that $\mathbf{M}_T = \mathbf{M}_{\mathcal{T}}$ Then there exists a matrix $\mathbf{R}$ such that

$$\mathbf{R}\mathbf{M}_T\mathbf{R}^* = I_n.$$

Proof. The case $n = 2m$ follows directly from [MH73, CH. 1, 6.3], with the modification that $\mathbf{M}_T = \mathbf{M}_T$ is the matrix representing $\mathcal{T}$ in the split sense rather than in the traditional sense.

For the case $n = 2m + 1$, we apply [MH73, CH. 3, 1.1] to argue that $(V, \mathcal{T})$ can be written $V = S \oplus A$, where S is split with respect to $\mathcal{T}$ of dimension $2m$ and A is anisotropic of dimension 1. Applying [MH73, CH. 1, 6.3] to S, we have that there exists a basis $\mathcal{B}'$ of V such that the matrix representing $\mathcal{T}$ in the split sense with respect to $\mathcal{B}'$ is of the form

$$\begin{bmatrix} I_m & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & I_m \end{bmatrix}.$$

Since the discriminant of $\mathcal{T}$ is 1, we may choose our basis so that C is equal to 1. Thus there exists a matrix $\mathbf{R}$ such that

$$\mathbf{R}\mathbf{M}_{\mathcal{T}}\mathbf{R}^* = I_n.$$

□

IV.3: Reduction to the Trivial Bundle Case

In this section, we show that we may reduce the proof of Theorem IV.1 to the case $\mathcal{V} = H^0(\mathcal{W}, \mathcal{O}_C) = K[x]/f(x)$. It will be useful to use the notation $A = K[x]/f(x)$, and to consider the vector spaces $H^0(\mathcal{W}, \mathcal{L})$ as free, 1-dimensional A-modules. The idea is that for any line bundle $\mathcal{L}$, the space $H^0(\mathcal{W}, \mathcal{L})$ of global sections has an orthogonal space structure which comes from its A-module structure.

We begin by defining an orthogonal space structure on the base space A.

Definition IV.23. *We define the A-valued bilinear form $(\cdot, \cdot)_A$ on A by $(g(x), h(x))_A = g(x)h(x)$. Suppose that the degree of f is n. We define the k-linear functional $\tau : A \to k$ on the k-basis $\{1, x, ..., x^{n-1}\}$ by $\tau(x^m) = \delta_{n-1}(x^m)$; that is, τ takes sends a polynomial to the coefficient of x^{n-1} in the polynomial. Finally, we define the k-valued bilinear form $\langle \cdot, \cdot \rangle_A$ on A by $\langle \cdot, \cdot \rangle_A = \tau \circ (\cdot, \cdot)_A$.*

Lemma IV.24. *The bilinear form $\langle \cdot, \cdot \rangle_A$ is non-degenerate and thus gives A an orthogonal space structure. Further, A has maximal index of isotropy.*

Proof. If $g(x)$ is a polynomial (class) of degree $0 \leq m < n$, then $\langle g(x), x^{n-1-m} \rangle_A \neq 0$, so that $\langle \cdot, \cdot \rangle_A$ is non-degenerate. If $n = 2m + 1$ or $n = 2m$ the subspace $\{1, x, ..., x^{m-1}\}$ is isotropic and of dimension m. □

Next, we define the orthogonal space structure on free, 1-dimensional A-modules M.

Definition IV.25. *Suppose that M is an A-module with an isomorphism $F : M \to A$. Define a k-valued bilinear form on M by $\langle \cdot, \cdot \rangle_M = \langle F(\cdot), F(\cdot) \rangle_A$.*

It follows directly from the definition that $\langle \cdot, \cdot \rangle_M$ gives M the structure of a split orthogonal space, and that F is both an isomorphism of A-modules and of orthogonal spaces. We derive some basic properties of the form $\langle \cdot, \cdot \rangle_M$ which we will use later.

Lemma IV.26. *Suppose that $S : A \to A$ is a linear transformation. Then we have an equality*

$$(F^{-1} \circ S \circ F)^* = (F^{-1} \circ S^* \circ F)$$

of maps on the orthogonal space M.

Proof. Since F is an isomorphism of orthogonal spaces, for any x, y in M we have the equalities

$$\langle (F^{-1} \circ S^* \circ F)(x), y \rangle_M = \langle (S^* \circ F)(x), F(y) \rangle_A = \langle F(x), (S \circ F)(y) \rangle_A$$

$$= \langle x, (F^{-1} \circ S \circ F)(y) \rangle_M.$$

Since this holds for arbitrary x, y, we obtain $(F^{-1} \circ S \circ F)^* = (F^{-1} \circ S^* \circ F)$. □

Lemma IV.27. *Suppose that g is an element of A, T_g denotes the multiplication by g map on A, and T'_g denotes the multiplication by g map on M. Then we have an equality of maps*

$$(F^{-1} \circ T_g \circ F) = T'_g.$$

Proof. Using the fact that all maps involved are morphisms of A-modules, we have for any x in M the equalities

$$(F^{-1} \circ T_g \circ F)(x) = (F^{-1} \circ T_g)(F(x)) = F^{-1}(g.F(x)) = g.(F^{-1}(F(x))) = g.x = T'_g(x).$$

Since this holds for any x in M, we have $(F^{-1} \circ T_g \circ F) = T'_g$. □

There are many orthogonal space structures on M varying by the choice of isomorphism F and they are all isomorphic, but for the A-modules we are interested in, which are global sections of line bundles, there is one particular orthogonal space structure we are interested in which is easily computable based on data from C. This structure is used in [Tho14]; while we do not need to work with it directly for our proofs, we include it here so that our arguments are in principle all effective (the proofs we cite from [MH73] being already all effective).

Let C be a hyperelliptic curve cut out by the equation $y^2 = x^n + f_1 x^{n-1} + ... + f_n$. Let $\mathcal{W}$ be the sublocus of non-infinite branch points on C. Given a degree 0 line bundle $\mathcal{L}$ on C, let $\mathcal{V}$ be the vector space $H^0(\mathcal{W}, \mathcal{L})$. We recall the following useful facts related to $\mathcal{V}$, which we will illustrate later by example.

Lemma IV.28 (Mumford Representation, see Lemma 3.2 of [Tho14])**.** *Any degree 0 line bundle $\mathcal{L}$ on C can be written in the form $\mathcal{L} = (mP_\infty - D)$, where $m \leq n$ and D is an effective divisor such that*

1. *no K-basepoint of D is equal to P_∞ and*
2. *no two K-basepoints of D are related under the involution of C.*

Lemma IV.29 (see Lemma 4.4 of [Tho14])**.** *Let P and D be as in Lemma IV.28. There exists a triplet (U, V, R) of polynomials in $k[x]$ satisfying the following properties.*

1. *the degree of U is m and the degree of V is $2n - m$,*
2. *the degree of R is no more than $m - 1$,*
3. *the equality $f = UV - R$ holds,*
4. *the set $\{U, xU, ..., x^{2n-m-1}U, (y - R), x(y - R), ..., x^{m-1}(y - R)\}$ is a basis of $\mathcal{V} = H^0(\mathcal{W}, \mathcal{L})$,*
5. *there exists an isomorphism $F : \mathcal{V} \to A$ such that the dot product $\square \cdot \square : \mathcal{V} \times \mathcal{V} \to A$ defined by $a \cdot b = F(a)F(b)$ is given by the following identities:*

$$x^i U \cdot x^j U = x^{i+j} U, x^i U \cdot x^j (y - R) = -x^{i+j} R, x^i (y - R) \cdot x^j (y - R) = -x^{i+j} V.$$

Example IV.30. *Let C be the genus 2 hyperelliptic curve defined by the affine equation*

$$y^2 = x(x^4 + x^3 + x^2 + x).$$

Let $P_0 = (0,0)$. Consider the line bundle $\mathcal{L} = P_\infty - P_0$. The Mumford Representation (U, V, R) is given by

$$U = x,\ V = x^4 + x^3 + x^2 + x,\ R = 0.$$

By Lemma IV.29, a basis of $\mathcal{V} = H^0(\mathcal{W}, \mathcal{L})$ is given by

$$e_1 = U,\ e_2 = xU,\ e_3 = x^2U,\ e_4 = x^3U,\ e_5 = y,$$

and the A-valued matrix of the dot product is

$$\begin{bmatrix} U & xU & x^2U & x^3U & 0 \\ xU & x^2U & x^3U & x^4U & 0 \\ x^2U & x^3U & x^4U & x^5U & 0 \\ x^3U & x^4U & x^5U & x^6U & 0 \\ 0 & 0 & 0 & 0 & -V \end{bmatrix}.$$

It follows by direct computation that the k-valued matrix of $\langle \cdot, \cdot \rangle_{\mathcal{V}}$ is

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 1 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix}.$$

Theorem IV.31. *Assume that the linear transformation given by multiplication by x is decomposable on A. If M is a free, 1-dimensional A-module, then multiplication by x is a decomposable linear transformation on M.*

Proof. Fix the isomorphism $F : M \to A$. Let $T_x : A \to A$ denote the multiplication by x map on A, and T'_x denote the multiplication by x map on M. By Lemma IV.27, we have $F^{-1} \circ T_x \circ F = T'_x$. Given a decomposition $T_x = S \circ S^*$, by Lemma IV.26, we have the equalities

$$F^{-1} \circ T_x \circ F = F^{-1} \circ S \circ S^* \circ F = F^{-1} \circ S \circ F \circ F^{-1} \circ S^* \circ F$$

$$= (F^{-1} \circ S \circ F) \circ (F^{-1} \circ S \circ F)^* = T'_x,$$

which shows that multiplication by x is a decomposable linear transformation on M. □

IV.4: Proof of Theorem IV.1

We now turn to the proofs of our main results. For an orthogonal space V, we fix a left action of $\mathrm{SO}(V)$ on $\mathrm{End}(V)$ acting by left multiplciation, a right action of $\mathrm{SO}(V)$ on $\mathrm{End}(V)$ acting by right adjoint multiplication, and an action of $G = \mathrm{SO}(V) \times \mathrm{SO}(V)$ on $\mathrm{End}(V)$ given by $(a, b) \cdot T = a \circ T \circ b^*$.

Lemma IV.32. *Suppose that $f(0) \neq 0$ $n = 2m$ or $n = 2m + 1$. Let $\mathcal{T}_x$ be the symmetric form associated to the self-adjoint transformation T_x on $\mathcal{V} = K[x]/f(x)$. The space $(\mathcal{V}, \mathcal{T}_x)$ is an orthogonal space containing a split orthogonal subspace S of dimension $2m$.*

Proof. If $n = 2m + 1$, we can see directly that the subspace $\{1, x, ..., x^{m-1}\}$ is a dimension m subspace isotropic with respect to $\mathcal{T}_x$. By Theorem IV.13, the index of isotropy $i(\mathcal{V})$ is at most m, so we have $i(\mathcal{V}) = m$. By applying that theorem again, we see that $(\mathcal{V}, \mathcal{T}_x)$ contains a split orthogonal subspace of dimension $2m$.

If $n = 2m$, we can similarly see that the subspace

$$\{1, x, ..., x^{m-1} + \frac{a_{m-1}}{2} x^{m-2}\},$$

where a_i is the coefficient of x^i in $f(x)$, is a dimension m subspace isotropic with respect to $\mathcal{T}_x$. The rest of the proof is similar to the odd case. □

Proof of Theorem IV.1. By Lemma IV.22, there exists a transformation R such that $R \circ T_x \circ R^* = I$. By Lemma IV.6, T_x is decomposable. By Lemma IV.7, the set of all S's such that $T_x = S \circ S^*$ breaks into two $\mathrm{SO}(\mathcal{V})$ right-orbits, one with determinant c and the other with determinant $-c$. □

Proof of Theorem I.6. Suppose we have a polynomial $f(x) = x^{2m+1} + a_{2m}x^{2m} + ... + a_1 x + c^2$ such that $c \neq 0$ and $\Delta(f) \neq 0$. Let C be the hyperelliptic curve of genus g given by

$$y^2 = f(x).$$

By [Tho14, Theorem 4.6], there is an injection.

$$\phi : J(C)/2J(C)(K) \to \mathrm{SO}(V) \backslash \mathrm{End}(V),$$

Following the proof in that article and applying our Theorem IV.1, we see that the image of ϕ lies in the space of decomposable matrices of determinant c^2 (it consists of orbits of endomorphisms of the form T_x).

For each $[A] \in J(C)/2J(C)(K)$, let T_A be an endomorphism in the class of $\phi([A])$. We define $\psi([A])$ to be the unique $G(K)$-orbit of a transformation S such that $\phi([A]) = S \circ S^*$ and S has determinant c.

First, we show this is independent of the choice of representative T_A in the orbit $\phi([A])$. If T_A and T'_A are in the same orbit, then we have $T_A = aT'_Aa^*$ for some $a \in \mathrm{SO}(V)$. Therefore if S and S' satisfy $S \circ S^* = T_A$ and $S' \circ (S')^* = T'_A$, then we have that $(aS') \circ (aS')^* = T_A$ and aS' and S both have determinant c. By Theorem IV.1, we have that there exists an element $b \in \mathrm{SO}(V)$ such that $aS'b^* = S$.

Lastly, we show that ψ is injective. Suppose that $[A]$ and $[A']$ in $J(C)/2J(C)(K)$ satisfy $\psi([A]) = \psi([A'])$. Let S_A and $S_{A'}$ be representatives for the orbits $\psi([A])$ and $\psi([A'])$, respectively. By assumption, there exists $(a, b) \in G = \mathrm{SO}(V) \times \mathrm{SO}(V)$ such that

$$S_A = aS_{A'}b^*.$$

Therefore we have that $T_A = S_A \circ (S_A)' = aT_{A'}a^*$, so that $\phi([A]) = \phi([A'])$. Since ϕ is injective, we have that $[A] = [A']$. □

In [Tho14], the author constructs for each $[A]$ a self-adjoint transoformation T_A in an orthogonal space V of discriminant 1 and maximal index of isotropy. This transformation is well-defined up to a choice of basis of V, so T_A is well-defined up to conjugation by $\mathrm{O}(V)$. Since n is assumed to be odd, the $\mathrm{O}(V)$ orbits are the same as the $\mathrm{SO}(V)$ orbits; when n is even, this is no longer the case, so that the analogous argument does not work.

BIBLIOGRAPHY

[Bea96] Arnaud Beauville. *Complex algebraic surfaces*, volume 34 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, second edition, 1996. Translated from the 1978 French original by R. Barlow, with assistance from N. I. Shepherd-Barron and M. Reid.

[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. In *Automorphic representations and L-functions*, volume 22 of *Tata Inst. Fundam. Res. Stud. Math.*, pages 23–91. Tata Inst. Fund. Res., Mumbai, 2013.

[BG14] Manjul Bhargava and Benedict H. Gross. Arithmetic invariant theory. In *Symmetry: representation theory and its applications*, volume 257 of *Progr. Math.*, pages 33–54. Birkhäuser/Springer, New York, 2014.

[BL04] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.

[Che55] Claude Chevalley. Invariants of finite groups generated by reflections. *Amer. J. Math.*, 77:778–782, 1955.

[CT13] Anna Cadoret and Akio Tamagawa. Note on torsion conjecture. In *Geometric and differential Galois theories*, volume 27 of *Sémin. Congr.*, pages 57–68. Soc. Math. France, Paris, 2013.

[Dol82] Igor Dolgachev. Weighted projective varieties. In *Group actions and vector fields (Vancouver, B.C., 1981)*, volume 956 of *Lecture Notes in Math.*, pages 34–71. Springer, Berlin, 1982.

[Hum72] James E. Humphreys. *Introduction to Lie algebras and representation theory*. Graduate Texts in Mathematics, Vol. 9. Springer-Verlag, New York-Berlin, 1972.

[Kul17] Avinash Kulkarni. An arithmetic invariant theory of curves from e_8. `https://arxiv.org/abs/1711.08843`, 2017.

[Lag22] Jef Laga. Graded lie algebras, compactified jacobians and arithmetic statistics. `https://arxiv.org/abs/2204.02048`, 2022.

[Loo93] Eduard Looijenga. Cohomology of $\mathcal{M}_3$ and $\mathcal{M}_3^1$. In *Mapping class groups and moduli spaces of Riemann surfaces (Göttingen, 1991/Seattle, WA, 1991)*, volume 150 of *Contemp. Math.*, pages 205–228. Amer. Math. Soc., Providence, RI, 1993.

[Maz86] Barry Mazur. Arithmetic on curves. *Bull. Amer. Math. Soc. (N.S.)*, 14(2):207–259, 1986.

[MH73] John Milnor and Dale Husemoller. *Symmetric bilinear forms*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73. Springer-Verlag, New York-Heidelberg, 1973.

[Pan05] Dmitri I. Panyushev. On invariant theory of θ-groups. *J. Algebra*, 283(2):655–670, 2005.

[Rei97] Miles Reid. Chapters on algebraic surfaces. In *Complex algebraic geometry (Park City, UT, 1993)*, volume 3 of *IAS/Park City Math. Ser.*, pages 3–159. Amer. Math. Soc., Providence, RI, 1997.

[Ric82] R. W. Richardson. Orbits, invariants, and representations associated to involutions of reductive groups. *Invent. Math.*, 66(2):287–312, 1982.

[Rom21] Beth Romano. On central extensions and simply laced Lie algebras. *J. Algebra*, 568:480–511, 2021.

[RS02] Karl Rubin and Alice Silverberg. Ranks of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 39(4):455–474, 2002.

[RT21] Beth Romano and Jack A. Thorne. E_8 and the average size of the 3-Selmer group of the Jacobian of a pointed genus-2 curve. *Proc. Lond. Math. Soc. (3)*, 122(5):678–723, 2021.

[Sha13] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer, Heidelberg, third edition, 2013. Varieties in projective space.

[Sha19] Ananth N. Shankar. 2-Selmer groups of hyperelliptic curves with marked points. *Trans. Amer. Math. Soc.*, 372(1):267–304, 2019.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[SW18] Arul Shankar and Xiaoheng Wang. Rational points on hyperelliptic curves having a marked non-Weierstrass point. *Compos. Math.*, 154(1):188–222, 2018.

[Tho13] Jack A. Thorne. Vinberg's representations and arithmetic invariant theory. *Algebra Number Theory*, 7(9):2331–2368, 2013.

[Tho14] Jack A. Thorne. A remark on the arithmetic invariant theory of hyperelliptic curves. *Math. Res. Lett.*, 21(6):1451–1464, 2014.

[Tho16] Jack A. Thorne. Arithmetic invariant theory and 2-descent for plane quartic curves. *Algebra Number Theory*, 10(7):1373–1413, 2016. With an appendix by Tasho Kaletha.

[Tit66] J. Tits. Classification of algebraic semisimple groups. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 33–62. Amer. Math. Soc., Providence, R.I., 1966.

[Vin76] È. B. Vinberg. The Weyl group of a graded Lie algebra. *Izv. Akad. Nauk SSSR Ser. Mat.*, 40(3):488–526, 709, 1976.

[Wei29] André Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52(1):281–315, 1929.

[Zar08] Yu. G. Zarhin. Del Pezzo surfaces of degree 1 and Jacobians. *Math. Ann.*, 340(2):407–435, 2008.