Arithmetic invariant theory and 2-descent for plane quartic curves

Jack A. Thorne*

April 29, 2016

Abstract

Given a smooth plane quartic curve C over a field k of characteristic 0, with Jacobian variety J, and a marked rational point $P \in C(k)$, we construct a reductive group G and a G-variety X, together with an injection $J(k)/2J(k) \hookrightarrow G(k)\backslash X(k)$. We do this using the Mumford theta group of the divisor 2Θ of J, and a construction of Lurie which passes from Heisenberg groups to Lie algebras.

Contents

Introduction

Motivation. Let C be a smooth, projective, geometrically connected algebraic curve over a field k of characteristic 0, and let J denote its Jacobian variety. It is of interest to calculate the group $J(k)/2J(k)$. For example, when $k = \mathbb{Q}$, this is often the first step in understanding the structure of the finitely generated abelian group $J(\mathbb{Q})$. Calculating the group $J(k)/2J(k)$ is known as performing a 2-descent.

In order to calculate $J(k)/2J(k)$, it is often very useful to be able to understand this group in terms of explicit objects in representation theory. This is particularly the case if one wishes to understand the behaviour of the groups $J(k)/2J(k)$ as the curve C is allowed to vary. A famous example is the description of this group in terms of binary quartic forms, in the case where $C = J$ is an elliptic curve [BSD63]. More recently, Bhargava, Gross and Wang have given a similar description in the case where C is an odd hyperelliptic curve, i.e. a hyperelliptic curve with a marked rational Weierstrass point $P \in C(k)$ [BG13,

*This research was partially conducted during the period the author served as a Clay Research Fellow.

Wan13]. In this case, the group $J(k)/2J(k)$ is understood in terms of equivalence classes of self-adjoint linear operators with fixed characteristic polynomial.

The aim of this paper is to give an invariant-theoretic description of the group $J(k)/2J(k)$ when C is a non-hyperelliptic genus 3 curve with a marked rational point $P \in C(k)$. Such a curve is canonically embedded as a quartic curve in $\mathbb{P}^2_k$, which explains the title of this paper. The set of such pairs (C, P) breaks up into 4 natural families, according to the behaviour of the projective tangent line to C at P (these are described below).

Our results can be summarized in broad terms as follows: for each family of curves, we obtain a reductive group G over k, an algebraic variety X on which G acts, and for each pair $x = (C, P)$ defined over k, a closed G-orbit $X_x \subset X$ and a canonical injection

$$J(k)/2J(k) \hookrightarrow G(k)\backslash X_x(k).$$

If k is separably closed, then the set $G(k)\backslash X_x(k)$ has a single element. In general, the set $X_x(k)$ of k-rational points breaks up into many $G(k)$-orbits, which become conjugate over the separable closure. The set of $G(k)$-orbits can be described in terms of Galois cohomology, and this allows us to make a link with the theory of 2-descent.

Two of the spaces X that we construct are in fact linear representations, and our results in these cases (although not our proofs) parallel those in [BG13, §4]. Bhargava and Gross apply the results of *loc. cit.* to understand the average size of the 2-Selmer group of the Jacobian of an odd hyperelliptic curve over $\mathbb{Q}$. We hope that our results will have similar applications in the future, but we do not pursue the study of Selmer groups in this paper.

The other two spaces we construct are global analogues of Vinberg's θ-groups, which have been previously studied from the point of view of geometric invariant theory by Richardson [Ric82b]. We wonder if they can have similar applications in arithmetic invariant theory, and if there are similar and simpler spaces which are related, for example, to elliptic curves.

Description of main results. We now describe more precisely what we prove in this paper. Let k be a field of characteristic 0. We are interested in the arithmetic of all pairs (C, P) over k, where C is a smooth non-hyperelliptic curve of genus 3, and $P \in C(k)$ is a marked rational point. We break up such pairs into 4 families, corresponding to the behaviour of the projective tangent line $\ell = T_P C$ in the canonical embedding:

Case E_7: ℓ meets C at exactly 3 points (the generic case).

Case $\mathfrak{e}_7$: ℓ meets C at exactly 2 points, with contact of order 3 at P (ℓ is a flex).

Case E_6: ℓ meets C at exactly 2 points, with contact of order 2 at P (ℓ is a bitangent line).

Case $\mathfrak{e}_6$: ℓ meets C at exactly 1 point (ℓ is a hyperflex).

The name for each case indicates the semisimple algebraic group or Lie algebra inside which we will construct the variety X described above. The definitions are as follows:

Case E_7: Let H be a split adjoint simple group of type E_7, and let $\theta : H \to H$ be a split stable involution (see Proposition 1.9 below). We define G to be the identity component of the θ-fixed group H^θ, and Y to be the connected component of the identity in the θ-inverted set $H^{\theta(h)=h^{-1}}$. (Equivalently, Y can be realized as the quotient H/G.)

Case $\mathfrak{e}_7$: Let H, θ, and G be as in case E_7. We define V to be the tangent space to Y at the identity, where Y is as in case E_7. Then V is a linear representation of G, and can be identified with the -1-eigenspace of θ in $\mathfrak{h} = \operatorname{Lie} H$.

Case E_6: Let H be instead a split adjoint simple group of type E_6, and let $\theta : H \to H$ be a split stable involution. We define G to be the identity component of the θ-fixed group H^θ, and Y to be the connected component of the identity in the θ-inverted set $H^{\theta(h)=h^{-1}}$.

Case $\mathfrak{e}_6$: Let H, θ, and G be as in case E_6. We define V to be the tangent space to Y at the identity, where Y is as in case E_6. Equivalently, $V = \mathfrak{h}^{\theta=-1} \subset \mathfrak{h}$.

In case E_7 or E_6, we let $X = Y$. In case $\mathfrak{e}_7$ or $\mathfrak{e}_6$, we let $X = V$. In each case the open subscheme $X^{\mathrm{s}} \subset X$ of geometric stable orbits (i.e. closed orbits with finite stabilizers) is non-empty, and can be realized as the complement of a discriminant hypersurface. A Chevalley restriction theorem holds, and if k is separably closed then two elements $x, y \in X^{\mathrm{s}}(k)$ are $G(k)$-conjugate if and only if they have the same image in the categorical quotient $X /\!\!/ G$. (We remark that the quotients $V /\!\!/ G$ are abstractly isomorphic to affine space. This is not so for the quotients $Y /\!\!/ G$, although it would be so if in their definition we replaced the adjoint group H by its simply connected cover.) The spaces V are linear representations of G of the type arising from Vinberg theory, and have been studied in the context of arithmetic invariant theory in e.g. [Tho13]. The spaces Y are a 'global' analogue of the representations V.

Our first main result is the construction of a point of $G(k)\backslash X^s(k)$ which corresponds to the trivial element of the group $J(k)/2J(k)$:

Theorem 1. *[Theorem 3.5]*

1. *In case E_7 or E_6, let $\mathcal{S}$ denote the functor k-alg $\to$ Sets which classifies pairs (C, P), where C is a smooth, non-hyperelliptic curve of genus 3, and P is a point of C as above. Then there is a canonical map*
$$\mathcal{S}(k) \to G(k)\backslash Y^s(k).$$
If k is separably closed, then this map is bijective.

2. *In case $\mathfrak{e}_7$ or $\mathfrak{e}_6$, let $\mathcal{S}$ denote the functor k-alg $\to$ Sets which classifies tuples (C, P, t), where C is a smooth non-hyperelliptic curve of genus 3, P is a point of C as above, and t is a non-zero element of the Zariski tangent space of C at P. Then there is a canonical map*
$$\mathcal{S}(k) \to G(k)\backslash V^s(k).$$
If k is separably closed, this map is bijective.

In any of the above cases, given $x \in \mathcal{S}(k)$ corresponding to a tuple $(C, P, \dots)$, we write J_x for the Jacobian of C and $X_x \subset X$ for the geometric stable orbit containing the image of x, where again $X = Y$ in case E_7 or E_6, and $X = V$ in case $\mathfrak{e}_7$ or $\mathfrak{e}_6$. As noted above, $G(k)$ acts transitively on $X_x(k)$ if k is separably closed, but in general this is not the case; instead, the orbits comprising $G(k)\backslash X_x(k)$ can be described in terms of Galois cohomology. Our main theorem shows how to construct orbits in $G(k)\backslash X_x(k)$ using rational points of $J_x(k)$:

Theorem 2. *[Theorem 3.6] Let notation be as above. Then there is a canonical injection $J_x(k)/2J_x(k) \hookrightarrow G(k)\backslash X_x(k)$. The image of the identity element of $J_x(k)$ is the image of x under the map of Theorem 1.*

We observe that the Jacobian J_x depends only on the curve C, but the set $G(k)\backslash X_x(k)$ depends on the choice of auxiliary data; an analogous situation arises when doing 2-descent on the Jacobian of a hyperelliptic curve which has more than one k-rational Weierstrass point.

Methods. The methods we adopt to prove Theorems 1 and 2 seem to be different to preceding work of a similar type. This reflects the fact that we are now in the territory of exceptional groups, whereas e.g. 2-descent on hyperelliptic curves can be understood using the invariant theory of Vinberg θ-groups which are constructed inside classical groups (in fact, groups of type A_n).

Our starting point is a classical geometric construction. For concreteness, we describe what happens just in the case of type E_6. Let us therefore take a smooth, non-hyperelliptic curve C over $\mathbb{C}$ of genus 3, and let $P \in C(\mathbb{C})$ be a marked point where the projective tangent line in the canonical embedding is a bitangent line. The double cover $\pi : S \to \mathbb{P}^2$ branched over C is a del Pezzo surface of degree 2, and the strict transform of ℓ is union of two (-1)-curves; blowing down one of these, we obtain a smooth cubic surface S.

There is a well-known connection between cubic surfaces and the root system of type E_6: let $\Lambda = K_S^{\perp} \subset H^2(S, \mathbb{Z})$ denote the orthogonal complement of the canonical class of S. Then Λ is in fact a root lattice of type E_6. This does not immediately provide a relation with geometric invariant theory because there is no functorial construction of a reductive group from a root lattice.

However, Lurie [Lur01] has observed that one can construct in a functorial way the group H corresponding to Λ given the additional data of a *double cover* of $V = \Lambda/2\Lambda$, i.e. a group extension

$$1 \longrightarrow \{\pm 1\} \longrightarrow \widetilde{V} \longrightarrow V \longrightarrow 1 \tag{0.1}$$

satisfying some additional conditions; in particular, that the quadratic form $q : V \to \mathbb{F}_2$ corresponding to this extension agrees with the one derived from the natural quadratic form on Λ.

It turns out that the realization of the cubic surface X using the plane quartic curve C is exactly the data required for input into Lurie's construction. Indeed, let J denote the Jacobian of the curve C. Then J has a natural principal polarization Θ, and associated to $\mathcal{L} = 2\Theta$ is the Mumford theta group

$$1 \longrightarrow \{\pm 1\} \longrightarrow \widetilde{H}_{\mathcal{L}} \longrightarrow J[2] \longrightarrow 1. \tag{0.2}$$

(More precisely, the Mumford theta group is a central extension of $J[2]$ by $\mathbb{G}_m$. The presence of the odd theta characteristic corresponding to the bitangent ℓ allows us to refine it to an extension by $\{\pm 1\}$.) We show that there is a canonical isomorphism $J[2] \cong \Lambda/2\Lambda$; pushing out the sequence (0.2) by this isomorphism, we obtain a sequence of type (0.1), to which Lurie's construction applies. We thus obtain from the data (C, ℓ) an algebraic group of type E_6. (We remark here that the isomorphism $J[2] \cong \Lambda/2\Lambda$ is well-known and classical; see for example [DO88, IX, §1]. We thank the anonymous referee for this reference.)

The principle underlying this paper is that the construction outlined above is sufficiently functorial that we can recover the arithmetic situation over any field k of characteristic 0 simply by Galois descent. To construct the orbits whose existence is asserted by Theorem 2, we simply twist the extension (0.2). More precisely, we recall in §1.3 below how a point of $J_x(k)$ gives rise to a twisted form of the Heisenberg group $\widetilde{H}_{\mathcal{L}}$. We then construct additional orbits by applying our version of Lurie's construction to this twisted Heisenberg group.

Other remarks. There are some minor subtleties in our construction that we remark on now. One point is that in cases $\mathfrak{e}_6$, $\mathfrak{e}_7$, we associate orbits not to pairs (C, P) but to triples (C, P, t), where t is a non-zero Zariski tangent vector at the point P. This reflects the fact that the space X constructed in this case has an extra symmetry: it is a linear representation of the reductive group G, so we are free to multiply elements by scalars. This scaling corresponds to scaling the tangent vector t. A similar feature appears in the work of Bhargava–Gross [BG13], where it allows one to 'clear denominators' when working over $\mathbb{Q}$, and restrict to integral orbits.

Another point is that in the geometric construction sketched above, we associate a point to a pair (C, ℓ), and do not need the point P which gives rise to the bitangent ℓ. Of course, ℓ being fixed, there are exactly two possible choices of point P. It turns out that in each case, the data of the point P is exactly the data required to rigidify the picture so that we obtain the expected bijection (as in Theorem 1) when k is separably closed. This is an essential feature, since we rely heavily on Galois descent.

Our modified version of Lurie's construction associates to an appropriate extension $\widetilde{V}$ with action by the absolute Galois group of k a triple $(\mathfrak{h}, \mathfrak{t}, \theta)$ consisting of a Lie algebra over k of the correct Dynkin type, a Cartan subalgebra $\mathfrak{t} \subset \mathfrak{h}$, and a stable involution θ of $\mathfrak{h}$ which acts as multiplication by -1 on $\mathfrak{t}$. For arithmetic applications, we extend this construction in a surprising way: we show that a representation of the group $\widetilde{V}$ appearing in the extension (0.1), and on which -1 acts as multiplication by -1, gives rise to a representation of the θ-fixed Lie algebra $\mathfrak{h}^{\theta}$.

The features of these constructions suggest that they should have an inverse, i.e. that given a tuple $(\mathfrak{h}, \mathfrak{t}, \theta)$ consisting of a simple Lie algebra $\mathfrak{h}$ over k, a Cartan subalgebra $\mathfrak{t} \subset \mathfrak{h}$ and an involution θ of $\mathfrak{h}$ which acts as -1 on $\mathfrak{t}$, one should be able to pass in the opposite direction to obtain a root lattice Λ with Γ_k-action and an extension $\widetilde{V}$ of $V = \Lambda/2\Lambda$ of type (0.1). The existence of such an inverse has been shown by Tasho Kaletha, and appears in an appendix to this paper. He finds the group $\widetilde{V}$ inside the simply connected cover

of the group $G = (H^\theta)^\circ$, where H is the adjoint simple group over k with Lie algebra $\mathfrak{h}$. In §3.2, we apply these results to calculate the number of orbits with given invariants in the case $k = \mathbb{R}$.

Organization of this paper. In §1 below, we recall some basic facts about quadratic forms, 2-descent for abelian varieties, and the invariant theory of the G-varieties under consideration here. In §2 we describe our modifications to Lurie's constructions. In §3 we apply these constructions to the geometry of plane quartics, in order to arrive at the results described in this introduction. We conclude in §3.2 with an explicit example in the case $k = \mathbb{R}$.

Acknowledgements. I am grateful to Manjul Bhargava, Dick Gross, and Tasho Kaletha for many interesting conversations. I would like to thank Tasho again for writing the appendix to this paper. Finally, I thank the anonymous referee for their helpful comments.

Notation. Throughout this paper, k will denote a field of characteristic 0, and k^s a fixed separable closure of k. We write $\Gamma_k = \mathrm{Gal}(k^s/k)$. If X is a k-vector space or a scheme of finite type over k, then we write X_{k^s} for the object obtained by extending scalars to k^s. If X is a smooth projective variety over k, then we write K_X for its canonical class. If $G, H, \ldots$ are connected algebraic groups over k, then we use gothic letters $\mathfrak{g}, \mathfrak{h}, \ldots$ to denote their Lie algebras. If H is an algebraic group over k, then we write $H^1(k, H)$ for the continuous cohomology set $H^1(\Gamma_k, H(k^s))$, where $H(k^s)$ is endowed with the discrete topology. If θ is an involution of H, then we write H^θ for the closed subgroup of H consisting of θ-fixed elements, and $\mathfrak{h}^\theta$ for the Lie algebra of H (equivalently, the $+1$-eigenspace of the differential of θ in $\mathfrak{h}$). We will make use of the equivalence between commutative finite k-groups and $\mathbb{Z}[\Gamma_k]$-modules of finite cardinality (given by $H \mapsto H(k^s)$).

By definition, a lattice $(\Lambda, \langle\cdot,\cdot\rangle)$ is a finite free $\mathbb{Z}$-module Λ together with a symmetric and positive-definite bilinear form $\langle\cdot,\cdot\rangle : \Lambda \times \Lambda \to \mathbb{Z}$. We define $\Lambda^\vee = \{\lambda \in \Lambda \otimes_{\mathbb{Z}} \mathbb{Q} \mid \langle\lambda, \Lambda\rangle \subset \mathbb{Z}\}$, which is naturally identified with $\mathrm{Hom}(\Lambda, \mathbb{Z})$. We call Λ a (simply laced) root lattice if it satisfies the following additional conditions:

- For each $\lambda \in \Lambda$, $\langle\lambda, \lambda\rangle$ is an even integer.
- The set $\Gamma = \{\lambda \in \Lambda \mid \langle\lambda, \lambda\rangle = 2\}$ generates Λ as an abelian group.

In this case, Γ is a simply laced root system, each $\gamma \in \Gamma$ being associated with the simple reflection $s_\gamma(x) = x - \langle x, \gamma\rangle\gamma$. If Γ is *irreducible*, then it is a root system of type A, D, or E. In any case, we write $W(\Lambda) \subset \mathrm{Aut}(\Lambda)$ for the Weyl group of Γ, a finite group generated by the simple reflections s_γ, $\gamma \in \Gamma$.

In several places, we will consider central group extensions of the form

$$1 \longrightarrow \{\pm 1\} \longrightarrow \widetilde{E} \longrightarrow E \longrightarrow 1.$$

If $\widetilde{e} \in \widetilde{E}$, then we will write $-\widetilde{e}$ for the element $(-1) \cdot \widetilde{e}$. We note that this is not necessarily equal to $\widetilde{e}^{-1}$. We write e for the image of $\widetilde{e}$ in E.

1 Background

We first recall some background material. For proofs of the results in §§1.1–1.2, we refer the reader to [GH04].

1.1 Quadratic forms over $\mathbb{F}_2$

Let V be a finite-dimensional $\mathbb{F}_2$-vector space, and let $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{F}_2$ be a strictly alternating pairing.

Definition 1.1. *A quadratic refinement of V is a function $q : V \to \mathbb{F}_2$ such that for all $v, w \in V$, we have $\langle v, w\rangle = q(v + w) + q(v) + q(w)$.*

In general, there is no distinguished quadratic refinement of V. However, we have the following result.

Proposition 1.2. *Suppose that the pairing $\langle \cdot, \cdot \rangle$ is non-degenerate.*

1. *Fix a decomposition $V = U \oplus U'$, where U, U' are isotropic subspaces of dimension $g \geq 0$. Then the function $q_{U,U'}(v) = \langle v_U, v_{U'} \rangle$ is a quadratic refinement. (Here we write v_U, $v_{U'}$ for the projections of $v \in V$ onto the two isotropic subspaces.)*

2. *The set of quadratic refinements of V is a principal homogeneous space for V, addition being defined by the formula $(v + q)(w) = q(w) + \langle v, w \rangle$.*

Definition 1.3. *Suppose that the pairing $\langle \cdot, \cdot \rangle$ is non-degenerate, and let q be a quadratic refinement of V. The Arf invariant $a(q) \in \mathbb{F}_2$ of q is defined as follows. Fix a decomposition $V = U \oplus U'$ into isotropic subspaces of dimension $g \geq 0$. Let $\{e_1, \ldots, e_g\}$ be a basis of U, and let $\{\epsilon_1, \ldots, \epsilon_g\}$ denote the dual basis of U'. Then $a(q) = \sum_{i=1}^{g} q(e_i)q(\epsilon_i)$.*

Lemma 1.4. *Suppose that the pairing $\langle \cdot, \cdot \rangle$ is non-degenerate, and let $\dim V = 2g \geq 0$.*

1. *The Arf invariant $a(q)$ is well-defined.*

2. *Let $\mathrm{Sp}(V)$ denote the group of automorphisms of the pair $(V, \langle \cdot, \cdot \rangle)$. Then $\mathrm{Sp}(V)$ has precisely 2 orbits on the set of quadratic refinements of V, which are distinguished by their Arf invariants. The set of refinements with $a(q) = 0$ has cardinality $2^{g-1}(2^g + 1)$ and the set of refinements with $a(q) = 1$ has cardinality $2^{g-1}(2^g - 1)$.*

3. *If q is a quadratic refinement and $v \in V$, then $a(q + v) = a(q) + q(v)$.*

1.2 Theta characteristics

Let k be a field of characteristic 0, and let C be a smooth, projective, geometrically irreducible curve over k, of genus $g \geq 2$. We write K_C for the canonical bundle of C, and $J = \mathrm{Pic}^0(C)$ for the Jacobian of C. We write $V = J[2]$, a finite k-group. We view V as an $\mathbb{F}_2$-vector space of dimension $2g$ with continuous Γ_k-action. The Weil pairing defines a non-degenerate, strictly alternating bilinear form $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{F}_2$ which is Γ_k-invariant.

Definition 1.5. 1. *A theta characteristic is a line bundle $\mathcal{L}$ on C such that $\mathcal{L}^{\otimes 2} \cong K_C$.*

2. *Let $\mathcal{L}$ be a theta characteristic. We say that $\mathcal{L}$ is odd (resp. even) if $h^0(\mathcal{L})$ is odd (resp. even).*

Here and below we write $h^0(\mathcal{L}) = \dim_k H^0(C, \mathcal{L})$ for any line bundle $\mathcal{L}$ on the curve C.

Lemma 1.6. 1. *As a principal homogeneous space for V, the k-variety of isomorphism classes of theta characteristics is canonically identified with the k-scheme of quadratic refinements of the Weil pairing: if $\mathcal{L}$ is a theta characteristic, we associate to it the quadratic refinement $q : V \to \mathbb{F}_2$ defined by the formula $q(v) = h^0(\mathcal{L} \otimes_{\mathcal{O}_C} v) + h^0(v) \bmod 2$.*

2. *With notation as above, the Arf invariant of q is $a(q) = h^0(\mathcal{L}) \bmod 2$.*

Henceforth we identify the set of theta characteristics of the curve C with the set of quadratic refinements $\kappa : V \to \mathbb{F}_2$.

1.3 Heisenberg groups and descent

We continue with the notation of §1.2. Let J^{g-1} denote the J-torsor of degree $g - 1$ line bundles on C; it contains the theta divisor W_{g-1}. Given a theta characteristic κ defined over k, we have the translation map $t_\kappa : J \to J^{g-1}$, $\mathcal{L} \mapsto \mathcal{L} \otimes \kappa$, and we define $\Theta_\kappa = t_\kappa^* W_{g-1}$. It is a symmetric divisor, and all symmetric theta

divisors arise in this fashion. (This is classical; see [BL04, Ch. 11].) Similarly, if $A \in J(k)$ then there is a translation map $t_A : J \to J$, $\mathcal{L} \mapsto \mathcal{L} \otimes A$.

The isomorphism class of the line bundle $\mathcal{L}_\kappa = \mathcal{O}_J(2\Theta_\kappa)$ is independent of the choice of κ, but there is no canonical choice of isomorphism as κ varies. In particular, even if κ is defined only over k^s, the field of definition of this bundle is equal to k. We choose a bundle $\mathcal{L}$ in this isomorphism class defined over k. We introduce the Heisenberg group $\widetilde{H}_\mathcal{L}$ of pairs (ω, φ), where $\omega \in J[2]$ and $\varphi : \mathcal{L} \to t_\omega^*\mathcal{L}$ is an isomorphism. It is an extension

$$0 \longrightarrow \mathbb{G}_m \longrightarrow \widetilde{H}_\mathcal{L} \longrightarrow J[2] \longrightarrow 0.$$

Lemma 1.7. *1. Let ω, $\eta \in J[2]$, and let $\widetilde{\omega}$, $\widetilde{\eta}$ denote lifts of these elements to $\widetilde{H}_\mathcal{L}$. Then $\widetilde{\omega}\widetilde{\eta}\widetilde{\omega}^{-1}\widetilde{\eta}^{-1} = (-1)^{\langle \omega, \eta \rangle}$.*

2. Let $\mathrm{Aut}(\widetilde{H}_\mathcal{L}; J[2])$ denote the group of automorphisms of $\widetilde{H}_\mathcal{L}$ fixing $\mathbb{G}_m$ pointwise and acting as the identity on $J[2]$. Then the map

$$\eta \mapsto ((\omega, \varphi) \mapsto (\omega, (-1)^{\langle \eta, \omega \rangle}\varphi))$$

defines an isomorphism $J[2] \cong \mathrm{Aut}(\widetilde{H}_\mathcal{L}; J[2])$.

Proof. The first part can be taken as the definition of the Weil pairing. The second part follows from [BL04, Lemma 6.6.6]. □

If κ is a theta characteristic defined over k, then we can define a character $\chi_\kappa : \widetilde{H}_\mathcal{L} \to \mathbb{G}_m$ by the formula $\chi_\kappa(\widetilde{\omega}) = \widetilde{\omega}^2(-1)^{q_\kappa(\omega)}$. (This makes sense since the square of any element of $\widetilde{H}_\mathcal{L}$ lies in $\mathbb{G}_m$.) We then have an exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow \ker \chi_\kappa \longrightarrow J[2] \longrightarrow 1. \tag{1.1}$$

This construction will play an important role later on; compare the required data at the beginning of §2 below.

Associated to J is the Kummer exact sequence:

$$0 \longrightarrow J[2] \longrightarrow J \longrightarrow J \longrightarrow 0,$$

and the associated short exact sequence in Galois cohomology:

$$0 \longrightarrow J(k)/2J(k) \xrightarrow{\delta} H^1(k, J[2]) \longrightarrow H^1(k, J)[2] \longrightarrow 0.$$

The map δ can be written down explicitly as follows: given $A \in J(k)$, choose $B \in J(k^s)$ such that $[2](B) = A$. Then the cohomology class $\delta(A)$ is represented by the cocycle $\sigma \mapsto {}^\sigma B - B$.

We now give another interpretation of this homomorphism in terms of the group $\widetilde{H}_\mathcal{L}$. The field of definition of the line bundle $t_B^*\mathcal{L}$ is equal to k; we let $\mathcal{L}_B$ denote a choice of descent to k, unique up to k-isomorphism. This allows us to define the Heisenberg group $\widetilde{H}_{\mathcal{L}_B}$ of pairs (ω, φ), where $\omega \in J[2]$ and φ is an isomorphism $\mathcal{L}_B \to t_\omega^*\mathcal{L}_B$. We also fix a choice of isomorphism $f : \mathcal{L}_B \to t_B^*\mathcal{L}$ over k^s.

The choice of f defines an isomorphism $F : (\widetilde{H}_\mathcal{L})_{k^s} \cong (\widetilde{H}_{\mathcal{L}_B})_{k^s}$, given by the formula

$$F : (\omega, \varphi) \mapsto (\omega, t_\omega^* f^{-1} \circ t_B^*\varphi \circ f). \tag{1.2}$$

We define a cocycle valued in $\mathrm{Aut}(\widetilde{H}_\mathcal{L}; J[2])$ by the formula $\sigma \mapsto F^{-1\sigma}F$.

Lemma 1.8. *This cocycle is equal to the cocycle $\sigma \mapsto {}^\sigma B - B$ under the identification of Lemma 1.7.*

In particular, this cocycle depends only on B, and not on any other choice.

Proof. The proof is by an explicit calculation, $F^{-1\sigma}F$ being given by

$$(\omega, \varphi) \mapsto \left(\omega, t^*_{\omega - B} f \circ t^*_{-B}\left[t^*_{\omega}{}^{\sigma} f^{-1} \circ t^*_{{}^{\sigma}B}\varphi \circ {}^{\sigma} f\right] \circ t^*_{-B} f^{-1}\right)$$

We must show that this expression is equal to $(\omega, (-1)^{\langle \omega, {}^{\sigma}B - B\rangle}\varphi)$. However, writing $\eta = {}^{\sigma}B - B$ and $\psi = t^*_{-{}^{\sigma}B}(f \circ {}^{\sigma} f^{-1})$, we have $(\eta, \psi) \in \widetilde{H}_{\mathcal{L}}$ and, by Lemma 1.7,

$$(\omega, (-1)^{\langle \omega, {}^{\sigma}B - B\rangle}\varphi) = (\eta, \psi)(\omega, \varphi)(\eta, \psi)^{-1}(\omega, \varphi)^{-1}(\omega, \varphi) = (\eta, \psi)(\omega, \varphi)(\eta, \psi)^{-1} = (\omega, t^*_{\omega+\eta}\psi \circ t^*_{\eta}\varphi \circ t^*_{\eta}\psi^{-1}).$$

Expanding this expression now shows it to be equal to $F^{-1\sigma}F$. □

1.4 Invariant theory of reductive groups with involution

Let k be a field of characteristic 0, and let H be a split adjoint simple group over k of type A, D, or E.

Proposition 1.9. *There exists a unique $H(k)$-conjugacy class of involutions θ of H satisfying the following two conditions:*

1. $\operatorname{tr}(d\theta : \mathfrak{h} \to \mathfrak{h}) = -\operatorname{rank} H$.
2. *The group $(H^{\theta})^{\circ}$ is split.*

Proof. The result [Tho13, Corollary 2.15] states that there is a unique $H(k)$-orbit of involutions $\theta : H \to H$ such that $\operatorname{tr} d\theta = -\operatorname{rank} H$ and $\mathfrak{h}^{d\theta=-1}$ contains a regular nilpotent element. The discussion there also shows by construction that for each θ in this class, the group $(H^{\theta})^{\circ}$ is split. We must show that if $\theta : H \to H$ is an involution such that $\operatorname{tr} d\theta = -\operatorname{rank} H$ and $(H^{\theta})^{\circ}$ is split, then $\mathfrak{h}^{d\theta=-1}$ contains a regular nilpotent. Let $\mathfrak{t}_0 \subset \mathfrak{h}^{d\theta=1}$ be a split Cartan subalgebra, and let $\mathfrak{t} \subset \mathfrak{h}$ be a split Cartan subalgebra containing $\mathfrak{t}_0$.

By [Tho13, Lemma 2.14] and [Tho13, Lemma 2.6], we can find a normal $\mathfrak{sl}_2$-triple (E, X, F) in $\mathfrak{h} \otimes_k k^s$ (i.e. a tuple of elements $E, X, F \in \mathfrak{h} \otimes_k k^s$ satisfying the relations

$$[E, F] = X,\ [X, E] = 2E,\ [X, F] = -2F,$$
$$\theta(X) = X,\ \theta(E) = -E,\ \text{and } \theta(F) = -F)$$

with E regular nilpotent and $X \in \mathfrak{t}_0 \otimes_k k^s$. Since X is part of an $\mathfrak{sl}_2$-triple, it follows that $\alpha(X) \in \mathbb{Z}$ for every root of $\mathfrak{t}$ in $\mathfrak{h}$, hence $X \in \mathfrak{t}$, hence $X \in \mathfrak{t}_0$. By [dG11, Proposition 7], we can find elements $E' \in \mathfrak{h}^{d\theta=-1}$ and $F' \in \mathfrak{h}^{d\theta=-1} \otimes_k k^s$ such that (E', X, F') is a normal $\mathfrak{sl}_2$-triple. In particular, E' is a regular nilpotent. This completes the proof. □

Henceforth we fix a choice of θ satisfying the conclusion of Proposition 1.9 and write $G = (H^{\theta})^{\circ}$. Then G is a split semisimple group. (For a proof that G is semisimple, see §A.2 of the appendix to this paper.) We will study the invariant theory of two different actions of G. We first consider $V = \mathfrak{h}^{d\theta=-1}$. Then V is a linear representation of the group G.

Theorem 1.10. 1. *V satisfies the Chevalley restriction theorem: if $\mathfrak{t} \subset V$ is a Cartan subalgebra, then the map $N_G(\mathfrak{t}) \to W_{\mathfrak{t}} = N_H(\mathfrak{t})/Z_H(\mathfrak{t})$ is surjective, and the inclusion $\mathfrak{t} \subset V$ induces an isomorphism*

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

In particular, the quotient $V/\!\!/G$ is isomorphic to affine space.

2. *Suppose that $k = k^s$, and let $x, y \in V$ be regular semisimple elements. Then x is $G(k)$-conjugate to y if and only if x, y have the same image in $V/\!\!/G$.*
3. *There exists a discriminant polynomial $\Delta \in k[V]$ such that for all $x \in V$, x is regular semisimple if and only if $\Delta(x) \neq 0$, if and only if the G-orbit of x is closed in V and $\operatorname{Stab}_G(x)$ is finite.*

Proof. This follows from results of Vinberg, which are summarized in [Pan05] or (in our case of interest) [Tho13, §2]. □

We now consider the variety $Y \subset H$, locally closed image of the morphism $H \to H, h \mapsto h^{-1}\theta(h)$. It is a connected component of the subvariety $\{h \in H \mid \theta(h) = h^{-1}\}$, and is in particular closed in H. Note that Y has a marked point (namely the identity element of H), and the tangent space to Y at this marked point is canonically isomorphic, as G-representation, to the representation V defined above.

Theorem 1.11. *1. Y satisfies the Chevalley restriction theorem: if $T \subset Y$ is a maximal torus, then $N_G(T) \to W_T = N_H(T)/Z_H(T)$ is surjective, and the inclusion $T \subset Y$ induces an isomorphism*

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

2. Suppose that $k = k^s$, and let $x, y \in Y$ be regular semisimple elements. Then x is $G(k)$-conjugate to y if and only if x, y have the same image in $Y /\!\!/ G$.

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

Proof. See [Ric82b, §0]. □

2 A group with involution

Let k be a field of characteristic 0. Suppose that we are given the following data:

- An irreducible simply laced root lattice $(\Lambda, \langle \cdot, \cdot \rangle)$ together with a continuous homomorphism $\Gamma_k \to W(\Lambda) \subset \mathrm{Aut}(\Lambda)$.
- A central extension $\widetilde{V}$ of $V = \Lambda/2\Lambda$:

  $$0 \to \{\pm 1\} \to \widetilde{V} \to V \to 0,$$

  together with a homomorphism $\Gamma_k \to \mathrm{Aut}(\widetilde{V})$. We suppose that Γ_k leaves invariant the subgroup $\{\pm 1\}$, and that the induced homomorphism $\Gamma_k \to \mathrm{Aut}(V)$ agrees with the homomorphism $\Gamma_k \to \mathrm{Aut}(\Lambda) \to \mathrm{Aut}(\Lambda/2\Lambda) = \mathrm{Aut}(V)$. We also suppose that for $\widetilde{v} \in \widetilde{V}$, we have the relation $\widetilde{v}^2 = (-1)^{\langle v, v \rangle/2}$.

In terms of this data we will define, following Lurie [Lur01], the following:

1. A simple Lie algebra $\mathfrak{h}$ over k of type equal to the Dynkin type of Λ.
2. A maximal torus T of H, the adjoint group over k with Lie algebra $\mathfrak{h}$, together with an isomorphism $T[2](k^s) \cong V^\vee$ of $\mathbb{Z}[\Gamma_k]$-modules.
3. An involution $\theta : H \to H$ leaving T stable, and satisfying $\theta(t) = t^{-1}$ for all $t \in T(k)$.

Suppose given further the data of a finite-dimensional k-vector space W and a homomorphism $\rho : \widetilde{V} \to \mathrm{GL}(W_{k^s})$ such that $\rho(-1) = -\mathrm{id}_W$ and for all $\sigma \in \Gamma_k$ and $\widetilde{v} \in \widetilde{V}$, we have $\rho({}^\sigma \widetilde{v}) = {}^\sigma \rho(\widetilde{v})$. Then we will further define:

4: A Lie algebra homomorphism $R : \mathfrak{h}^\theta \to \mathfrak{gl}(W)$.

(Using the equivalence between $\mathbb{Z}[\Gamma_k]$-modules of finite cardinality and commutative finite k-groups, ρ corresponds to a homomorphism $\widetilde{V} \to \mathrm{GL}(W)$ of k-groups.)

Let $\widetilde{\Lambda} = \Lambda \times_V \widetilde{V}$, a central extension of Λ by $\{\pm 1\}$. Let $\Gamma \subset \Lambda$ be the set of roots, and $\widetilde{\Gamma} \subset \widetilde{\Lambda}$ its inverse image. Following Lurie [Lur01], we define L' to be the free abelian group on symbols $X_{\widetilde{\gamma}}$ for $\widetilde{\gamma} \in \widetilde{\Gamma}$, modulo the relation $X_{\widetilde{\gamma}} = -X_{-\widetilde{\gamma}}$. (Thus $\{\widetilde{\gamma}, -\widetilde{\gamma}\}$ is the inverse image in $\widetilde{\Gamma}$ of $\gamma \in \Gamma$.) We set $L = \Lambda^\vee \oplus L'$, and define a bracket $[\cdot, \cdot] : L \times L \to L$ by the formulae:

- $[\lambda, \lambda'] = 0$ for all λ, $\lambda' \in \Lambda^\vee$.
- $[\lambda, X_{\widetilde{\gamma}}] = -[X_{\widetilde{\gamma}}, \lambda] = \langle \lambda, \gamma \rangle X_{\widetilde{\gamma}}$ for $\lambda \in \Lambda^\vee$.
- $[X_{\widetilde{\gamma}}, X_{\widetilde{\gamma}'}] = X_{\widetilde{\gamma}\widetilde{\gamma}'}$ if $\gamma + \gamma' \in \Gamma$.
- $[X_{\widetilde{\gamma}}, X_{\widetilde{\gamma}'}] = \epsilon_{\widetilde{\gamma}\widetilde{\gamma}'}\gamma$ if $\gamma + \gamma' = 0$. (By definition, $\epsilon_{\widetilde{\gamma}\widetilde{\gamma}'} = \widetilde{\gamma}\widetilde{\gamma}' \in \{\pm 1\} \subset \mathbb{Z}$.)
- $[X_{\widetilde{\gamma}}, X_{\widetilde{\gamma}'}] = 0$ otherwise.

Theorem 2.1. *1. L is a Lie algebra over $\mathbb{Z}$. There is a natural action of Γ_k on L, respecting the Lie bracket $[\cdot, \cdot]$.*

2. Let $\mathfrak{h} = (L \otimes_k k^s)^{\Gamma_k}$. Then $\mathfrak{h}$ is a simple Lie algebra over k of Dynkin type equal to the type of the root lattice Λ.

Proof. 1. That L is a Lie algebra over $\mathbb{Z}$ of the required type follows from [Lur01, §3.1]. The Galois group Γ_k acts on Λ and on $\widetilde{\Gamma}$ by the given data. We make it act on $L = \Lambda \oplus L'$ by its standard action on Λ and on L' by permuting basis vectors $X_{\widetilde{\gamma}}$, $\widetilde{\gamma} \in \widetilde{\Gamma}$. It is immediate from the definition that this respects the bracket.

2. By Galois descent, the natural map $\mathfrak{h}_{k^s} \to L \otimes_k k^s$ is an isomorphism. The result follows immediately from this.

□

Let H denote the simple adjoint group over k with Lie algebra $\mathfrak{h}$. Let $\mathfrak{t} = (\Lambda^\vee \otimes_k k^s)^{\Gamma_k} \subset \mathfrak{h}$; it is the Lie algebra of a maximal torus T of H, whose module of characters $X^*(T_{k^s})$ is identified with the $\mathbb{Z}[\Gamma_k]$-module Λ. In particular, there is an isomorphism of $\mathbb{Z}[\Gamma_k]$-modules $T[2](k^s) \cong \Lambda^\vee / 2\Lambda^\vee \cong V^\vee$.

We now define the involution θ. Given $\widetilde{\gamma} \in \widetilde{\Gamma}$, we define $Y_{\widetilde{\gamma}} = X_{\widetilde{\gamma}^{-1}}$. By definition, then, $[X_{\widetilde{\gamma}}, Y_{\widetilde{\gamma}}] = \gamma \in \Lambda$. It easy to check that $Y_{-\widetilde{\gamma}} = -Y_{\widetilde{\gamma}}$. We define an involution $\sigma : L \to L$ by taking σ to be multiplication by -1 on Λ and by taking $\sigma(X_{\widetilde{\gamma}}) = -Y_{\widetilde{\gamma}}$.

Proposition 2.2. *1. σ is a well-defined Lie algebra involution, and respects the action of the group Γ_k.*

2. Let θ denote the involution of $\mathfrak{h}$ induced by σ by functoriality. Then $\operatorname{tr} \theta = -\operatorname{rank} \mathfrak{h}$.

Proof. 1. We must check that σ preserves the relations defining $[\cdot, \cdot]$. Let us show that $\sigma[X_{\widetilde{\gamma}}, X_{\widetilde{\gamma}'}] = \sigma X_{\widetilde{\gamma}\widetilde{\gamma}'} = -Y_{\widetilde{\gamma}\widetilde{\gamma}'}$ is equal to $[\sigma X_{\widetilde{\gamma}}, \sigma X_{\widetilde{\gamma}'}] = [X_{\widetilde{\gamma}^{-1}}, X_{\widetilde{\gamma}'^{-1}}] = X_{\widetilde{\gamma}^{-1}\widetilde{\gamma}'^{-1}}$, when $\gamma + \gamma' \in \Gamma$. Equivalently, we must show that $\widetilde{\gamma}\widetilde{\gamma}' = -\widetilde{\gamma}'\widetilde{\gamma}$. By the definition of $\widetilde{\Lambda}$, it is equivalent to show that $\langle \gamma, \gamma' \rangle$ is odd. Since we work in a simply laced root system, this is implied by the condition that $\gamma + \gamma'$ is a root.

2. This follows because θ acts as -1 on $\mathfrak{t}$.

□

We define $G = (H^\theta)^\circ$. We define N_V to be the image of the natural homomorphism $V \to V^\vee$; it is a $\mathbb{Z}[\Gamma_k]$-module, and the induced symplectic form on N_V is non-degenerate and Γ_k-equivariant. The isomorphism $T[2] \cong V^\vee$ restricts to an isomorphism $(T[2] \cap G) \cong N_V$ (cf. [Tho13, Corollary 2.8]).

It remains to define, given a finite-dimensional k-vector space W and a Galois-equivariant homomorphism $\rho : \widetilde{V} \to \mathrm{GL}(W_{k^s})$ such that $\rho(-1) = -\mathrm{id}_W$, a Lie algebra homomorphism $R : \mathfrak{g} \to \mathfrak{gl}(W)$. Let us first assume that $k = k^s$. Then the Lie algebra $\mathfrak{g}$ is spanned by the elements $X_{\widetilde{\gamma}} + X_{-\widetilde{\gamma}^{-1}} = Z_{\widetilde{\gamma}}$, say. Let $\pi : \widetilde{\Gamma} \to \widetilde{V}$ denote the natural map. We define a morphism $R : \mathfrak{g} \to \mathfrak{gl}(W)$ of k-vector spaces by the formula

$$R(Z_{\widetilde{\gamma}}) = \rho(\pi(\widetilde{\gamma}))/2.$$

This is well-defined since $Z_{\widetilde{\gamma}} = -Z_{-\widetilde{\gamma}} = -Z_{\widetilde{\gamma}^{-1}}$, and $\pi(\widetilde{\gamma}) = (-1)^{\langle \gamma, \gamma \rangle / 2} \pi(\widetilde{\gamma})^{-1} = -\pi(\widetilde{\gamma})^{-1}$. In the case $k \neq k^s$, this defines a homomorphism $\mathfrak{g}_{k^s} \to \mathfrak{gl}(W_{k^s})$ which commutes with the action of Γ_k, and we write $R : \mathfrak{g} \to \mathfrak{gl}(W)$ for the homomorphism obtained by Galois descent.

Proposition 2.3. *$R : \mathfrak{g} \to \mathfrak{gl}(W)$ is a Lie algebra homomorphism.*

Proof. We can again assume that $k = k^s$. We must show that, given $\widetilde{\gamma}$, $\widetilde{\gamma}' \in \widetilde{\Gamma}$, we have

$$R([Z_{\widetilde{\gamma}}, Z_{\widetilde{\gamma}'}]) = [R(Z_{\widetilde{\gamma}}), R(Z_{\widetilde{\gamma}'})].$$

We now break up into cases according to the value of $\langle \gamma, \gamma' \rangle$.

1. If $\langle \gamma, \gamma' \rangle = \pm 2$, then $\gamma' = \pm\gamma$, hence $\widetilde{\gamma}' = \pm\widetilde{\gamma}^{\pm 1}$, and both sides of the above equation are zero.
2. If $\langle \gamma, \gamma' \rangle = \pm 1$, then $\gamma \mp \gamma'$ is a root. Let us assume for simplicity that $\langle \gamma, \gamma' \rangle = -1$, so that $\gamma + \gamma'$ is a root, and $[Z_{\widetilde{\gamma}}, Z_{\widetilde{\gamma}'}] = Z_{\widetilde{\gamma}\widetilde{\gamma}'}$. We must show that

   $$\rho(\pi(\widetilde{\gamma}\widetilde{\gamma}'))/2 = \rho(\pi(\widetilde{\gamma})) \cdot \rho(\pi(\widetilde{\gamma}'))/4 - \rho(\pi(\widetilde{\gamma}')) \cdot \rho(\pi(\widetilde{\gamma}))/4.$$

   This follows from the fact that $\widetilde{\gamma}'\widetilde{\gamma} = (-1)^{\langle \gamma, \gamma' \rangle}\widetilde{\gamma}\widetilde{\gamma}' = -\widetilde{\gamma}\widetilde{\gamma}'$ and $\rho(-1) = -\mathrm{id}_W$.
3. If $\langle \gamma, \gamma' \rangle = 0$ then neither of $\gamma \pm \gamma'$ is a root, and the left hand side of the above equation is zero. On the other hand, $\pi(\widetilde{\gamma})$ and $\pi(\widetilde{\gamma}')$ commute, so the right hand side is also zero.

This concludes the proof. □

The above constructions are evidently functorial in $\widetilde{V}$, in the following sense: given $\widetilde{V}$, $\widetilde{V}_B$ satisfying the conditions at the beginning of this section, and a Γ_k-equivariant isomorphism $f : \widetilde{V} \to \widetilde{V}_B$, we obtain an isomorphism of associated simple adjoint groups $F : H \cong H_B$, intertwining θ, θ_B, and restricting to an isomorphism $T \to T_B$ which induces the identity on Λ. In this connection, we have the following lemma.

Lemma 2.4. *1. Let us write $\mathrm{Aut}(\widetilde{V}; V)$ for the group of automorphisms of $\widetilde{V}$ leaving the central subgroup $\{\pm 1\}$ invariant and inducing the identity on V. Then there is a canonical isomorphism $V^\vee \cong \mathrm{Aut}(\widetilde{V}; V)$, given by $f \mapsto (\widetilde{v} \mapsto (-1)^{f(v)} \cdot \widetilde{v})$.*

2. Let $f \in V^\vee$, and let F denote the induced automorphism of the triple (H, θ, T). Let s denote the image of f under the canonical isomorphism $V^\vee \cong T[2](k^s)$. Then $F = \mathrm{Ad}(s)$.

Proof. 1. Immediate.

2. The automorphism f induces the automorphism $\widetilde{\gamma} \mapsto (-1)^{f(\gamma)}\widetilde{\gamma}$ of $\widetilde{\Gamma}$. We must therefore show that $(-1)^{f(\gamma)} = \langle \gamma, s \rangle$. However, this follows from the definition of the element s.

□

3 Plane quartic curves

Let k be a field of characteristic 0 and C a smooth (geometrically connected, projective) non-hyperelliptic curve of genus 3 over k. The canonical embedding then gives C as a plane quartic curve in $\mathbb{P}^2_k$; let us write $\pi : S \to \mathbb{P}^2_k$ for the double cover of $\mathbb{P}^2_k$ branched over S. Then S is a del Pezzo surface of degree 2, i.e. a smooth surface with $-K_S$ ample and $K_S^2 = 2$. (We note that if $k \neq k^s$, then S depends, up to isomorphism, on a choice of defining equation of C; a particular choice will be specified below. The set of isomorphism classes is a torsor for $k^\times/(k^\times)^2$.)

Proposition 3.1. *1. The group $\mathrm{Pic}(S_{k^s})$ is free of rank 8 over $\mathbb{Z}$. Its natural intersection pairing is unimodular.*

2. The sublattice $\Lambda = K_S^\perp \subset \mathrm{Pic}(S_{k^s})$ is a root lattice of type E_7.

3. Suppose that ℓ is a bitangent line of C in its canonical embedding. Then $\pi^{-1}(\ell_{k^s}) = e \cup f$ is a union of two smooth curves of genus 0. Define $\Lambda_\ell = \langle e, f \rangle^\perp \subset \Lambda$. Then Λ_ℓ is a root lattice of type E_6.

4. There are natural isomorphisms $\Lambda^\vee \cong \mathrm{Pic}(S_{k^s})/\mathbb{Z}K_S$ and $\Lambda_\ell^\vee \cong \mathrm{Pic}(S_{k^s})/\langle e, f \rangle$.

5. *Each of* $\mathrm{Pic}(S_{k^s})$, Λ, *and* Λ_ℓ *(when it is defined) has a natural structure of* $\mathbb{Z}[\Gamma_k]$*-module, which respects the intersection pairings.*

Proof. This is all classical; see [GH94, pp. 545–549] and [Dol12, Ch. 8]. It is useful to note that S_{k^s} can be realized as the blow-up of $\mathbb{P}^2_{k^s}$ at 7 points in general position. □

We define N_C to be the image of the natural map $\Lambda/2\Lambda \to \Lambda^\vee/2\Lambda^\vee$. Viewing $C \subset S$ as the ramification locus of π, we see that there is a natural Γ_k-equivariant map $\mathrm{Pic}(S_{k^s}) \to \mathrm{Pic}(C_{k^s})$ given by restriction of line bundles.

Proposition 3.2. *There is a commutative diagram of finite* k*-groups*

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

Proof. We first define the maps. The top map is induced by the composite

$$\Lambda^\vee \cong \mathrm{Pic}(S)/\mathbb{Z}K_S \to \mathrm{Pic}(C)/\mathbb{Z}K_C,$$

which takes image in $(\mathrm{Pic}(C)/\mathbb{Z}K_C)[2] \subset \mathrm{Pic}(C)/\mathbb{Z}K_C$. It is well-defined since $K_S|_C = -K_C$, and if D is any divisor class on S then $2D|_C \sim (D + \iota^* D)|_C$ is a multiple of K_C (where $\iota : S \to S$ is the involution which swaps sheets). The left and right maps are the natural inclusions. To see that the bottom map is derived from the top one, it is enough to note that if D is a divisor class in Λ, then $\deg D|_C = \langle K_S, D\rangle = 0$, so $D|_C \in \mathrm{Pic}^0(C)[2]$.

We now show that the top and bottom maps are isomorphisms. We can assume that $k = k^s$. The groups in the top row have the same cardinality 2^7. If ℓ is a bitangent line of C corresponding to an odd theta characteristic $\kappa \in (\mathrm{Pic}(C)/\mathbb{Z}K_C)[2]$, and $\pi^{-1}(\ell) = e \cup f$, then the image of $e \in \Lambda^\vee$ in $(\mathrm{Pic}(C)/\mathbb{Z}K_C)[2]$ equals κ. The group $(\mathrm{Pic}(C)/\mathbb{Z}K_C)[2]$ is generated by the odd theta characteristics. This shows that the top arrow is surjective, hence an isomorphism. The groups in the bottom row have the same cardinality 2^6, and the bottom arrow is injective. It is therefore also an isomorphism, and this completes the proof. □

As pointed out in the introduction, Proposition 3.2 is essentially classical.

Proposition 3.3. 1. *Under the isomorphism* $N_C \cong \mathrm{Pic}^0(C)[2]$ *of Proposition 3.2, the natural symplectic form on* N_C *is identified with the Weil pairing on* $\mathrm{Pic}^0(C)[2]$.

2. *Let* ℓ *be a* k*-rational bitangent line of* C*, and let* κ *denote the corresponding* k*-rational theta characteristic. Let* $q_\ell : N_C \to \mathbb{F}_2$ *denote the quadratic form corresponding to the isomorphism* $\Lambda_\ell/2\Lambda_\ell \cong N_C$*, and let* $q_\kappa : \mathrm{Pic}^0(C)[2] \to \mathbb{F}_2$ *be the quadratic form induced by* κ*. Then, under the isomorphism* $N_C \cong \mathrm{Pic}^0(C)[2]$ *of Proposition 3.2,* q_ℓ *and* q_κ *are identified.*

Proof. Since q_ℓ and q_κ are quadratic refinements of the symplectic forms, it suffices to prove the second part. These quadratic forms have Arf invariant 1, and therefore have each exactly 28 zeroes. It therefore suffices to show that q_ℓ and q_κ have at least 28 zeroes in common. To do this, we can assume that $k = k^s$. If κ' is any odd theta characteristic of C, then $\kappa - \kappa' \in \mathrm{Pic}^0(C)[2]$ is a zero of q_κ, and there are exactly 28 such elements. (Use the formula $a(q + v) = a(q) + q(v)$ of Lemma 1.4.) We must therefore show that if $v \in \Lambda_\ell$ has image $\kappa - \kappa'$, then $\langle v, v\rangle$ is divisible by 4. This is an easy calculation in $\mathrm{Pic}(S_{k^s})$. □

We now fix a rational point $P \in C(k)$. We define elements of certain tori and their Lie algebras, following [Loo93, §1]. We break into 4 cases, according to the geometry of the point P. Let ℓ denote the tangent line to C at P in $\mathbb{P}^2_k$, and $K = \pi^{-1}(\ell)$ its inverse image, an anti-canonical curve in S.

Case E_7: ℓ not a flex

In the most general case, the tangent line at P to C in its plane embedding meets C at 3 distinct points and therefore has contact of order 2 at P. We define a point of the torus $T = \mathrm{Hom}(\Lambda, \mathbb{G}_m)$, up to inversion. Indeed, in this case K is an irreducible rational curve with a unique nodal singularity at P. There is a unique choice of S for which the tangent directions of K at P are defined over k; we make this choice. Restriction of line bundles induces a homomorphism $\mathrm{Pic}(S) \to \mathrm{Pic}(K)$. An element of $\mathrm{Pic}(S)$ is orthogonal to K_S (under the intersection pairing) if and only if its restriction to K has degree 0, so we obtain an induced homomorphism $\Lambda \to \mathrm{Pic}^0(K)$. Choosing a group isomorphism $\mathrm{Pic}^0(K) \cong \mathbb{G}_m$, we now obtain a point $\kappa_C \in T(k)$, well-defined up to inversion.

Case $\mathfrak{e}_7$: ℓ a flex, not a hyperflex

We now suppose that the tangent line to C at P has contact of order exactly 3, and fix in addition a non-zero tangent vector t in the Zariski tangent space of C at P. We define a point κ_C of the Lie algebra $\mathfrak{t}$ of the torus $T = \mathrm{Hom}(\Lambda, \mathbb{G}_m)$, well-defined up to multiplication by -1. The curve K is irreducible and rational with a unique cuspidal singularity, at P. Restriction induces a morphism $\Lambda \to \mathrm{Pic}^0(K)$. To write down κ_C, it therefore suffices to give a normalization of the isomorphism $\mathrm{Pic}^0(K) \cong \mathbb{G}_a$, at least up to sign.

To do this we find it convenient to introduce explicit co-ordinates. Using Riemann–Roch, it is easy to show that there are unique functions $x, y \in k(C)^\times$ satisfying the following conditions:

- $x \in H^0(C, \mathcal{O}_C(2P + Q))$ and $y \in H^0(C, \mathcal{O}_C(3P - Q))$.
- Let $z \in \mathcal{O}_{C,P}$ be a co-ordinate such that $dz(t) = 1$. Then $x = z^{-2} + \dots$ and $y = z^{-3} + \dots$ locally at P.
- x and y satisfy the equation

$$y^3 = x^3 y + p_{10}x^2 + x(p_2 y^2 + p_8 y + p_{14}) + p_6 y^2 + p_{12} y + p_{18}$$

for some $p_2, \dots, p_{18} \in k$.

Then we can choose homogeneous co-ordinates X, Y, Z on $\mathbb{P}^2_k$ such that C is given by the equation

$$Y^3 Z = X^3 Y + p_{10}X^2 Z^2 + X(p_2 Y^2 Z + p_8 Y Z^2 + p_{14} Z^3) + p_6 Y^2 Z^2 + p_{12} Y Z^3 + p_{18} Z^4,$$

and this equation is uniquely determined by the triple (C, P, t). We use it to define the surface S. Then a chart in S is the affine surface

$$w^2 = z_0 - (x_0^3 + p_{10}x_0^2 z_0^2 + \dots + p_{18} z_0^4),$$

where $x_0 = X/Y$, $z_0 = Z/Y$, and the curve K is given locally by the equation $z_0 = 0$. Let $f : \widetilde{K} \to K$ be the normalization. A co-ordinate in $\widetilde{K}$ at the point above P is given by w/x_0. We use the isomorphism $\mathbb{G}_a \cong \mathrm{Pic}^0(K)$, $t \mapsto \delta(1 + tw/x_0)$, where δ is the connecting homomorphism of the exact sequence of sheaves on K:

$$0 \longrightarrow \mathcal{O}_K^\times \longrightarrow f_*\mathcal{O}_{\widetilde{K}}^\times \longrightarrow f_*\mathcal{O}_{\widetilde{K}}^\times / \mathcal{O}_K^\times \longrightarrow 0.$$

Case E_6: ℓ a bitangent, not a hyperflex

We now suppose that ℓ meets C at two distinct points, say P, Q, and that it has contact of order 2 at each point. Then the root subsystem $\Lambda_\ell \subset \Lambda$ is defined, and we will define a point of the torus $T = \mathrm{Hom}(\Lambda_\ell, \mathbb{G}_m)$. The curve $K_{k^s} = e_{k^s} \cup f_{k^s}$ is a union of two smooth conics, which meet transversely at two distinct points. We choose S so that these conics are defined over k. We thus obtain a homomorphism $\Lambda_\ell \to \mathrm{Pic}^0(K)^-$, where $(?)^-$ denotes the -1-eigenspace of the involution induced by switching sheets. The group $\mathrm{Pic}^0(K)^-$ is canonically isomorphic to $\mathbb{G}_m$, the isomorphism being specified as in [Loo93, §1.12]: if $s \in \mathbb{G}_m$ tends to 0, then e is contracted to P and f is contracted to Q. We define $\kappa_C \in T(k)$ to be the point obtained via this isomorphism. If the roles of e and f are reversed, then κ_C is replaced by κ_C^{-1}.

Case $\mathfrak{e}_6$: ℓ a hyperflex

We now suppose that ℓ has contact of order 4 with C at P, and fix in addition a non-zero tangent vector t in the Zariski tangent space of C at P. Then the root system $\Lambda_\ell \subset \Lambda$ is defined, and we will define a point κ_C of the Lie algebra $\mathfrak{t}$ of the torus $T = \mathrm{Hom}(\Lambda_\ell, \mathbb{G}_m)$. Restriction once more induces a map $\Lambda_\ell \to \mathrm{Pic}^0(K)^-$, and we obtain a point $\kappa_C \in \mathfrak{t}$ by specifying an isomorphism $\mathrm{Pic}^0(K)^- \cong \mathbb{G}_a$. To do this, we again introduce explicit co-ordinates. There are unique functions $x, y \in k(C)^\times$ satisfying the following conditions:

- $x \in H^0(C, \mathcal{O}_C(3P))$ and $y \in H^0(C, \mathcal{O}_C(4P))$.
- Let $z \in \mathcal{O}_{C,P}$ be a co-ordinate such that $dz(t) = 1$. Then $x = z^{-3} + \dots$ and $y = z^{-4} + \dots$ locally at P.
- x and y satisfy the equation

$$y^3 = x^4 + y(p_2x^2 + p_5x + p_8) + p_6x^2 + p_9x + p_{12}$$

  for some $p_2, \dots, p_{12} \in k$.

Then we can choose homogeneous co-ordinates X, Y, Z on $\mathbb{P}^2_k$ such that C is given by the equation

$$Y^3Z = X^4 + Y(p_2X^2Z + p_5XZ^2 + p_8Z^3) + p_6X^2Z^2 + p_9XZ^3 + p_{12}Z^4,$$

and this equation is uniquely determined by the triple (C, P, t). We use it to define the surface S. A chart in S is the affine surface

$$w^2 = z_0 - (x_0^4 + \dots + p_{12}z_0^4),$$

where $x_0 = X/Y$ and $z_0 = Z/Y$. The curve $K = e \cup f$ is a union of 2 smooth conics which are tangent at the point P, and is given in the above chart by the equation $z_0 = 0$. A co-ordinate at P in both e and f is given by x_0. We use the isomorphism $\mathbb{G}_a \cong \mathrm{Pic}^0(K)^-$, $t \mapsto \delta(1 + tx, 1)$, where δ is the connecting homomorphism in the exact sequence of sheaves on K:

$$0 \longrightarrow \mathcal{O}_K^\times \longrightarrow \mathcal{O}_e^\times \oplus \mathcal{O}_f^\times \longrightarrow (\mathcal{O}_e^\times \oplus \mathcal{O}_f^\times)/\mathcal{O}_K^\times \longrightarrow 0.$$

If the roles of e and f are reversed, then κ_C is replaced by $-\kappa_C$.

In each case, we write $\mathcal{S} : k\text{-alg} \to \mathrm{Sets}$ for the functor of data $(C, P, \dots)$ considered above. This means:

- In case E_7, $\mathcal{S}$ is the functor of pairs (C, P), where C is a non-hyperelliptic curve of genus 3 and P is a point of C which is not a flex or a bitangent in the canonical embedding. More precisely, for each $A \in k$-alg, $\mathcal{S}(A)$ is the set of isomorphism classes of pairs (π, P) consisting of a proper flat morphism $\pi : C \to \mathrm{Spec}\, A$ and a section $P : \mathrm{Spec}\, A \to C$ of π such that for each geometric point $\overline{s}$ of $\mathrm{Spec}\, A$, the pair $(C_{\overline{s}}, P_{\overline{s}})$ is of this type.
- In case $\mathfrak{e}_7$, $\mathcal{S}$ is the functor of triples (C, P, t), where C is a non-hyperelliptic curve of genus 3, P is a point of C which is a flex (but not a hyperflex) in the canonical embedding, and t is a non-zero element of the Zariski tangent space of C at P.
- In case E_6, $\mathcal{S}$ is the functor of pairs (C, P), where C is a non-hyperelliptic curve of genus 3 and P is a point such that T_PC is a bitangent in the canonical embedding of C.
- In case $\mathfrak{e}_6$, $\mathcal{S}$ is the functor of triples (C, P, t), where C is a non-hyperelliptic curve of genus 3, P is a point which is a hyperflex in the canonical embedding, and t is a non-zero element of the Zariski tangent space of C at P.

We can now state the following reformulation of some results of Looijenga:

Theorem 3.4. *Suppose that $k = k^s$.*

- *In case E_7, let Λ_0 be a root lattice of the corresponding type, and let $T_0 = \mathrm{Hom}(\Lambda_0, \mathbb{G}_m)$. Then the Weyl group $W = W(\Lambda_0)$ acts on T_0, and the assignment $(C, P) \to \kappa_C$ induces a bijection $\mathcal{S}(k) \to (T_0^{rss} /\!\!/ W)(k)$.*

- *In case E_6, let Λ_0 be a root lattice of the corresponding type, and let $T_0 = \mathrm{Hom}(\Lambda_0, \mathbb{G}_m)$. Fix a non-trivial class $e_0 \in \Lambda_0^\vee / \Lambda_0$. Then the Weyl group $W = W(\Lambda_0)$ acts on T_0, and the assignment $(C, P) \to \kappa_C$ induces a bijection $\mathcal{S}(k) \to (T_0^{rss} /\!\!/ W)(k)$.*

- *In case $\mathfrak{e}_7$, let Λ_0 be a root lattice of the corresponding type, and let $\mathfrak{t}_0 = \mathrm{Hom}(\Lambda_0, \mathbb{G}_a)$. Then the Weyl group $W = W(\Lambda_0)$ acts on $\mathfrak{t}_0$, and the assignment $(C, P, t) \to \kappa_C$ induces a bijection $\mathcal{S}(k) \to (\mathfrak{t}_0^{rss} /\!\!/ W)(k)$.*

- *In case $\mathfrak{e}_6$, let Λ_0 be a root lattice of the corresponding type, and let $\mathfrak{t}_0 = \mathrm{Hom}(\Lambda_0, \mathbb{G}_a)$. Fix a non-trivial class $e_0 \in \Lambda_0^\vee / \Lambda_0$. Then the Weyl group $W = W(\Lambda_0)$ acts on $\mathfrak{t}_0$, and the assignment $(C, P, t) \to \kappa_C$ induces a bijection $\mathcal{S}(k) \to (\mathfrak{t}_0^{rss} /\!\!/ W)(k)$.*

The subscript 'rss' indicates the open subset of regular semisimple elements, i.e. the complement of all root hyperplanes.

Proof. We first explain what happens in the case of type E_7. For any field k (not necessarily separably closed), and any pair $(C, P) \in \mathcal{S}(k)$, we have constructed a point κ_C of the torus $T = \mathrm{Hom}(\Lambda, \mathbb{G}_m)$, where Λ is the root lattice with $\mathbb{Z}[\Gamma_k]$-action constructed above using the curve C.

When $k = k^s$, this action is trivial, and we can choose an isomorphism $\Lambda \cong \Lambda_0$ of root lattices, which is well-defined up to the action of the group $\mathrm{Aut}(\Lambda_0)$. The Dynkin diagram of type E_7 has no extra symmetries, so in fact $\mathrm{Aut}(\Lambda_0) = W$ (see [Bou02, Ch. VI, No. 1.5, Proposition 16]). We thus obtain an isomorphism $T \cong T_0$, well-defined up to the action of W, and a point $\kappa_C \in (T_0 /\!\!/ W)(k) = T_0(k)/W$. Note that κ_C is well-defined only up to inversion, but W contains the element -1. The result [Loo93, Proposition 1.8] now states that the point κ_C is regular semisimple, and that the map $\mathcal{S}(k) \to (T_0^{\mathrm{rss}} /\!\!/ W)(k)$ is a bijection. (In fact, the result is stated when $k = \mathbb{C}$, but the proof is algebro-geometric in nature and goes through without change when k is any separably closed field of characteristic 0.) Indeed, the construction given there is exactly the one we have explicated above.

We now explain what happens in the case of type E_6. Our construction gives a point $\kappa_C = \kappa(C, P, e)$ of the torus $T = \mathrm{Hom}(\Lambda_\ell, \mathbb{G}_m)$, where e is a choice of irreducible component of the strict transform of the bitangent line ℓ at P inside S; we have $\kappa(C, P, f) = \kappa(C, P, e)^{-1}$. The automorphism group $\mathrm{Aut}(\Lambda_0)$ is now strictly larger than W, because the Dynkin diagram of type E_6 has extra symmetries, the quotient $\mathrm{Aut}(\Lambda_0)/W$ being generated by the automorphism -1. In fact, these ambiguities cancel out.

Indeed, the quotient $\Lambda_\ell^\vee / \Lambda_\ell$ is cyclic of order 3, and the quotient $\mathrm{Aut}(\Lambda_0)/W$ acts faithfully on it. We can mark the non-trivial elements of $\Lambda_\ell^\vee / \Lambda_\ell$ by e and f as follows: the class corresponding to e is the one containing the classes of the 27 lines on S which intersect e (but not f), and the class corresponding to f is the one containing the classes of the 27 lines which intersect f (but not e). Let $\lambda_e : \Lambda_\ell \to \Lambda_0$ be an isomorphism which sends the class in $\Lambda_\ell^\vee / \Lambda_\ell$ corresponding to e to e_0. Then λ_e is determined up to the action of $W(\Lambda_0)$. The point $\lambda_e \kappa(C, P, e) \in (T_0 /\!\!/ W)(k)$ is therefore well-defined, and we have $\lambda_f \kappa(C, P, f) = (\lambda_e \kappa(C, P, e)^{-1})^{-1} = \lambda_e \kappa(C, P, e) \bmod W_0$. This gives a map $\mathcal{S}(k) \to (T_0 /\!\!/ W)(k)$ which is independent of any choices, and which is shown to be a bijection into $(T_0^{\mathrm{rss}} /\!\!/ W)(k)$ by [Loo93, Proposition 1.13].

The Lie algebra cases are very similar, making reference to [Loo93, Proposition 1.11] and [Loo93, Proposition 1.15]. □

3.1 Construction of orbits

We now come to the most important part of this paper. In each of the cases E_7, $\mathfrak{e}_7$, E_6 and $\mathfrak{e}_6$ described above, we give a semisimple group G over k, together with a G-variety X, and write down orbits in $G(k)\backslash X(k)$ corresponding to elements of the groups $J(k)/2J(k)$. We must first fix 'reference data'. This means:

- In cases E_7 and $\mathfrak{e}_7$, we fix a choice of pair (H, θ), where H is a split adjoint simple group over k of type E_7, and θ is an involution satisfying the conditions of Proposition 1.9. We define $G = (H^\theta)^\circ$, and

fix an inner class of isomorphisms $\mathfrak{g} \cong \mathfrak{sl}_8$; equivalently, we distinguish one of the two 8-dimensional representations of $\mathfrak{g}$ as the 'standard representation'. The group H has no outer automorphisms, but the group H^θ has two connected components, and the non-identity component acts on the identity component G by outer automorphisms, exchanging the two choices of standard representation. Indeed, the component group can be calculated using [Ree10, Proposition 2.1] and the Kac co-ordinates of the inner automorphism θ, which appear in the tables in [RLYG12]. The proof of [Ree10, Proposition 2.1] shows that we can find a representative of the non-trivial component which normalizes a maximal torus of G but which does not act on this torus in the same way as any Weyl element of G; the induced automorphism of G must therefore be outer.

- In cases E_6 and $\mathfrak{e}_6$, we fix a choice of pair (H, θ), where H is a split adjoint simple group over k of type E_6, and θ is an involution satisfying the conditions of Proposition 1.9. We define $G = (H^\theta)^\circ = H^\theta$, and distinguish one of the two 27-dimensional representations of $\mathfrak{h}$ as the 'standard representation'. The connectedness of H^θ can be shown as above using the papers [Ree10, RLYG12].

We recall that in §1.4 we have defined two G-varieties Y and V in terms of the pair (H, θ). We use these to define the G-variety X as follows:

- In cases E_7 and E_6, we define $X = Y \subset H$.
- In cases $\mathfrak{e}_7$ and $\mathfrak{e}_6$, we define $X = V \subset \mathfrak{h}$.

In each case there is a G-invariant open subscheme $X^{\mathrm{s}} \subset X$ of regular semisimple (equivalently, stable) orbits. We can now state our first main theorem:

Theorem 3.5. *In each case, the assignment $(C, P, \dots) \mapsto \kappa_C$ determines a map*

$$\mathcal{S}(k) \to G(k)\backslash X^s(k). \tag{3.1}$$

If $k = k^s$, then this map is bijective.

We observe that the theorem has already been proved in the case $k = k^s$. Indeed, in this case, the set $G(k)\backslash X^s(k)$ can be understood, via the Chevalley isomorphisms of §1.4, in terms of Weyl group orbits in a maximal torus or Cartan subalgebra. Via this isomorphism, the theorem becomes Theorem 3.4. Our problem, then, is to lift this construction so that it works over any field. This also explains the need for the 'reference data' described at the beginning of §3.1: it will provided the correct rigidification, in analogy with what happens in the proof of Theorem 3.4.

We remark that in cases $\mathfrak{e}_7$ and $\mathfrak{e}_6$, the functor $\mathcal{S}$ is representable (as the triples (C, P, t) have no automorphisms). This implies that for any field k, the map $\mathcal{S}(k) \to G(k)\backslash V^{\mathrm{s}}(k)$ is injective, and the composite $\mathcal{S}(k) \to G(k)\backslash V^{\mathrm{s}}(k) \to (V^{\mathrm{s}}/\!\!/G)(k)$ is bijective.

Proof. Let us first treat the E_7 case. Let $(C, P) \in \mathcal{S}(k)$, and let $V = \Lambda/2\Lambda$. The point κ_C defined above lies in $T(k)$, where $T = \mathrm{Hom}(\Lambda, \mathbb{G}_m)$, and is well-defined up to inversion. We are going to define an extension $\widetilde{V}$ of V, with Γ_k-action, and then apply the constructions of §2 to build a group around the torus T. Let $\widetilde{H}_{\mathcal{L}}$ be the Heisenberg group defined in §1.3; it fits into an exact sequence

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \widetilde{H}_{\mathcal{L}} \longrightarrow \mathrm{Pic}^0(C)[2] \longrightarrow 1.$$

According to Proposition 3.2, there is a canonical injection $\mathrm{Pic}^0(C)[2] \hookrightarrow V^\vee$ of finite k-groups. Dualizing, we obtain a surjection $V \to \mathrm{Pic}^0(C)[2]$, and we push out the above extension by this surjection to obtain a central extension

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \widetilde{E} \longrightarrow V \longrightarrow 1.$$

The commutator pairing of $\widetilde{E}$ descends to the natural symplectic form on V (since this is true for $\widetilde{H}_{\mathcal{L}}$, by Lemma 1.7, and the kernel of $V \to \mathrm{Pic}^0(C)[2]$ is exactly the radical of this symplectic form). Since V is endowed with a Γ_k-invariant quadratic form $q : V \to \mathbb{F}_2$, we can define a character $\chi_q : \widetilde{E} \to \mathbb{G}_m$ by the

formula $\widetilde{e} \mapsto (-1)^{q(e)}\widetilde{e}^2$. This makes sense since for any $\widetilde{e} \in \widetilde{E}$, we have $\widetilde{e}^2 \in \mathbb{G}_m$. Taking $\widetilde{V} = \ker \chi_q$ then gives the desired extension

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

(This is a slight variant on the procedure leading to the extension (1.1).) Note that if $W = H^0(\mathrm{Pic}^0(C), \mathcal{L})$, then there is a natural homomorphism of k-groups $\widetilde{V} \to \mathrm{GL}(W)$. Indeed, the group $\widetilde{H}_{\mathcal{L}}$ acts on W by definition by pullback of sections; we can then pull back this action along the homomorphism $\widetilde{V} \to \widetilde{H}_{\mathcal{L}}$. If $k = k^s$, then this is an 8-dimensional irreducible representation of the abstract group $\widetilde{V}(k^s)$, which sends -1 to $-\mathrm{id}_{W_{k^s}}$.

In §2 we have associated to the triple $(\Lambda, \widetilde{V}, W)$ a simple adjoint group H_0 of type E_7, together with a stable involution θ and maximal torus $T \subset H_0$, and a representation of $\mathfrak{g}_0 = \mathfrak{h}_0^\theta$ on W. By definition, the torus T is canonically isomorphic to $\mathrm{Hom}(\Lambda, \mathbb{G}_m)$, and θ acts on it by $t \mapsto t^{-1}$. The group H_0 is split; in fact, since $\mathfrak{g}_0$ is a form of $\mathfrak{sl}_8$ with an 8-dimensional representation which is defined over k, $\mathfrak{g}_0$ is split. The Lie algebras $\mathfrak{g}_0$ and $\mathfrak{h}_0$ are semisimple Lie algebras of rank 7, so this implies that $\mathfrak{h}_0$ must also be split.

By Proposition 1.9, there is an isomorphism $\varphi : H \to H_0$ satisfying $\theta_0\varphi = \varphi\theta$. This isomorphism is defined uniquely up to $H^\theta(k)$-conjugacy. The group H^θ is disconnected, with two connected components; the non-trivial component acts on the connected component $G = (H^\theta)^\circ$ by outer automorphisms. In order to pin down the isomorphism φ up to $G(k)$-conjugacy, we observe that $\varphi^*(W)$ is an irreducible 8-dimensional representation of $\mathfrak{g}$, which is therefore isomorphic either to the fixed 'standard representation' or its dual. After possibly modifying φ, we can therefore assume that φ carries W to the standard representation of $\mathfrak{g}$. The isomorphism φ is then indeed determined uniquely up to $G(k)$-conjugacy.

It follows that the orbit $G(k) \cdot \varphi^{-1}(\kappa_C) \in G(k)\backslash Y(k)$ is well-defined. (Note in particular that κ_C is defined only up to inversion, but that θ acts on κ_C by inversion and lies in $G(k)$ (in fact in the centre of $G(k)$), so the orbit is independent of any choices.) To complete the proof in this case, we must show that $\varphi^{-1}(\kappa_C)$ is stable (equivalently, regular semisimple in T), and that the map we have defined is a bijection if $k = k^s$. This follows from the discussion preceding the proof of this theorem, and Theorem 3.4.

Let us now treat the E_6 case. The inverse image $\pi^{-1}(\ell) = e \cup f$ of the bitangent ℓ at P in the surface S determines the root lattice Λ_ℓ, and we set $V = \Lambda_\ell/2\Lambda_\ell$. The natural symplectic pairing on V is non-degenerate, and the quadratic form $q : V \to \mathbb{F}_2$ arising from the form on on Λ_ℓ agrees with the quadratic form on V arising from the isomorphism $V \cong \mathrm{Pic}^0(C)[2]$ and the odd theta characteristic κ corresponding to ℓ, by Proposition 3.3. We then have the Heisenberg group $\widetilde{H}_{\mathcal{L}}$:

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \widetilde{H}_{\mathcal{L}} \longrightarrow \mathrm{Pic}^0(C)[2] \longrightarrow 1.$$

Pushing out by the isomorphism $V \cong \mathrm{Pic}^0(C)[2]$, we obtain an extension (isomorphic to $\widetilde{H}_{\mathcal{L}}$):

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \widetilde{E} \longrightarrow V \longrightarrow 1.$$

We define a character $\chi_q : \widetilde{E} \to \mathbb{G}_m$ by the formula $\widetilde{e} \mapsto (-1)^{q(e)}\widetilde{e}^2$, and set $\widetilde{V} = \ker \chi_q$. Then $\widetilde{V}$ is an extension

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

We define $W = H^0(\mathrm{Pic}^0(C), \mathcal{L})$; then $\widetilde{V}$ acts on W through the homomorphism $\widetilde{V} \to \widetilde{H}_{\mathcal{L}}$. Applying the constructions of §2 to the triple $(\Lambda_\ell, \widetilde{V}, W)$, we obtain an adjoint group H_0 of type E_6 equipped with a stable involution θ_0, together with an action of the Lie algebra $\mathfrak{g}_0 = \mathfrak{h}_0^{\theta_0}$ on W. Since $\mathfrak{g}_0$ is an inner form of $\mathfrak{sp}_8$ and has an 8-dimensional representation defined over k, it must be split. This implies that H_0 has split rank at least 4; by the classification of forms of E_6 [Tit66, pp. 58–59], we see that H_0 must be quasi-split, and split by a quadratic extension. This quadratic extension is the smallest extension splitting the Galois action on $\Lambda_\ell^\vee/\Lambda_\ell$. Since the geometric irreducible components e and f of $\pi^{-1}(\ell)$ are defined over k, this action is trivial, and we see that H_0 is also split.

Applying Proposition 1.9 once more, we see that there is an isomorphism $\varphi_e : H \to H_0$ such that $\varphi_e\theta = \theta_0\varphi_e$. Such an isomorphism is determined up to $H^\theta(k) = G(k)$-conjugacy (as H^θ is connected in this

case). Moreover, we can assume that under the isomorphism φ_e, the minuscule representation of H_0 with weights in $\Lambda_\ell^\vee/\Lambda_\ell$ corresponding to e is identified with the 'standard representation' of H.

The orbit $G(k)\cdot\varphi_e^{-1}(\kappa_C)$ is then well-defined: reversing the roles of e and f in our construction replaces $\kappa_C=\kappa(C,P,e)$ by $\kappa(C,P,f)=\kappa(C,P,e)^{-1}$, and θ_0 is an outer automorphism, acting on $\Lambda_\ell^\vee/\Lambda_\ell\cong\mathbb{Z}/3\mathbb{Z}$ as multiplication by -1, so we can take $\varphi_f=\varphi_e\circ\theta_0$. Then we have

$$G(k)\cdot\varphi_f^{-1}(\kappa(C,P,f))=G(k)\cdot\varphi_f^{-1}(\theta_0(\kappa(C,P,e))=G(k)\cdot\varphi_e^{-1}(\kappa(C,P,e)).$$

This shows that we have constructed a well-defined map $\mathcal{S}(k)\to G(k)\backslash X(k)$. The rest of the theorem in this case follows from the discussion preceding the proof of this theorem, and Theorem 3.4.

The arguments in the Lie algebra cases are very similar, with maximal tori replaced by Cartan subalgebras. We omit the details. □

Fix $x=(C,P,\dots)\in\mathcal{S}(k)$. Let $\pi: X\to X/\!\!/G$ denote the natural quotient map, and let $X_x=\pi^{-1}\pi(x)$. Then we know that $X_x\subset X^{\mathrm{s}}$ consists of a single G-orbit (see §1.4), but $X_x(k)$ may break up into several $G(k)$-orbits which all become conjugate over k^s. Let J_x denote the Jacobian of C. We now state our second main theorem, which shows how to construct elements of the set $G(k)\backslash X_x(k)$ from the set $J_x(k)$:

Theorem 3.6. *With notation as above, there is a canonical map*

$$J_x(k)/2J_x(k)\hookrightarrow G(k)\backslash X_x(k). \tag{3.2}$$

It is functorial in k in the obvious sense.

The map (3.2) will extend the map of Theorem 3.5, in the sense that the image of the identity element of $J_x(k)/2J_x(k)$ under (3.2) equals the image of $x\in\mathcal{S}(k)$ under (3.1).

Proof. The proof is a twist of the proof of Theorem 3.5, using the ideas of §1.3. We treat first the E_7 case. Let $A\in J_x(k)$ be a rational point. Choose $B\in J_x(k^s)$ such that $[2](B)=A$. Then the field of definition of the line bundle $t_B^*\mathcal{L}$ is equal to k, and we choose a bundle $\mathcal{L}_B$ over k which becomes isomorphic to $t_B^*\mathcal{L}$ over k^s. We continue to denote $\Lambda=\mathrm{Pic}(S_{k^s})$, $V=\Lambda/2\Lambda$, and associate to $\mathcal{L}_B$ the Heisenberg group $\widetilde{H}_{\mathcal{L}_B}$, which fits into an exact sequence

$$1\longrightarrow\mathbb{G}_m\longrightarrow\widetilde{H}_{\mathcal{L}_B}\longrightarrow J_x[2]\longrightarrow 1.$$

Arguing exactly as in the proof of Theorem 3.5, we obtain an extension

$$1\longrightarrow\{\pm1\}\longrightarrow\widetilde{V}_B\longrightarrow V\longrightarrow 1,$$

together with a homomorphism $\widetilde{V}_B\to\widetilde{H}_{\mathcal{L}_B}$ through which the group $\widetilde{V}_B$ acts on the space $W_B=H^0(J_x,\mathcal{L}_B)$, an 8-dimensional k-vector space. Over k^s, this defines an irreducible representation of the abstract group $\widetilde{V}_B(k^s)$.

Using the constructions of §2, we associate to the triple $(\Lambda,\widetilde{V}_B,W_B)$ a group H_B with involution θ_B, maximal torus $T_B\cong\mathrm{Hom}(\Lambda,\mathbb{G}_m)$, and an action of the Lie algebra $\mathfrak{g}_B=\mathfrak{h}_B^{\theta_B}$ on W_B. Just as in the proof of Theorem 3.5, the existence of W_B implies that the groups H_B and G_B are split, and $T_B(k)$ has a point κ_C, well-defined up to inversion. By Proposition 1.9, we can find an isomorphism $\varphi_B: H\to H_B$ which intertwines θ and θ_B, and under which W_B corresponds to the 'standard representation' of $\mathfrak{g}\cong\mathfrak{sl}_8$. The choice of φ_B is then unique up to the action of $G(k)$, and we associate to the point B the orbit $G(k)\cdot\varphi_B^{-1}(\kappa_C)\subset Y_x(k)$.

We observe that if $A=B=0$, the identity of $J_x(k)$, then the above construction reduces to that of Theorem 3.5. In general, we must show that the orbit $G(k)\cdot\varphi_B^{-1}(\kappa_C)\subset P_x(k)$ depends only on the image of A in $J_x(k)/2J_x(k)$ (and not on the choice of B), and that distinct elements of $J_x(k)/2J_x(k)$ give rise to distinct orbits. Let $\varphi_0^{-1}(\kappa_C)\in Y_x(k)$ be the point constructed in the proof of Theorem 3.5. Since $G(k^s)$ acts transitively on $P_x(k^s)$, a well-known principle asserts that there is a canonical bijection

$$G(k)\backslash Y_x(k)\cong\ker\left(H^1(k,Z_G(\varphi_0^{-1}(\kappa_C)))\to H^1(k,G)\right), \tag{3.3}$$

under which the base orbit $G(k)\cdot\varphi_0^{-1}(\kappa_C)$ corresponds to the marked element; see, for example, [BG14, Proposition 1]. By [Tho13, Corollary 2.10] and Proposition 3.2, there is a canonical isomorphism

$$Z_G(\varphi_0^{-1}(\kappa_C))\cong Z_{G_0}(\kappa_C)\cong \text{image }(V\to V^\vee)\cong J_x[2].$$

We will show that under the composite

$$G(k)\backslash Y_x(k)\hookrightarrow H^1(k,Z_G(\varphi_0^{-1}(\kappa_C)))\cong H^1(k,J_x[2]),$$

the orbit $G(k)\cdot\varphi_B^{-1}(\kappa_C)$ is mapped to the image of A under the 2-descent homomorphism of §1.3.

The pullback t_B^* defines a canonical isomorphism $\widetilde{V}\cong\widetilde{V}_B$ over k^s by the formula of (1.2). This gives rise to an isomorphism of triples $F:(H_0,\theta_0,T_0)\cong(H_B,\theta_B,T_B)$ which induces the identity on $\mathrm{Hom}(\Lambda,\mathbb{G}_m)$ under the identification of this torus with T_0 and T_B. According to Lemma 2.4, we can identify $F^{-1\sigma}F$ with an element of $V^\vee$. Lemma 1.8 now implies that this element in fact lies in the image of the homomorphism $V\to V^\vee$, and that under the identification of this image with $J_x[2]$, is identified with the cocycle $\sigma\mapsto {}^\sigma B-B$. This identity of cocycles implies the desired identity of cohomology classes, and completes the proof in this case.

The proof of the theorem in the remaining cases E_6, $\mathfrak{e}_7$, and $\mathfrak{e}_6$ simply requires analogous modifications to the proof of Theorem 3.5. We work out the E_6 case here. Let us therefore take $x=(C,P)\in\mathcal{S}(k)$, so that P is a point such that $T_PC=\ell$ is a bitangent in the canonical embedding of the curve C. The root lattice Λ_ℓ is defined, and we define $V=\Lambda_\ell/2\Lambda_\ell$. The natural symplectic pairing on V is non-degenerate, and the quadratic form $q:V\to\mathbb{F}_2$ arising from the form on on Λ_ℓ agrees with the quadratic form on V arising from the isomorphism $V\cong J_x[2]$ and the odd theta characteristic κ corresponding to ℓ, by Proposition 3.3. Let $A\in J_x(k)$, and choose a point $B\in J_x(k^s)$ with $[2](B)=A$. Let $\mathcal{L}_B$ be a descent of the line bundle $t_B^*\mathcal{L}$ to k. We then have the Heisenberg group $\widetilde{H}_{\mathcal{L}_B}$:

$$1\longrightarrow\mathbb{G}_m\longrightarrow\widetilde{H}_{\mathcal{L}_B}\longrightarrow J_x[2]\longrightarrow 1.$$

Arguing exactly as in the proof of Theorem 3.5, we obtain an extension

$$1\longrightarrow\{\pm1\}\longrightarrow\widetilde{V}_B\longrightarrow V\longrightarrow 1,$$

and $\widetilde{V}_B$ acts on the 8-dimensional k-vector space $W_B=H^0(J_x,\mathcal{L}_B)$ through a homomorphism $\widetilde{V}_B\to\widetilde{H}_{\mathcal{L}_B}$. We can apply the constructions of §2 to the triple $(\Lambda_\ell,\widetilde{V}_B,W_B)$ to obtain a group H_B with involution θ_B, maximal torus $T_B\cong\mathrm{Hom}(\Lambda,\mathbb{G}_m)$, and an action of the Lie algebra $\mathfrak{g}_B=\mathfrak{h}_B^{\theta_B}$ on W_B. The existence of W_B implies that the groups H_B and G_B are split, and $T_B(k)$ has a point $\kappa_C=\kappa(C,P,e)$ which depends on a choice of component e of $\pi^{-1}(\ell)=e\cup f$. By Proposition 1.9, we can find an isomorphism $\varphi_{B,e}:H\to H_B$ which intertwines θ and θ_B, and under which the 'standard representation' of $\mathfrak{h}$ corresponds to the minuscule representation of $\mathfrak{h}_B$ corresponding to the class of e in $\Lambda_\ell^\vee/\Lambda_\ell$. The choice of $\varphi_{B,e}$ is then unique up to the action of $G(k)$, and we associate to the point B the orbit $G(k)\cdot\varphi_{B,e}^{-1}(\kappa(C,P,e))\subset Y_x(k)$. Just as in the E_7 case, we can check that the map $B\mapsto G(k)\cdot\varphi_{B,e}^{-1}(\kappa(C,P,e))$ descends to an injection $J_x(k)/2J_x(k)\hookrightarrow G(k)\backslash Y_x(k)$. This completes the proof. □

3.2 An example

To illustrate our theorem, we describe explicitly what happens in the $\mathfrak{e}_6$ case, when $k=\mathbb{R}$. Then the reference group H is a split adjoint group of type E_6 over $\mathbb{R}$, $H^\theta=G$ is isomorphic to PSp_8, a projective symplectic group in 8 variables, and $V=\mathfrak{h}^{d\theta=-1}$ is a 42-dimensional irreducible subrepresentation of $\wedge^4(8)$. The corresponding family of curves is the family (C,P,t) of smooth non-hyperelliptic genus 3 curves, equipped with a point P which is a hyperflex in the canonical embedding, and a non-zero Zariski tangent vector $t\in T_PC$. It consists of the smooth members in the family

$$y^3=x^4+y(p_2x^2+p_5x+p_8)+p_6x^2+p_9x+p_{12}$$

(here we are using the affine chart which makes P the unique point at infinity). For each tuple

$$(p_2, p_5, p_8, p_6, p_9, p_{12}) \in \mathbb{R}^6$$

for which this curve is smooth, we can write down the following data:

- Topological invariants of the curve $C(\mathbb{R}) \subset \mathbb{P}^2(\mathbb{R})$: following [GH81], we write $n(C)$ for the number of connected components of $C(\mathbb{R})$, and $a(C) = 0$ or 1 depending on whether or not $C(\mathbb{C}) - C(\mathbb{R})$ is disconnected.
- A stable G-orbit $V_x \subset V^s$, and an $H(\mathbb{R})$-conjugacy class of maximal tori $T \subset H$ (T is the stabilizer in H of the base orbit in $V_x(\mathbb{R})$, which is regular semisimple).
- An injection $J(\mathbb{R})/2J(\mathbb{R}) \hookrightarrow G(\mathbb{R})\backslash V_x(\mathbb{R})$, where J is the Jacobian of the curve C.

The isomorphism classes of tori in H are in bijection with the conjugacy class of elements in the Weyl group W of order 2 [Ree11, §6]. It turns out that these correspond to the possible topological types of the curve $C(\mathbb{R})$ in $\mathbb{P}^2(\mathbb{R})$, as follows:

conjugacy class	$n(C)$	$a(C)$	no. of real bitangents	$\#J(\mathbb{R})/2J(\mathbb{R})$	$\#G(\mathbb{R})\backslash V_x(\mathbb{R})$
1	4	0	28	2^3	36
s_1	3	1	16	2^2	10
s_1s_2	2	1	8	2	3
$s_1s_2s_3$	1	1	4	1	1
τ	2	0	4	2	3

The table should be interpreted as follows: suppose that a curve C has the given invariants. (It follows from the table on [GH81, p. 174] that the only possible values for the pair $(n(C), a(C))$ are the ones listed above.) Then the real structure on the torus T is the one determined by the Weyl element in the left-hand column, and the data in the remaining three columns is as given. Here $s_1, s_2, s_3 \in W$ are commuting simple reflections, and $\tau \in W$ may be constructed as follows: choose a D_4 root system inside Λ. Then $-1 \in W(D_4)$, and τ is the element that acts as -1 on the span of the D_4 roots, and as $+1$ on their orthogonal complement. The elements $1, s_1, s_1s_2, s_1s_2s_3$, and τ are pairwise non-conjugate in W and every involution in W is conjugate to one of these. (For the classification of conjugacy classes of involutions in Weyl groups, see [Ric82a].)

One can check explicitly that each of the above combinations of $(n(C), a(C))$ does indeed occur. The table can be verified as follows. It follows from our theory that there is an isomorphism $J[2](\mathbb{C}) \cong \Lambda_\ell/2\Lambda_\ell$ under which the action τ of complex conjugation corresponds to the action of an involution $w \in W(\Lambda_\ell) = W$ and which identifies the Weil pairing on the left-hand side with the natural symplectic pairing on the right. On the other hand, [GH81, Proposition 4.4] shows that the data of the pair $(J[2](\mathbb{C}), \tau)$ (as symplectic $\mathbb{F}_2$-vector space with involution) is sufficient to recover $n(C)$ and $a(C)$. A calculation shows that the Weyl involutions biject with the possible choices for the pair $(n(C), a(C))$. This determines the number of real bitangents and the quantity $\#J(\mathbb{R})/2J(\mathbb{R})$.

We justify the final column using the results in the appendix. The set $G(\mathbb{R})\backslash V_x(\mathbb{R})$ is in canonical bijection with the set $\ker(H^1(\mathbb{R}, J[2]) \to H^1(\mathbb{R}, G))$, the marked element corresponding to the trivial element of $J(\mathbb{R})/2J(\mathbb{R})$. We analyze this kernel using the diagram of $\mathbb{R}$-groups with exact rows, whose existence is asserted by the main result in the appendix to this paper:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_2 & \longrightarrow & \mathrm{Sp}_8 & \longrightarrow & \mathrm{PSp}_8 & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \mu_2 & \longrightarrow & \widetilde{V} & \longrightarrow & J[2] & \longrightarrow & 1, \end{array}$$

where $\widetilde{V}$ is the extension used in the proof of Theorem 3.5; it is a subgroup of the Heisenberg group $\widetilde{H}_{\mathcal{L}}$. Using the triviality of the set $H^1(\mathbb{R}, \mathrm{Sp}_8)$, we get an identification

$$G(\mathbb{R})\backslash V_x(\mathbb{R}) \cong \ker(H^1(\mathbb{R}, J[2]) \to H^1(\mathbb{R}, G)) \cong \ker(H^1(\mathbb{R}, J[2]) \to H^2(\mathbb{R}, \mu_2)),$$

where the arrow $q : H^1(\mathbb{R}, J[2]) \to H^2(\mathbb{R}, \mu_2) \cong \mathbb{Z}/2\mathbb{Z}$ is the connecting map arising from the bottom row of the above commutative diagram. (Note that we are working here with non-abelian Galois cohomology; the connecting map is defined, because μ_2 is central, but it need not be a homomorphism of groups.)

Tate duality gives a perfect pairing on $H^1(\mathbb{R}, J[2])$, with respect to which $J(\mathbb{R})/2J(\mathbb{R})$ is a maximal isotropic subspace. The map q is a quadratic refinement of this pairing, in the sense of §1.1, which is identically zero on the subspace $J(\mathbb{R})/2J(\mathbb{R})$ (see [PR12, Corollary 4.7]). It follows that $a(q) = 0$, and the set $q^{-1}(0)$ has $2^{g-1}(2^g + 1)$ elements, where $g = \dim_{\mathbb{F}_2} J(\mathbb{R})/2J(\mathbb{R})$. This leads to the final column in the above table.

Appendix A. A converse to Lurie's functorial construction of simply laced Lie algebras

By Tasho Kaletha[1]

In §2 a construction due to Lurie was recalled, which associates in a functorial way a semi-simple Lie algebra $\mathfrak{h}$ to a simply laced root lattice Λ equipped with an extension $\tilde{V}$ of $V = \Lambda/2\Lambda$ by $\{\pm 1\}$. In fact, the construction produces not just $\mathfrak{h}$, but also some additional structure, including a Cartan subalgebra $\mathfrak{t}$. This construction was moreover refined in several ways. It was shown that an action of the Galois group of a field k on $\tilde{V}$ is translated to a k-structure on $\mathfrak{h}$; it was shown that $\mathfrak{h}$ comes equipped with a stable involution θ (i.e. an involution satisfying the first condition of Proposition 1.9); and finally a construction was described that produces from a rational representation ρ of the finite algebraic k-group $\tilde{V}$ with $\rho(-1) = -1$ a rational representation $d\pi$ of the Lie-algebra $\mathfrak{g} = \mathfrak{h}^\theta$.

The purpose of this appendix is to provide a converse to this refinement of Lurie's construction. The basic question is: given $\mathfrak{h}$, $\mathfrak{t}$, and θ, is it possible to recover the extension $\tilde{V}$ in a concrete way? That this should be the case, and in fact where the extension is to be found, was suggested to us by Jack Thorne. His idea was that the extension $\tilde{V}$ should be the preimage in G_{sc} of the 2-torsion subgroup of T_{sc}, where T_{sc} is the maximal torus of the simply connected group H_{sc} with Lie-algabra $\mathfrak{h}$ given by the Cartan subalgebra $\mathfrak{t}$, and G_{sc} is the simply connected group with Lie-algebra $\mathfrak{g}$. In this appendix we will show that this preimage is indeed an extension of V by $\{\pm 1\}$ and we will moreover construct an isomorphism from this extension to $\tilde{V}$ that preserves the action of the Galois group of k and intertwines the representations ρ and π.

We thank Jack Thorne for sharing with us this interesting question and for including our results into his paper.

A.1 Statement of two propositions

Let k be a field of characteristic 0, k^s a fixed separable closure, $\Gamma_k = \mathrm{Gal}(k^s/k)$. Let Λ be a finite free $\mathbb{Z}$-module equipped with a symmetric bilinear form $\langle -, - \rangle : \Lambda \otimes \Lambda \to \mathbb{Z}$ and satisfying the conditions

- $\mathrm{rk}\Lambda > 1$.
- For any non-zero $\lambda \in \Lambda$, the value $\langle \lambda, \lambda \rangle$ is a positive even integer.
- The set $\Gamma = \{\lambda \in \Lambda | \langle \lambda, \lambda \rangle = 2\}$ generates Λ.

As discussed in [Lur01], these are precisely the root lattices of simply laced root systems. Here we are excluding the system A_1. The subset $\Gamma \subset \Lambda$ is the set of roots. We shall place the additional assumption that Γ is irreducible. This assumption is made just for convenience and can easily be removed.

Write $q(\lambda) = \frac{1}{2}\langle \lambda, \lambda \rangle$, this is a quadratic form. Let $V = \Lambda/2\Lambda$ and let

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

be an extension of groups (we write the group law of $\tilde{V}$ multiplicatively) with the property that for each $\tilde{v} \in \tilde{V}$ and its image $v \in V$, the equality $\tilde{v}^2 = (-1)^{q(v)}$ holds. This equation characterizes the isomorphism class of this extension.

Assume we are given an action of Γ_k on Λ that preserves $\langle -, - \rangle$, as well as an action of Γ_k on $\tilde{V}$ that preserves the subgroup $\{\pm 1\}$, such that the two actions on V induced from these coincide. Let $\tilde{\Lambda} = \Lambda \times_V \tilde{V}$ and let $\tilde{\Gamma} \subset \tilde{\Lambda}$ be the preimage of Γ. The extension $\tilde{\Lambda}$ of Λ by $\{\pm 1\}$ inherits an action of Γ_k and this action preserves $\tilde{\Gamma}$.

Let $\mathfrak{h}$ be the Lie algebra associated to this data as described in §2. It comes equipped with a Cartan subalgebra $\mathfrak{t}$ and a map $\tilde{\Gamma} \to \mathfrak{h}$ sending each $\tilde{\gamma}$ to a non-zero root vector $X_{\tilde{\gamma}} \in \mathfrak{h}_\gamma$ and having the properties

- $X_{-\tilde{\gamma}} = -X_{\tilde{\gamma}}$;

[1]This research is supported in part by NSF grant DMS-1161489.

- $[X_{\tilde\gamma}, X_{\tilde\gamma'}] = X_{\tilde\gamma\tilde\gamma'}$ if $\gamma + \gamma' \in \Gamma$ (by assumption $\tilde\gamma\tilde\gamma' \in \tilde\Gamma$);
- $[X_{\tilde\gamma}, X_{\tilde\gamma'}] = (\tilde\gamma\tilde\gamma')H_\gamma$ if $\gamma' = -\gamma$, where $H_\gamma \in \mathfrak{t}$ is the coroot for γ (by assumption $\tilde\gamma\tilde\gamma' \in \{\pm 1\}$).

Let $H = \mathrm{Aut}(\mathfrak{h})^\circ$ be the corresponding adjoint group, H_{sc} its simply connected cover, and θ the involution of $\mathfrak{h}$ which acts by -1 on $\mathfrak{t}$ and by $\theta(X_{\tilde\gamma}) = -X_{\tilde\gamma^{-1}}$ on the root subspaces. It induces an involution on H and H_{sc} as well and this involution acts by inversion of the maximal tori T and T_{sc} whose Lie algebra is $\mathfrak{t}$. Let $\mathfrak{g} = \mathfrak{h}^\theta$ be the fixed Lie subalgebra and $G = H^{\theta,\circ}$ the connected component of the fixed subgroup. Let $G' = H_{\mathrm{sc}}^\theta$. According to [Ste68, Theorem 8.1] G' is connected. Its image in H is equal to G. Since θ commutes with the action of Γ_k, the groups G and G' are defined over k.

Proposition A.1. *The group G' is semi-simple and its fundamental group has order 2.*

Let G_{sc} be the simply connected cover of G. We will from now on denote the fundamental group of G' by $\{\pm 1\} \subset G_{\mathrm{sc}}$. For a root $\gamma \in \Gamma$, let $\gamma^\vee$ be the corresponding coroot. The map

$$V \to T_{\mathrm{sc}}, \qquad [\gamma] \mapsto \gamma^\vee(-1)$$

identifies V with the 2-torsion subgroup of T_{sc} and this subgroup belongs to G'. We form the pull-back extension

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & G_{\mathrm{sc}} & \longrightarrow & G' & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & X & \longrightarrow & V & \longrightarrow & 1 \end{array}$$

This extension inherits an action of Γ_k.

Finally, given a rational representation $\rho : \tilde V \to \mathrm{GL}(W)$ of the algebraic k-group $\tilde V$ on a finite-dimensional k-vector space W such that $\rho(-1) = -1$, we define a representation $d\pi : \mathfrak{g} \to \mathfrak{gl}(W)$ by $d\pi(X_{\tilde\gamma} - X_{\tilde\gamma^{-1}}) = \rho(\tilde\gamma)/2$, and let $\pi : G_{\mathrm{sc}} \to \mathrm{GL}(W)$ be the corresponding rational representation of G_{sc}. Recall that Proposition 2.3 asserts that $d\pi$ is indeed a Lie-algebra representation.

Proposition A.2. *There exists an isomorphism of extensions $\Phi : \tilde V \to X$ which is Γ_k-equivariant and intertwines ρ with $\pi|_X$ for all representations ρ as above.*

A.2 Proof of Proposition A.1

According to [RLYG12, §5.3], the involution θ is stable and hence its conjugacy class is uniquely determined. A description of this conjugacy class for each Dynkin type is given in [RLYG12, §8] in terms of Kac diagrams. The normalized Kac diagram of the stable involution contains a unique node with label 1, and all other nodes have label 0. According to [Ree10, §3.7], this implies that the center of G is finite. Thus G, and hence also G' is semi-simple. Its Dynkin diagram is obtained by removing the unique node with label 1 from the Kac diagram of the stable involution. In order to prove that the fundamental group of G' has order 2, we argue as follows. According to [Ree10, §3.7], the order of the center of G is given by b_ι, where ι is the index of the unique node with label 1 in the Kac diagram, and b_ι is an integer defined in [Ree10, §3.3], which according to Theorem 3.7 in loc. cit. is equal to 2 if θ is inner and to 1 if θ is outer. Since θ acts by -1 on the Cartan subalgebra $\mathfrak{t}$, it is inner if and only if -1 belongs to the Weyl group of $(\mathfrak{t}, \mathfrak{h})$.

The kernel of the map $G' \to G$ is equal to $Z(H_{\mathrm{sc}})^\theta$. Thus the center of G' has size $|Z(H_{\mathrm{sc}})^\theta| \cdot b_\iota$. The proof will be complete once we show that this number is equal to one half of the connection index of the Dynkin diagram of G. This can be done by inspection of the individual cases $A_n, n > 1$, D_n, E_6, E_7, E_8. We give the examples of the exceptional types E_6, E_7, and E_8, and leave the discussion of the classical types A_n and D_n to the reader.

For type E_6, the Kac diagram of θ is given by the last row of Table 3 of [RLYG12, §8.1] and has the form 0 0 0 $\Leftarrow$ 0 1, so G has type C_4. Since θ is outer, G is adjoint. There are no θ-fixed points in the center of H_{sc}, thus $G' \cong \mathrm{PSp}_4$.

For type E_7, the Kac diagram of θ is given by the last row of Table 4 and has the form $\overset{0}{\underset{1}{}}\,0\,0\,0\,0\,0\,0$, so G is of type A_7. The center of G has now order 2, because θ is inner, and moreover the fixed points of θ in $Z(H_{\mathrm{sc}})$ also have order 2, so the center of G' has order 4.

For type E_8, the Kac diagram of θ is given by the last row in Table 5 and has the form $\overset{1}{\underset{0}{}}\,0\,0\,0\,0\,0\,0\,0$, so G is of type D_8. The center of G has order 2, because θ is inner. Since $Z(H_{\mathrm{sc}}) = 1$, the center of G' also has order 2.

For the classical types, the relevant diagrams are those in row 2 of Table 10 (H is of type A_{2n} and G is of type B_n), row 3 of Table 11 with $k = n-1$ (H is of type A_{2n-1} and G is of type D_n), row 3 of Table 14 for $k = n$ even (H is of type D_n and G is of type $D_{\frac{n}{2}} \times D_{\frac{n}{2}}$), and row 3 of Table 15 with $l = n$ odd (H is of type D_n and G is of type $B_{\frac{n-1}{2}} \times B_{\frac{n-1}{2}}$). Note that θ is inner for D_{even} and outer for A_n and D_{odd}.

A.3 Proof of Proposition A.2

A.3.1 The group SO_n

We define the group SO_n to be the subgroup of SL_n fixed by the transpose-inverse automorphism. This group is semi-simple when $n > 2$. For $n = 2$, it is non-canonically isomorphic to $\mathbb{G}_m$ over k^s. One can specify an isomorphism by fixing a 4-th root of unity $i \in k^s$. Then we have

$$\mathbb{G}_m \to \mathrm{SO}_2, \qquad x \mapsto \frac{1}{2}\begin{bmatrix} x + x^{-1} & i(x - x^{-1}) \\ -i(x - x^{-1}) & x + x^{-1} \end{bmatrix}.$$

For future reference, we record the formula

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}^2 = \begin{bmatrix} a^2 - b^2 & 2ab \\ -2ab & a^2 - b^2 \end{bmatrix}$$

for the squaring map $\mathrm{SO}_2 \xrightarrow{(\,)^2} \mathrm{SO}_2$.

A.3.2 Construction of the isomorphism $\tilde{V} \to X$

Choose a set of simple roots $\Delta \subset \Gamma$. The image Δ_V of Δ in V is a set of generators for this group, and the relations on this set are $2v = 0$ for all $v \in \Delta_V$. Let $\tilde{\Delta}$ be the preimage of Δ in $\tilde{\Lambda}$, and $\tilde{\Delta}_V$ be the image of $\tilde{\Delta}$ in $\tilde{V}$. Then $\tilde{\Delta}_V$ is a set of generators for $\tilde{V}$, and the relations on this set are $\tilde{v}^2 = (-1)$ and $\tilde{v}\tilde{w} = (-1)^{\langle v,w\rangle}\tilde{w}\tilde{v}$.

We now define a map $\phi : \tilde{\Delta} \to X$. Given $\tilde{\gamma} \in \tilde{\Delta}$ we obtain a monomorphism $\eta_{\tilde{\gamma}} : \mathrm{SL}_2 \to H_{\mathrm{sc}}$ with θ-stable image that translates the action of θ on its image to the action of transpose-inverse on SL_2. The fixed subgroup SO_2 of this action therefore lands in G'.

Lemma A.3. *The preimage of $\eta_{\tilde{\gamma}}(SO_2)$ in G_{sc} is connected.*

The proof of this lemma will be given in section A.3.6. Granting this lemma, it follows from Proposition A.1 that there exists a unique homomorphism $\phi_{\tilde{\gamma}} : \mathrm{SO}_2 \to G_{\mathrm{sc}}$ making the following diagram commute.

$$\begin{array}{ccc} \mathrm{SO}_2 & \xrightarrow{\phi_{\tilde{\gamma}}} & G_{\mathrm{sc}} \\ \downarrow{\scriptstyle (\,)^2} & & \downarrow \\ \mathrm{SO}_2 & \xrightarrow{\eta_{\tilde{\gamma}}} & G' \end{array}$$

This homomorphism is injective. We let $\phi(\tilde{\gamma}) = \phi_{\tilde{\gamma}}\left(\begin{bmatrix} & 1 \\ -1 & \end{bmatrix}\right)$. By the above diagram, the image of $\phi(\tilde{\gamma})$ in G' is equal to $\gamma^\vee(-1)$, which shows that $\phi(\tilde{\gamma}) \in X$. Moreover, $\phi(\tilde{\gamma})^2 = \phi_{\tilde{\gamma}}(-1)$ is a non-trivial element of G_{sc} whose image in G' is trivial, hence $\phi(\tilde{\gamma})^2 = -1$.

We thus obtain a map $\phi : \tilde{\Delta} \to X$ which descends to a map $\Phi : \tilde{\Delta}_V \to X$ and whose image contains a set of generators for X. We claim that Φ is Γ_k-equivariant. Given $\sigma \in \Gamma_k$ we have $\eta_{\sigma\tilde{\gamma}} = \sigma \circ \eta_{\tilde{\gamma}}$, and

hence $\phi_{\sigma\tilde{\gamma}} = \sigma \circ \phi_{\tilde{\gamma}}$, where on the right sides of these equations σ denotes the action of σ on G' and G_{sc} respectively. Thus $\phi(\sigma\tilde{\gamma}) = \sigma\phi(\tilde{\gamma})$ for all $\tilde{\gamma} \in \tilde{\Gamma}$ and this establishes the Γ_k-equivariance of Φ.

Our task is to show that Φ respects the relation $\tilde{v}\tilde{w} = (-1)^{\langle v,w\rangle}\tilde{w}\tilde{v}$. Once this is done, it will extend to a surjective homomorphism $\Phi : \tilde{V} \to X$, which will then have to be bijective because its source and target have the same cardinality. It will furthermore be Γ_k-equivariant.

A.3.3 The isomorphism $\mathbf{PGL}_2 \to \mathbf{SO}_3$

Consider the adjoint action of PGL_2 on its Lie-algebra $\mathfrak{sl}_2$. Fix a 4-th root of unity $i \in k^s$ as well as an element $\sqrt{2} \in k^s$. The basis

$$\sqrt{2}^{-1}\begin{bmatrix} 1 & \\ & -1 \end{bmatrix} \qquad (i\sqrt{2})^{-1}\begin{bmatrix} & 1 \\ -1 & \end{bmatrix} \qquad \sqrt{2}^{-1}\begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$$

is an orthonormal basis for the symmetric bilinear form $\mathrm{tr}(AB)$ and provides an isomorphism $\mathrm{PGL}_2 \to \mathrm{SO}_3$ defined over k^s, which is explicitly given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto (ad-bc)^{-1}\begin{bmatrix} ad+bc & i(ac+bd) & bd-ac \\ -i(ab+cd) & \frac{a^2+b^2+c^2+d^2}{2} & i\frac{a^2-b^2+c^2-d^2}{2} \\ -(ab-cd) & i\frac{c^2+d^2-a^2-b^2}{2} & \frac{a^2-b^2-c^2+d^2}{2} \end{bmatrix}.$$

Its derivative $\mathfrak{sl}_2 \to \mathfrak{so}_3$ is given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} 0 & i(b+c) & b-c \\ -i(b+c) & 0 & 2ia \\ c-b & -2ia & 0 \end{bmatrix}.$$

A.3.4 The relation $\tilde{v}\tilde{w} = (-1)^{\langle v,w\rangle}\tilde{w}\tilde{v}$

In section A.3.2 we constructed a map $\Phi : \tilde{\Delta}_V \to X$. In order to show that it extends to an isomorphism $\tilde{V} \to X$, it remains to check that for $\tilde{v}, \tilde{w} \in \tilde{\Delta}_V$ with images $v, w \in \Delta_V$ we have

$$\Phi(\tilde{v})\Phi(\tilde{w}) = (-1)^{\langle v,w\rangle}\Phi(\tilde{w})\Phi(\tilde{v}). \tag{A.4}$$

Let $\tilde{\gamma}, \tilde{\delta} \in \tilde{\Gamma}$ be preimages of $\tilde{v}, \tilde{w}$, and $\gamma, \delta \in \Delta$ be their images. We have either $\langle \gamma, \delta\rangle = 0$ or $\langle \gamma, \delta\rangle = -1$. In the first case, the cocharacters $\eta_{\tilde{\gamma}}$ and $\eta_{\tilde{\delta}}$ commute and hence their images are contained in a common maximal torus of G'. The preimage in G_{sc} of this maximal torus is a maximal torus of G_{sc} and contains the images of $\phi_{\tilde{\gamma}}$ and $\phi_{\tilde{\delta}}$, and we conclude that these two cocharacters also commute. This proves (A.4) in the case $\langle \gamma, \delta\rangle = 0$ and we are left with the case $\langle \gamma, \delta\rangle = -1$. Then the elements $\{X_{\tilde{\gamma}^{\pm 1}}, X_{\tilde{\delta}^{\pm 1}}, X_{(\tilde{\gamma}\tilde{\delta})^{\pm 1}}\}$ generate a subalgebra of $\mathfrak{h}$ isomorphic to $\mathfrak{sl}_3$. Even more, there is a preferred embedding $\mu_{\tilde{\gamma},\tilde{\delta}} : \mathfrak{sl}_3 \to \mathfrak{h}$ given by

$$\begin{bmatrix} 0 & 1 & \\ & 0 & \\ & & 0 \end{bmatrix} \mapsto X_{\tilde{\gamma}} \qquad \begin{bmatrix} 0 & & \\ & 0 & 1 \\ & & 0 \end{bmatrix} \mapsto X_{\tilde{\delta}} \qquad \begin{bmatrix} 0 & & 1 \\ & 0 & \\ & & 0 \end{bmatrix} \mapsto X_{\tilde{\gamma}\tilde{\delta}}.$$

It integrates to an embedding $\mu_{\tilde{\gamma},\tilde{\delta}} : \mathrm{SL}_3 \to H_{\mathrm{sc}}$. The embeddings $\eta_{\tilde{\gamma}}, \eta_{\tilde{\delta}} : \mathrm{SL}_2 \to H_{\mathrm{sc}}$ factor through $\mu_{\tilde{\gamma},\tilde{\delta}}$ and give embeddings

$$\mathrm{SO}_2 \to \mathrm{SO}_3, \qquad \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mapsto \begin{bmatrix} a & b & \\ -b & a & \\ & & 1 \end{bmatrix}$$

and

$$\mathrm{SO}_2 \to \mathrm{SO}_3, \qquad \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mapsto \begin{bmatrix} 1 & & \\ & a & b \\ & -b & a \end{bmatrix}.$$

We compose these with the isomorphism $\mathrm{SO}_3 \to \mathrm{PGL}_2$ of section A.3.3, for which we fix the elements $i, \sqrt{2} \in k^s$ as discussed there. This gives two embeddings $\mathrm{SO}_2 \to \mathrm{PGL}_2$.

The first one is characterized by

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mapsto \begin{bmatrix} \alpha & \beta \\ \beta & \alpha \end{bmatrix}$$

where $\alpha^2 + \beta^2 = a$ and $2i\alpha\beta = b$. The composition of this with the squaring map on SO_2 lifts to the map

$$\mathrm{SO}_2 \to \mathrm{SL}_2, \qquad \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mapsto \begin{bmatrix} a & b/i \\ b/i & a \end{bmatrix}.$$

The image of $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ under this map is equal to $\begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}$.

The second embedding $\mathrm{SO}_2 \to \mathrm{PGL}_2$ is given by

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mapsto \begin{bmatrix} \sqrt{a-ib} & \\ & \sqrt{a-ib}^{-1}. \end{bmatrix}$$

Note that this is well-defined with an arbitrary choice of $\sqrt{a-ib}$. Its composition with the squaring map on SO_2 lifts to the map

$$\mathrm{SO}_2 \to \mathrm{SL}_2, \qquad \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \mapsto \begin{bmatrix} (a-ib) & \\ & (a-ib)^{-1} \end{bmatrix}.$$

The image of $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ under this map is equal to $\begin{bmatrix} -i & \\ & i \end{bmatrix}$. The claim now follows from

$$\begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix} \cdot \begin{bmatrix} -i & \\ & i \end{bmatrix} = - \begin{bmatrix} -i & \\ & i \end{bmatrix} \cdot \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}.$$

A.3.5 Intertwining property of $\Phi : \tilde{V} \to X$

Let $\rho : \tilde{V} \to \mathrm{GL}(W)$ be a rational representation of the finite algebraic k-group $\tilde{V}$ on a finite-dimensional k-vector space W, having the property that $\rho(-1) = -1$. Let $\pi : G_{\mathrm{sc}} \to \mathrm{GL}(W)$ be the rational representation obtained from it. We want to show that Φ intertwines ρ with $\pi|_X$. It is enough to show that, for $\tilde{\gamma} \in \tilde{\Delta}$ with image $\tilde{v} \in \tilde{V}$, we have the following equality in $\mathrm{GL}(W)(k^s)$:

$$\pi(\Phi(\tilde{v})) = \rho(\tilde{v}).$$

Let $\gamma \in \Delta$ be the image of $\tilde{\gamma}$. Choose $\delta \in \Delta$ with $\langle \gamma, \delta \rangle = -1$ and let $\tilde{\delta} \in \tilde{\Delta}$ be a preimage. Let $\tilde{w} \in \tilde{V}$ be the image of $\tilde{\delta}$. Let $Q \subset \tilde{V}$ be the subgroup generated by $\tilde{v}, \tilde{w}$. It is isomorphic to the quaternion group.

Let $\mu_{\tilde{\gamma},\tilde{\delta}} : \mathfrak{sl}_3 \to \mathfrak{h}$ be the embedding determined by $\tilde{\gamma}$ and $\tilde{\delta}$ as in section A.3.4. It determines an embedding $\mu_{\tilde{\gamma},\tilde{\delta}} : \mathrm{SL}_3 \to H_{\mathrm{sc}}$.

Decompose $W = \oplus_{i=1}^n W_i$ under $\rho|_Q$ into irreducible representations over k^s. The condition $\rho(-1) = -1$ forces all W_i to be isomorphic to the unique 2-dimensional representation of Q. Moreover, by construction of $d\pi$, each subspace W_i of W is preserved by the action of $d\pi(\mu_{\tilde{\gamma},\tilde{\delta}}(\mathfrak{so}_3))$, hence also by the action of $\pi(\mu_{\tilde{\gamma},\tilde{\delta}}(\mathrm{SO}_3))$. We can thus focus on a single W_i. Choosing a suitable basis for W_i over k^s, we obtain from $\rho|_Q$ the embedding $Q \to \mathrm{SL}_2(k^s)$ given by

$$\tilde{v} \mapsto \begin{bmatrix} & -i \\ -i & \end{bmatrix} \qquad \tilde{w} \mapsto \begin{bmatrix} -i & \\ & i \end{bmatrix} \qquad \tilde{v}\tilde{w} \mapsto \begin{bmatrix} & 1 \\ -1 & \end{bmatrix}.$$

Reviewing the construction of $d\pi$, we see that the restriction to W_i of $d\pi \circ \mu_{\tilde{\gamma},\tilde{\delta}}$ provides the isomorphism $\mathfrak{so}_3 \to \mathfrak{sl}_2$ given by

$$\begin{bmatrix} 0 & 1 & \\ -1 & 0 & \\ & & 0 \end{bmatrix} \mapsto \frac{1}{2} \begin{bmatrix} & -i \\ -i & \end{bmatrix}, \quad \begin{bmatrix} 0 & & \\ & 0 & 1 \\ & -1 & 0 \end{bmatrix} \mapsto \frac{1}{2} \begin{bmatrix} -i & \\ & i \end{bmatrix}, \quad \begin{bmatrix} 0 & & 1 \\ & 0 & \\ -1 & & 0 \end{bmatrix} \mapsto \frac{1}{2} \begin{bmatrix} & 1 \\ -1 & \end{bmatrix},$$

which one easily checks to be the inverse of the isomorphism of section A.3.3. Thus, the composition of the isomorphism $\mathrm{SL}_2 \to \mathrm{Spin}_3$ of section A.3.3 with the embedding $\mu_{\tilde{\gamma},\tilde{\delta}} : \mathrm{Spin}_3 \to G_{\mathrm{sc}}$ provides a representation of SL_2 on W_i which in the chosen basis of W_i is given by the identity map $\mathrm{SL}_2 \to \mathrm{SL}_2$. However, the discussion of section A.3.4 shows that $\Phi(\tilde{v}) \in G_{\mathrm{sc}}$ is the image of the element $\begin{bmatrix} & -i \\ -i & \end{bmatrix}$ under the composition of the isomorphism $\mathrm{SL}_2 \to \mathrm{Spin}_3$ of section A.3.3 with the embedding $\mu_{\tilde{\gamma},\tilde{\delta}} : \mathrm{Spin}_3 \to G_{\mathrm{sc}}$. We conclude that $\rho(\tilde{v})$ and $\pi(\Phi(\tilde{v}))$ are represented by the same matrix in $\mathrm{SL}_2(k^s) \subset \mathrm{GL}(W_i)(k^s)$.

A.3.6 Proof of Lemma A.3

We note first that the statement of the lemma is equivalent to the claim that the preimage of $\gamma^\vee(-1)$ in G_{sc} has order 4. Indeed, if the preimage of $\eta_{\tilde{\gamma}}(\mathrm{SO}_2)$ in G_{sc} is connected, then identifying SO_2 with $\mathbb{G}_m$ we obtain via pull-back along $\eta_{\tilde{\gamma}}$ the non-split extension $1 \to \{\pm 1\} \to \mathbb{G}_m \to \mathbb{G}_m \to 1$, and the element $\gamma^\vee(-1)$ corresponds to the element -1 of the right copy of $\mathbb{G}_m$, which evidently has two preimages of order 4. On the other hand, if the preimage of $\eta_{\tilde{\gamma}}(\mathrm{SO}_2)$ in G_{sc} is disconnected, the the corresponding extension is the split extension $1 \to \{\pm 1\} \to \{\pm 1\} \times \mathbb{G}_m \to \mathbb{G}_m \to 1$ and the element $-1 \in \mathbb{G}_m$ has two lifts of order 2.

We have the element $\tilde{\gamma} \in \tilde{\Gamma}$ and the corresponding element $\gamma \in \Gamma$. The chosen base Δ of Γ in the discussion of section A.3.2 will be unimportant. We first claim that there exists a maximal torus $S_{\mathrm{sc}} \subset H_{\mathrm{sc}}$, a Borel subgroup C containing S_{sc}, and a root α of H_{sc} with respect to S_{sc} such that θ preserves the pair (S_{sc}, C) as well as the root α and $\gamma^\vee(-1) = \alpha^\vee(-1)$. Indeed, choose a base Δ for Γ such that the corresponding Kostant cascade M (see [Kos]) contains γ. For each $\beta \in M$, choose a preimage $\tilde{\beta} \in \tilde{\Gamma}$. Let

$$g = \prod_{\beta \in M} \eta_{\tilde{\beta}} \begin{bmatrix} i/2 & 1 \\ -1/2 & -i \end{bmatrix} \in H_{\mathrm{sc}}.$$

Then one checks that $S_{\mathrm{sc}} := \mathrm{Ad}(g)T_{\mathrm{sc}}$ is normalized by θ. If we transport the action of θ on S_{sc} back to T_{sc} via the isomorphism $\mathrm{Ad}(g)$, we obtain the automorphism $\mathrm{Ad}(g^{-1}\theta(g)) \circ \theta$ and one computes that $\mathrm{Ad}(g^{-1}\theta(g))$ acts as the product of reflections $\prod_{\beta \in M} s_\beta$, which according to [Kos, Prop. 1.10] represents the longest element of the Weyl group with respect to the basis Δ. This shows that $\mathrm{Ad}(g^{-1}\theta(g)) \circ \theta$ preserves the basis Δ. It also evidently fixes the root γ. Let $\alpha = \mathrm{Ad}(g)\gamma$, and let C be the Borel subgroup corresponding to the basis $\mathrm{Ad}(g)\Delta$. Finally, $\alpha^\vee(-1) = \gamma^\vee(-1)$ follows from the fact that the element $g \in H_{\mathrm{sc}}$ centralizes $\gamma^\vee(-1) \in H_{\mathrm{sc}}$. Indeed, the image of $\eta_{\tilde{\beta}}$ for $\beta \in M \setminus \{\gamma\}$ centralizes the image of $\gamma^\vee$, while the image of $\eta_{\tilde{\gamma}}$ centralizes the element $\gamma^\vee(-1)$. The claim is proved.

We are now interested in showing that the preimage of $\alpha^\vee(-1)$ in G_{sc} has order 4. For this it is convenient to use again the equivalent formulation that the preimage of $\alpha^\vee(\mathbb{G}_m)$ in G_{sc} is connected. By passing from γ to α we are now in the more advantageos situation that this preimage belongs to the preimage in G_{sc} of $G' \cap S_{\mathrm{sc}} = S_{\mathrm{sc}}^\theta$, which is a maximal torus. Call this maximal torus $\tilde{S} \subset G_{\mathrm{sc}}$. We form the pull-back diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & \tilde{S} & \longrightarrow & S_{\mathrm{sc}}^\theta & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow{\scriptstyle \alpha^\vee} & & \\ 1 & \longrightarrow & \{\pm 1\} & \longrightarrow & ? & \longrightarrow & \mathbb{G}_m & \longrightarrow & 1 \end{array}$$

and would like to show that the bottom extension is not split. Passing to character modules we obtain the push-out diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X^*(S_{\mathrm{sc}})_\theta & \longrightarrow & X^*(\tilde{S}) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha^\vee} & & \downarrow & & \| & & \\ 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & X^*(?) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \end{array}$$

and would still like to show that the bottom extension is not split. This is equivalent to showing that for one, hence any, lift $\dot{1} \in X^*(?)$ of $1 \in \mathbb{Z}/2\mathbb{Z}$, we have $2\dot{1} \in \mathbb{Z} \smallsetminus 2\mathbb{Z}$. This in turn is equivalent to showing that

for one, hence any, lift $\dot{1} \in X^*(\tilde{S})$ of $1 \in \mathbb{Z}/2\mathbb{Z}$, we have $\alpha^\vee(2\dot{1}) \notin \alpha^\vee(2X^*(S_{\mathrm{sc}})_\theta)$. Now $X^*(S_{\mathrm{sc}})$ is the weight lattice of the group H_{sc} with respect to the torus S_{sc}. Since $\alpha^\vee$ is a coroot, we have $\alpha^\vee(X^*(S_{\mathrm{sc}})_\theta) = \mathbb{Z}$. Our task is then to show that the image in $\mathbb{Q}$ of $X^*(\tilde{S})$ under $\alpha^\vee$ is not contained in $\mathbb{Z}$. But $X^*(\tilde{S})$ is equal to the weight lattice of the group G_{sc} relative to the maximal torus $\tilde{S}$. We thus have to show that $\alpha^\vee \in X_*(S_{\mathrm{sc}})^\theta$ does not belong to the coroot lattice of G'.

To that end, we need to describe the root and coroot systems of G'. Let $R \subset X^*(S_{\mathrm{sc}})$ and $R^\vee \subset X_*(S_{\mathrm{sc}})$ be the root and coroot systems of H_{sc}, and let $\Delta \subset R$ be the base given by the Borel subgroup C. We choose a non-zero root vector $X_\beta \in \mathfrak{h}_\beta$ for each $\beta \in \Delta$ subject to the condition $X_{\theta\beta} = \theta X_\beta$ provided $\theta\beta \neq \beta$. For $\beta \in \Delta$ satisfying $\theta\beta = \beta$ we have $\theta X_\beta = \epsilon X_\beta$ with $\epsilon \in \{1, -1\}$. Letting $\{\check{\omega}_\beta | \beta \in \Delta\}$ be the system of fundamental coweights, we set $s \in S$ to be the product of $\check{\omega}_\beta(-1)$ for all $\beta \in \Delta$ with $\theta\beta = \beta$ and $\theta X_\beta = -X_\beta$. Then $s \in S^\theta$ is of order 2 and $\theta = \mathrm{Ad}(s)\theta_0$, with θ_0 an automorphism of H_{sc} preserving the splitting $(S_{\mathrm{sc}}, C, \{X_\beta\})$. The root system of G' is a subset $R' \subset X^*(S_{\mathrm{sc}}^\theta) = X^*(S_{\mathrm{sc}})_\theta$. The duality between $X^*(S_{\mathrm{sc}})$ and $X_*(S_{\mathrm{sc}})$ induces a duality between $X^*(S_{\mathrm{sc}})_\theta$ and $X_*(S_{\mathrm{sc}})^\theta$. The coroot system of G' is a subset $R'^\vee \subset X_*(S_{\mathrm{sc}})^\theta$. The system $R' \subset X^*(S_{\mathrm{sc}})_\theta$ and its dual system $R'^\vee \subset X_*(S_{\mathrm{sc}})^\theta$ can be described using the results of [Ste68], which are summarized in [KS99, §1.1,§1.3]. As evident from the discussion there, the root system A_{2n} behaves differently from all other root systems, a phenomenon that manifests itself in the occurrence of restricted roots of type R_2 and R_3. It is therefore convenient to treat the special case of A_{2n} separately. Fortunately, this special case is rather easy.

Assuming that R is of type A_{2n}, we enumerate $\Delta = \{\alpha_1, \ldots, \alpha_{2n}\}$ with $\theta(\alpha_i) = \alpha_{2n+1-i}$. Since θ has no fixed points in Δ, we have $\theta_0 = \theta$. Thus the projection of Δ to $X^*(S_{\mathrm{sc}})_\theta$ forms a set of simple roots for R'. Let $\alpha'_i \in R'$ denote the projection of α_i. Then $\alpha'_1, \ldots, \alpha'_{n-1}$ are of type R_1, and the corresponding coroots are given by $\alpha_i'^\vee = \alpha_i^\vee + \alpha_{2n+1-i}^\vee$. On the other hand α'_n is of type R_2 and its coroot is given by $2(\alpha_n^\vee + \alpha_{n+1}^\vee)$. It follows that the coroot lattice of G' is the sublattice of $X_*(S_{\mathrm{sc}})^\theta$ spanned by the points $\{\alpha_1^\vee + \alpha_{2n}^\vee, \ldots, \alpha_{n-1}^\vee + \alpha_{n+2}^\vee, 2(\alpha_n^\vee + \alpha_{n+1}^\vee)\}$. On the other hand, we may assume without loss of generality that α is the highest root of R (by making the same assumption on the root γ, bearing in mind that the highest root is always part of the Kostant cascade). Then $\alpha^\vee = \alpha_1^\vee + \cdots + \alpha_{2n}^\vee$ evidently does not belong to the coroot lattice of G'. This completes the discussion of the case A_{2n}.

The remaining root systems can now be treated uniformly, because all occurring restricted roots are of type R_1. According to the discussion in [KS99, §1.3], the root system R' is given by the image of the set

$$\dot{R}' = \{\beta \in R | \theta\beta = \beta \Rightarrow \beta(s) = 1\}$$

under the natural projection $X^*(S_{\mathrm{sc}}) \to X^*(S_{\mathrm{sc}})_\theta$. For the description of $R'^\vee$, we have the following lemma.

Lemma A.4. *For any element of $\beta' \in R'$ represented by $\beta \in \dot{R}'$, the coroot $\beta'^\vee \in X_*(S_{sc})^\theta$ is given by*

$$\begin{cases} \beta^\vee & , \theta\beta = \beta \\ \beta^\vee + \theta\beta^\vee & , \theta\beta \neq \beta \end{cases}$$

Proof. Since β' is of type type R_1, we know that if $\theta\beta \neq \beta$ then $\theta\beta \perp \beta$. According to [Bou02, Chap. VI, §1, no. 1], $\beta'^\vee$ is the unique element of the dual space of $X^*(S_{\mathrm{sc}})_\theta \otimes \mathbb{Q}$ with the properties $\langle \beta'^\vee, \beta' \rangle = 2$ and $s_{\beta', \beta'^\vee}(R') \subset R'$, where $s_{\beta', \beta'^\vee}(x) = x - \langle \beta'^\vee, x \rangle \beta'$ is the reflection determined by $\beta', \beta'^\vee$. We need to check that the elements given in the statement of the lemma satisfy these properties. The first property is immediate. For the second property we take $\beta_1, \beta_2 \in \dot{R}'$ and let $\beta'_1, \beta'_2 \in R'$ be their images. Let $\beta_1'^\vee \in X_*(S_{\mathrm{sc}})^\theta$ be given by the table above. We need to show that $s_{\beta'_1, \beta_1'^\vee}(\beta'_2) \in R'$. If β_2 is perpendicular to both β_1 and $\theta\beta_1$, or if $\beta'_1 = \pm\beta'_2$, then the claim is clear. We thus assume that this is not the case.

If β_1 is fixed by θ, then $s_{\beta'_1, \beta_1'^\vee}(\beta'_2)$ is the image of $s_{\beta_1, \beta_1^\vee}(\beta_2)$. This element of R belongs to $\dot{R}'$, because it is fixed by θ precisely when β_2 is, and in this case it kills s, since both β_1 and β_2 do.

If β_1 is not fixed by θ, but β_2 is, then we have $\langle \beta_1^\vee + \theta\beta_1^\vee, \beta_2 \rangle = 2\langle \beta_1^\vee, \beta_2 \rangle = 2\epsilon \neq 0$ and conclude that $s_{\beta'_1, \beta_1'^\vee}(\beta'_2)$ is the image of $\beta_2 - 2\epsilon\beta_1$, which coincides with the image of $\beta_2 - \epsilon\beta_1 - \epsilon\theta\beta_1$. The latter element belongs to R, because $\beta_1 \perp \theta\beta_1$. It is furthermore fixed by θ and kills s, so belongs to $\dot{R}'$.

Now assume that both β_1, β_2 are not fixed by θ. If $\langle \beta_1^\vee, \beta_2 \rangle$ and $\langle \theta\beta_1^\vee, \beta_2 \rangle$ are both non-zero and have opposite signs, then $s_{\beta'_1, \beta_1'^\vee}(\beta'_2) = \beta'_2$. If $\langle \beta_1^\vee, \beta_2 \rangle$ and $\langle \theta\beta_1^\vee, \beta_2 \rangle$ are both non-zero and have the same

sign $\epsilon \in \{1, -1\}$, then $s_{\beta_1', \beta_1'^\vee}(\beta_2')$ is equal to the image of $\beta_2 - 2\epsilon\beta_1$, which coincides with the image of $\beta_2 - \epsilon\beta_1 - \epsilon\theta\beta_1$. As above this element belongs to R. It is moreover not θ-fixed, thus belongs to $\dot{R}'$. It remains to consider the cases where exactly one of $\langle \beta_1^\vee, \beta_2 \rangle$ and $\langle \theta\beta_1^\vee, \beta_2 \rangle$ is non-zero. We will give the computation only in the case $\langle \beta_1^\vee, \beta_2 \rangle = 0$, $\langle \theta\beta_1^\vee, \beta_2 \rangle = -1$, the other cases being analogous. The element $s_{\beta_1', \beta_1'^\vee}(\beta_2') \in X^*(S_{\mathrm{sc}})_\theta$ is equal to the image of $\beta_2 + \beta_1 \in R$ and we claim that this element is not θ-fixed. If it were, we'd have $\beta_2 = \theta\beta_2 + \theta\beta_1 - \beta_1$ and applying $\langle \theta\beta_1^\vee, - \rangle$ we would obtain $-1 = 0 + 2 - 0$. □

Armed with this lemma we complete the proof of Lemma A.3 as follows. We have the element $\alpha^\vee \in X_*(S_{\mathrm{sc}})^\theta$, which is a coroot for the group H_{sc}. We wish to show that it does not belong to the coroot lattice for the group G'. Assume the contrary. Then inside of the lattice $X_*(S_{\mathrm{sc}})^\theta$ we have the equation $\alpha^\vee = \sum n_i \beta_i'^\vee$ for some integers n_i and some roots $\beta_i' \in R'$. We choose for each β_i' a lift $\beta_i \in \dot{R}'$ and apply the previous lemma, thereby obtaining

$$\alpha^\vee = \sum n_i \beta_i^\vee + \sum n_i (\beta_i^\vee + \theta\beta_i^\vee),$$

where we have subdivided the set of $\{\beta_i\}$ into the cases corresponding to the statement of above lemma. This equation holds inside the coroot lattice of H_{sc}. Since R is a simply laced root system, the bijection $R \to R^\vee, \beta \mapsto \beta^\vee$ extends to a $\mathbb{Z}$-linear bijection from the root lattice to the coroot lattice. This tells us that we have the equation

$$\alpha = \sum n_i \beta_i + \sum n_i (\beta_i + \theta\beta_i)$$

in the root lattice of H_{sc}, i.e. in $X^*(S)$. However, the right hand side is a character of S which kills the element $s \in S$. This would imply that $\alpha \in \dot{R}'$, which would then imply that θ acts trivially on the root space $\mathfrak{h}_\alpha$. This is however false, because for $X = \mathrm{Ad}(g)X_{\tilde{\gamma}} \in \mathfrak{h}_\alpha$ we have

$$\theta(X) = \mathrm{Ad}(g)\mathrm{Ad}(g^{-1}\theta(g))\theta(X_{\tilde{\gamma}}) = \mathrm{Ad}(g)\mathrm{Ad}\eta_{\tilde{\gamma}} \begin{bmatrix} & -i \\ -i & \end{bmatrix} (-X_{\tilde{\gamma}^{-1}}) = -X.$$

The proof of Lemma A.3 is now complete.

References

[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. 2nd augmented ed.* Berlin: Springer, 2nd augmented ed. edition, 2004.

[Bou02] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 4–6.* Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 2002. Translated from the 1968 French original by Andrew Pressley.

[BSD63] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[dG11] Willem A. de Graaf. Computing representatives of nilpotent orbits of θ-groups. *J. Symb. Comput.*, 46(4):438–458, 2011.

[DO88] Igor Dolgachev and David Ortland. Point sets in projective spaces and theta functions. *Astérisque*, (165):210 pp. (1989), 1988.

[Dol12] Igor V. Dolgachev. *Classical algebraic geometry. A modern view.* Cambridge: Cambridge University Press, 2012.

[GH81] Benedict H. Gross and Joe Harris. Real algebraic curves. *Ann. Sci. École Norm. Sup. (4)*, 14(2):157–182, 1981.

[GH94] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry. 2nd ed.* New York, NY: John Wiley & Sons Ltd., 2nd ed. edition, 1994.

[GH04] Benedict H. Gross and Joe Harris. On some geometric constructions related to theta characteristics. In *Contributions to automorphic forms, geometry, and number theory*, pages 279–311. Johns Hopkins Univ. Press, Baltimore, MD, 2004.

[Kos] B. Kostant. The cascade of orthogonal roots and the coadjoint structure of the nilradical of a Borel subgroup of a semisimple Lie group. Preprint. Available at `http://arxiv.org/abs/1101.5382`.

[KS99] Robert E. Kottwitz and Diana Shelstad. Foundations of twisted endoscopy. *Astérisque*, (255):vi+190, 1999.

[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.

[Lur01] Jacob Lurie. On simply laced Lie algebras and their minuscule representations. *Comment. Math. Helv.*, 76(3):515–575, 2001.

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

[PR12] Bjorn Poonen and Eric Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012.

[Ree10] Mark Reeder. Torsion automorphisms of simple Lie algebras. *Enseign. Math. (2)*, 56(1-2):3–47, 2010.

[Ree11] Mark Reeder. Elliptic centralizers in Weyl groups and their coinvariant representations. *Represent. Theory*, 15:63–111, 2011.

[Ric82a] R. W. Richardson. Conjugacy classes of involutions in Coxeter groups. *Bull. Austral. Math. Soc.*, 26(1):1–15, 1982.

[Ric82b] R.W. Richardson. Orbits, invariants, and representations associated to involutions of reductive groups. *Invent. Math.*, 66:287–312, 1982.

[RLYG12] Mark Reeder, Paul Levy, Jiu-Kang Yu, and Benedict H. Gross. Gradings of positive rank on simple Lie algebras. *Transform. Groups*, 17(4):1123–1190, 2012.

[Ste68] Robert Steinberg. *Endomorphisms of linear algebraic groups.* Memoirs of the American Mathematical Society, No. 80. American Mathematical Society, Providence, R.I., 1968.

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

[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, 1966.

[Wan13] Xiaoheng Wang. *Pencils of quadrics and Jacobians of hyperelliptic curves.* ProQuest LLC, Ann Arbor, MI, 2013. Thesis (Ph.D.)–Harvard University.