

# *Algebra & Number Theory*

Volume 20  
2026  
No. 1

**Reduction theory for stably graded Lie algebras**

Jack A. Thorne



# Reduction theory for stably graded Lie algebras

Jack A. Thorne

We define a reduction covariant for the representations à la Vinberg associated to stably graded Lie algebras. We then give an analogue of the LLL algorithm for the odd split special orthogonal group and show how this can be combined with our theory to effectively reduce the coefficients of vectors in a representation connected to 2-descent for odd hyperelliptic curves.

1. Introduction	195
2. The reduction covariant	197
3. Example: the stable $\mathbf{Z}/2\mathbf{Z}$ -grading of $\mathfrak{sl}_{2g+1}$	200
4. A reduction algorithm for $\mathrm{SO}(J)$	202
5. Example: Reducing a self-adjoint linear operator	206
References	207

## 1. Introduction

Let  $\mathfrak{h}$  be a semisimple Lie algebra over a field  $k$  of characteristic 0, and let  $m \geq 1$ . By a  $\mathbf{Z}/m\mathbf{Z}$ -grading, we mean a direct sum decomposition

$$\mathfrak{h} = \bigoplus_{i \in \mathbf{Z}/m\mathbf{Z}} \mathfrak{h}_i,$$

where for all  $i, j$  we have  $[\mathfrak{h}_i, \mathfrak{h}_j] \subset \mathfrak{h}_{i+j}$ . To such a grading, we can associate a pair  $(G, V)$ , where  $G$  is the connected component of the identity in the group of automorphisms of  $\mathfrak{h}$  which preserve the grading, and  $V = \mathfrak{h}_1$  is a  $k$ -vector space which is naturally a representation of the reductive group  $G$ . This representation is coregular, in the sense that the ring  $k[V]^G$  of invariant polynomials is freely generated and the geometric quotient  $B = \mathrm{Spec} k[V]^G$  is isomorphic to affine space [Vinberg 1976].

We say that the grading is stable if  $V$  contains  $G$ -orbits which are stable in the sense of geometric invariant theory (i.e., closed, with finite stabilizers in  $G$ ). In this case the  $G$ -invariant locus  $V^s \subset V$  of stable vectors is Zariski open and non-empty, and it is of interest to study the set of  $G(k)$ -orbits in a given geometric stable orbit. The stable gradings have been classified in [Reeder et al. 2012] (at least when  $k$  is algebraically closed) and experience shows that it is frequently the case that there is a family of projective curves  $C \rightarrow B^s$  and for each  $b \in B^s(k)$  an injection

$$\mathrm{Pic}^0 C_b(k)/m \mathrm{Pic}^0 C_b(k) \hookrightarrow G(k) \backslash V_b(k).$$

MSC2020: 11F06, 20G20.

Keywords: reduction theory, arithmetic groups.

When  $k = \mathbf{Q}$ , this can often be extended to an injection

$$\mathrm{Sel}_m \mathrm{Pic}^0 C_b \hookrightarrow G(\mathbf{Q}) \backslash V_b(\mathbf{Q}),$$

with source the  $m$ -Selmer group of the Jacobian variety  $\mathrm{Pic}^0 C_b$  and image contained in the image of the map

$$G(\mathbf{Z}) \backslash V_b(\mathbf{Z}) \rightarrow G(\mathbf{Q}) \backslash V_b(\mathbf{Q})$$

(for a suitable choice of integral structures). For example, this is the case for stable  $\mathbf{Z}/m\mathbf{Z}$ -gradings of the semisimple Lie algebras of types  $A_2$ ,  $D_4$ ,  $E_6$  and  $E_8$  for  $m = 2, 3, 4$  and  $5$ , respectively, in which case  $C$  can be taken to be the Weierstrass family of elliptic curves (see [Cremona et al. 2010; Fisher 2013]), and for the stable  $\mathbf{Z}/2\mathbf{Z}$ -gradings of the semisimple Lie algebras of types  $A_n$ ,  $D_n$ , and  $E_n$  (see [Bhargava and Gross 2013; Shankar 2019; Laga 2022], for example).

It is therefore of particular interest to be able to understand the sets  $G(\mathbf{Z}) \backslash V_b(\mathbf{Z})$  of integral orbits. This is the goal of reduction theory, which can be understood in this context to have two steps.

In the first step, one defines a *reduction covariant*, i.e., a  $G(\mathbf{R})$ -equivariant map

$$\mathcal{R} : V^s(\mathbf{R}) \rightarrow X_G,$$

where  $X_G$  is the symmetric space of  $G$  (i.e., the homogeneous space  $G(\mathbf{R})/K$ , where  $K$  is a maximal compact mod centre subgroup of  $G(\mathbf{R})$ ). In the second step, one introduces a notion of reducedness for elements of the symmetric space  $X_G$ , and says that an element  $T \in V^s(\mathbf{R})$  is reduced if its reduction covariant  $\mathcal{R}(T)$  satisfies this condition. For example, suppose given a fundamental set  $\mathcal{F} \subset X_G$  for the action of  $G(\mathbf{Z})$ , i.e., a subset of  $\mathcal{F}$  such that  $G(\mathbf{Z}) \cdot \mathcal{F} = X_G$  and  $\mathcal{F}$  intersects each orbit of  $G(\mathbf{Z})$  finitely many times. Then we could say that  $T$  is  $\mathcal{F}$ -reduced if  $\mathcal{R}(T) \in \mathcal{F}$ . An immediate consequence is that any  $T \in V^s(\mathbf{R})$  is  $G(\mathbf{Z})$ -conjugate to an  $\mathcal{F}$ -reduced element, and that if  $b \in B(\mathbf{Z}) \cap B^s(\mathbf{R})$  then  $V_b(\mathbf{Z})$  contains only finitely many  $\mathcal{F}$ -reduced elements.

In this paper we consider both the first and second steps described in the previous paragraph. Reduction covariants have been defined in the literature in some isolated cases for representations arising from stably graded Lie algebras (including, in the papers [Cremona et al. 2010; Fisher 2013], for the representations  $V$  associated to  $m$ -descent on elliptic curves for  $m = 2, 3, 4, 5$ ). The first main result (Theorem 2.7) of this paper is the definition of a reduction covariant  $\mathcal{R} : V^s(\mathbf{R}) \rightarrow X_G$  for any stably  $\mathbf{Z}/m\mathbf{Z}$ -graded Lie algebra. To define it, we think of  $X_G$  as the space of Cartan involutions of the real semisimple group  $G_{\mathbf{R}}$ . It turns out that for any Cartan subspace  $\mathfrak{c} \subset V_{\mathbf{R}}$ , there is a unique Cartan involution of  $\mathfrak{h}_{\mathbf{R}}$  which respects the grading and leaves  $\mathfrak{c}$  invariant. A stable vector  $T$  is contained in a unique Cartan subspace, and we define  $\mathcal{R}(T)$  to be the restriction of the Cartan involution associated to this subspace to  $G_{\mathbf{R}}$ .

Regarding the second step, a good starting point is the reduction theory of Borel and Harish-Chandra [Borel and Harish-Chandra 1962; Borel 2019]. They defined Siegel sets  $\mathfrak{S}_t \subset G(\mathbf{R})$ , which are rather explicit fundamental sets in the sense defined above, and which can serve to define a notion of reducedness. However, what is lacking in general is an explicit algorithm to transport elements into the Siegel set.

One case where the existing theory works well is when  $G$  is isogenous to  $\mathrm{SL}_n$  (or more generally, a product of such groups). In this case  $X_G$  may be identified with the set of lattices in  $\mathbf{R}^n$  of covolume 1 and lattice reduction algorithms (such as the LLL algorithm described in [Lenstra et al. 1982]) apply without change. The second main result of this paper, which appears in §4, is an algorithm to transport elements of  $X_G$  into a Siegel set in the case that  $G$  is a split special orthogonal group  $\mathrm{SO}_{2g+1}$ . This is the group that appears for the stable  $\mathbf{Z}/2\mathbf{Z}$ -grading of  $\mathfrak{sl}_{2g+1}$ , used in [Bhargava and Gross 2013] to study the 2-Selmer groups of Jacobians of odd hyperelliptic curves. This algorithm is based on the LLL algorithm. Roughly speaking, we observe that the two main steps of the LLL algorithm correspond either to acting by “integral unipotent transformations” or “simple reflections in  $S_n$ ”. We simply replace  $S_n$  by the Weyl group of  $\mathrm{SO}_{2g+1}$ . We consider the analogue of this, where  $\mathrm{SO}_{2g+1}$  is replaced by any split semisimple group, in another paper [Romano and Thorne 2025].

**1.1. Outline.** In §2, we define the reduction covariant  $\mathcal{R}$  using the theory of the Cartan involution. In §3, we compute the covariant explicitly in the case of the stable  $\mathbf{Z}/2\mathbf{Z}$ -grading of  $\mathfrak{sl}_{2g+1}$ . In §4, we give our algorithm to move a given element of  $X_{\mathrm{SO}_{2g+1}}$  into a Siegel set. Finally, in §5, we show how these ideas work together in an explicit example.

**1.2. Notation.** In this paper, a reductive group over a field  $k$  means a smooth connected linear algebraic group over a field  $k$  of trivial unipotent radical. In particular, by a reductive group  $H$  over  $\mathbf{R}$  we mean a connected algebraic group (although the associated set  $H(\mathbf{R})$  of real points might not be connected). Similarly, a semisimple group is a reductive group of trivial radical.

We will use gothic letters to denote Lie algebras (so  $\mathrm{Lie} H = \mathfrak{h}$ ) and subscripts to denote base extension (so if  $H$  is an algebraic group over  $\mathbf{R}$ , then  $(\mathrm{Lie} H) \otimes_{\mathbf{R}} \mathbf{C} = \mathfrak{h}_{\mathbf{C}}$ ). We use the notations  $Z_H(\cdot)$  and  $Z_{\mathfrak{h}}(\cdot)$  to denote group and Lie algebra centralizer, respectively.

We use superscript 0 to denote the connected component of the identity. Thus if  $H$  is a linear algebraic group over  $\mathbf{R}$  then there is an inclusion  $H(\mathbf{R})^0 \subset H^0(\mathbf{R})$  which is not in general an equality.

## 2. The reduction covariant

We will summarise the necessary properties of Cartan involutions of real reductive groups before proving the existence of the reduction covariant described in the introduction.

### 2.1. Background on Cartan involutions.

**Definition 2.2.** Let  $\mathfrak{h}$  be a semisimple Lie algebra over  $\mathbf{R}$ . A Cartan involution of  $\mathfrak{h}$  is a Lie algebra involution  $\theta : \mathfrak{h} \rightarrow \mathfrak{h}$  satisfying the following equivalent conditions:

- (1) The symmetric bilinear form  $B_{\theta}(X, Y) = -B(X, \theta Y) : \mathfrak{h} \times \mathfrak{h} \rightarrow \mathbf{R}$  (where  $B$  is the Killing form) is positive definite.
- (2) The  $\mathbf{R}$ -vector subspace  $\{X \in \mathfrak{h}_{\mathbf{C}} \mid \theta(X) = \bar{X}\}$  is a real form of  $\mathfrak{h}_{\mathbf{C}}$  which is compact, in the sense that its Killing form is negative definite.

It is convenient to define Cartan involutions for disconnected groups. We do this following [Adams and Taïbi 2018] (see also [Mostow 1955]).

**Definition 2.3.** Let  $H$  be a linear algebraic group over  $\mathbf{R}$  such that  $H^0$  is reductive. A Cartan involution of  $H$  is an involution  $\theta : H \rightarrow H$  such that

$$K_\theta = \{h \in H(\mathbf{C}) \mid \theta(h) = \bar{h}\}$$

is a compact subgroup of  $H(\mathbf{C})$  that meets every connected component of  $H(\mathbf{C})$ .

If  $\theta$  is a Cartan involution, then  $H(\mathbf{R})^\theta = K_\theta \cap H(\mathbf{R})$  is a maximal compact subgroup of  $H(\mathbf{R})$  [Adams and Taïbi 2018, §4].

Given an automorphism  $\theta$  of an algebraic group  $H$ , we will also write  $\theta$  for the induced automorphism of its Lie algebra  $\mathfrak{h}$ . The following proposition is well-known.

**Proposition 2.4.** *Let  $H$  be a semisimple group over  $\mathbf{R}$ , and let  $\theta$  be an involution of  $H$ . Then  $\theta : H \rightarrow H$  is a Cartan involution if and only if  $\theta : \mathfrak{h} \rightarrow \mathfrak{h}$  is a Cartan involution.*

**Proposition 2.5.** *Let  $H$  be a reductive group over  $\mathbf{R}$ .*

- (1) *Cartan involutions of  $H$  exist. If  $\theta, \theta'$  are Cartan involutions of  $H$ , then there exists  $h \in H(\mathbf{R})^0$  such that  $\theta' = \text{Ad}(h) \circ \theta \circ \text{Ad}(h^{-1})$ .*
- (2) *Suppose  $M \subset H$  is a closed subgroup and  $\theta$  is a Cartan involution of  $H$  such that  $\theta(M) = M$ . Then  $M^0$  is reductive and  $\theta|_M$  is a Cartan involution of  $M$ .*
- (3) *Suppose  $M \subset H$  is a closed subgroup with  $M^0$  reductive and that  $\theta_M$  is a Cartan involution of  $M$ . Then there exists a Cartan involution  $\theta_H$  of  $H$  extending  $\theta_M$ .*

*Proof.* See [Adams and Taïbi 2018, Theorem 3.12]. □

If  $H$  is a reductive group over  $\mathbf{R}$ , then we write  $X_H$  for the set of Cartan involutions of  $H$ . Proposition 2.5(1) shows that this is a homogeneous space for  $H(\mathbf{R})$ .

## 2.6. Application to graded Lie algebras.

**Theorem 2.7.** *Let  $\mathfrak{h}$  be a semisimple Lie algebra over  $\mathbf{R}$ . Suppose given a stable  $\mathbf{Z}/m\mathbf{Z}$ -grading  $\mathfrak{h} = \bigoplus_{i \in \mathbf{Z}/m\mathbf{Z}} \mathfrak{h}_i$ , and let  $(G, V)$  be the associated pair. Then:*

- (1) *For any stable vector  $T \in V^s(\mathbf{R})$ , there exists a unique Cartan involution  $\theta_T$  of  $H$  such that  $[T, \theta_T(T)] = 0$  and  $\theta_T(\mathfrak{h}_i) \subset \mathfrak{h}_{-i}$  for each  $i \in \mathbf{Z}/m\mathbf{Z}$ .*
- (2) *The map  $\mathcal{R} = \mathcal{R}_\mathfrak{h} : V^s(\mathbf{R}) \rightarrow X_G$  defined by  $T \mapsto \theta_T|_G$  is  $G(\mathbf{R})$ -equivariant.*

*Proof.* Let  $H$  denote the adjoint group over  $\mathbf{R}$  with Lie algebra  $\mathfrak{h}$ ; then  $\text{Aut}(H) = \text{Aut}(\mathfrak{h})$ , and the embedding  $\text{Ad} : H \rightarrow \text{Aut}(H)$  allows us to identify  $H$  with the connected component of the identity of the linear algebraic group  $\text{Aut}(H)$ . Since  $T$  is stable, it is regular semisimple when viewed as an element of  $\mathfrak{h}$  [Reeder et al. 2012, Lemma 13]. Let  $\mathfrak{c} = Z_\mathfrak{h}(T)$ , a Cartan subalgebra of  $\mathfrak{h}$  since  $T$  is regular semisimple, and let  $C = Z_H(T)$  denote the maximal torus of  $H$  with Lie algebra  $\mathfrak{c}$ .

Let us first establish uniqueness. If a Cartan involution  $\theta_T$  with the given properties exists, then the identity  $[T, \theta_T(T)] = 0$  shows that  $\theta_T$  normalises  $\mathfrak{c}$  and  $C$ . The restriction of  $\theta_T$  to  $C$  must be a Cartan involution of  $C$ . The torus  $C$  has a unique Cartan involution  $\theta_C$ , so if  $\theta'_T$  is another Cartan involution with the given properties, then we can write  $\theta'_T = t\theta_T$  for some  $t \in C(\mathbf{R})$ .

Giving an  $\mathbf{Z}/m\mathbf{Z}$ -grading is equivalent to giving a homomorphism  $\mu_m \rightarrow \text{Aut}(\mathfrak{h})$ . Let  $\sigma : \mathfrak{h}_{\mathbf{C}} \rightarrow \mathfrak{h}_{\mathbf{C}}$  be the image of  $e^{2\pi i/m} \in \mu_m(\mathbf{C})$ . The inclusion  $\theta_T(\mathfrak{h}_i) \subset \mathfrak{h}_{-i}$  may be equivalently expressed as  $\sigma\theta_T = \theta_T\bar{\sigma}$ . The identities  $\sigma\theta_T = \theta_T\bar{\sigma}$ ,  $\sigma t\theta_T = t\theta_T\bar{\sigma}$  together imply that  $t \in C^\sigma(\mathbf{R})$ . This group is finite (because the grading is stable), hence compact, which implies that  $t, \theta_T$  commute, and so  $t^2 = 1$ . We now consider the positive definite symmetric bilinear forms  $B_{\theta_T}, B_{t\theta_T}$  on  $\mathfrak{h}$ . Computing

$$B_{t\theta_T}(X, Y) = -B(X, t\theta_T Y) = -B(t^{-1}X, \theta_T Y) = B_{\theta_T}(t^{-1}X, Y) = B_{\theta_T}(X, tY)$$

shows that (with respect to the inner product determined by  $B_{\theta_T}$ )  $t$  is an orthogonal endomorphism of  $\mathfrak{h}$  with the property that  $B_{\theta_T}(tX, X) > 0$  for every non-zero  $X \in \mathfrak{h}$ . Since  $t^2 = 1$ , this is only possible if  $t = 1$ , hence  $\theta_T = \theta'_T$ .

We now establish existence of  $\theta_T$ . Let  $M = C \times \mu_m \subset \text{Aut}(H)$ , and let  $\theta_M$  be the Cartan involution of  $M$  given by the formula  $\theta_M(c \times \sigma) = \theta_C(c) \times \bar{\sigma}$ . To show that this is a group homomorphism, we must show that the identity  $\sigma\theta_C = \theta_C\bar{\sigma}$  holds in  $\text{Aut}(C_{\mathbf{C}})$ . Let  $K_C \subset C(\mathbf{C})$  be the unique maximal compact subgroup. If  $x \in K_C$ , then  $\theta_C(x) = \bar{x}$  and  $\sigma(x) \in K_C$ . For such  $x$ , we have  $\sigma\theta_C(x) = \sigma(\bar{x})$  and  $\theta_C\bar{\sigma}(x) = \overline{\sigma(x)} = \sigma(\bar{x}) = \sigma\theta_C(x)$ . Since  $K_C$  is Zariski dense in  $C_{\mathbf{C}}$ , this shows that in fact  $\sigma\theta_C = \theta_C\bar{\sigma}$ .

By Proposition 2.5, we can extend  $\theta_M$  to a Cartan involution  $\theta$  of  $\text{Aut}(H)$ . We set  $\theta_T = \theta|_H$ . We claim that  $\theta_T$  has the desired properties. It normalises  $C$  by construction, so satisfies  $[T, \theta_T(T)] = 0$ . We must show that  $\sigma\theta_T = \theta_T\bar{\sigma}$  in  $\text{Aut}(H)(\mathbf{C})$ . To this end, we note that if  $h \in H(\mathbf{C}) \subset \text{Aut}(H)(\mathbf{C})$ , and  $\alpha \in \text{Aut}(H)(\mathbf{C})$ , then  $\alpha h \alpha^{-1} = \alpha(h)$ . (More transparently, we have  $\alpha \circ \text{Ad}(h) \circ \alpha^{-1} = \text{Ad}(\alpha(h))$ .) Since  $\theta : \text{Aut}(H) \rightarrow \text{Aut}(H)$  is a group homomorphism, we have

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

The right-hand side equals  $\theta(\alpha)(\theta_T(h))$ , while the left-hand side equals

$$\theta(\alpha(h)) = \theta_T(\alpha(h)).$$

Since  $h$  is arbitrary, this gives the identity  $\theta(\alpha) \circ \theta_T = \theta_T \circ \alpha$  (composition in  $\text{Aut}(H)(\mathbf{C})$ ). Taking  $\alpha = \bar{\sigma}$  and using the identity  $\theta(\bar{\sigma}) = \theta_M(\bar{\sigma}) = \sigma$ , we find  $\sigma\theta_T = \theta_T\bar{\sigma}$ , as required. This completes the proof of the first part of the theorem. The second part follows from the properties that uniquely characterize  $\theta_T$ .  $\square$

We now record some basic properties of the reduction covariant  $\mathcal{R}$ .

**Proposition 2.8.** (1) *Let  $\mathfrak{h}, \mathfrak{h}'$  be semisimple Lie algebras over  $\mathbf{R}$ . Suppose given stable  $\mathbf{Z}/m\mathbf{Z}$ -gradings*

$$\mathfrak{h} = \bigoplus_{i \in \mathbf{Z}/m\mathbf{Z}} \mathfrak{h}_i, \quad \mathfrak{h}' = \bigoplus_{i \in \mathbf{Z}/m\mathbf{Z}} \mathfrak{h}'_i.$$

*Let  $\mathfrak{h}'' = \mathfrak{h} \oplus \mathfrak{h}'$  with its induced  $\mathbf{Z}/m\mathbf{Z}$ -grading. Then, with the obvious notation,  $\mathcal{R}_{\mathfrak{h}''} = \mathcal{R}_{\mathfrak{h}} \times \mathcal{R}_{\mathfrak{h}'}$ .*

(2) Let  $\mathfrak{h}$  be a semisimple Lie algebra over  $\mathbf{R}$ . Suppose given a stable  $\mathbf{Z}/m\mathbf{Z}$ -grading  $\mathfrak{h} = \bigoplus_{i \in \mathbf{Z}/m\mathbf{Z}} \mathfrak{h}_i$ , and let  $(G, V)$  be the associated pair. Let  $\mathfrak{h}' = \text{Res}_{\mathbf{C}/\mathbf{R}}(\mathfrak{h}_{\mathbf{C}})$ , with its induced grading  $\mathfrak{h}' = \bigoplus_{i \in \mathbf{Z}/m\mathbf{Z}} \text{Res}_{\mathbf{C}/\mathbf{R}}(\mathfrak{h}_{i,\mathbf{C}})$ . Then this grading is stable and its associated pair may be identified as

$$(G', V') = (\text{Res}_{\mathbf{C}/\mathbf{R}} G_{\mathbf{C}}, \text{Res}_{\mathbf{C}/\mathbf{R}} V_{\mathbf{C}}).$$

Moreover, there is a commutative diagram

$$\begin{array}{ccc} V^s(\mathbf{R}) & \longrightarrow & V^s(\mathbf{C}) = (V')^s(\mathbf{R}) \\ \mathcal{R}_{\mathfrak{h}} \downarrow & & \downarrow \mathcal{R}_{\mathfrak{h}'} \\ X_G & \longrightarrow & X_{G'} \end{array}$$

*Proof.* The first part follows quickly from the definition of  $\mathcal{R}$ . For the second, we note that the stability of the grading of  $\mathfrak{h}'$  can be checked over  $\mathbf{C}$ . There is an isomorphism  $\mathfrak{h}'_{\mathbf{C}} \cong \mathfrak{h}_{\mathbf{C}} \oplus \mathfrak{h}_{\mathbf{C}}$ , so the grading of  $\mathfrak{h}'$  is stable. It is easy to check that  $(G', V')$  has the claimed form.

All arrows in the commutative diagram are the natural ones, except for the bottom arrow, which we need to define. Let  $\theta_G$  be a Cartan involution of  $G$ . We can then check directly from the definition that the involution  $\theta'_G$  of  $G'_{\mathbf{C}} \cong G_{\mathbf{C}} \times G_{\mathbf{C}}$ , given on complex points  $(x_1, x_2) \in G(\mathbf{C}) \times G(\mathbf{C})$  by the formula  $\theta'_G(x_1, x_2) = (\theta_G(x_2), \theta_G(x_1))$ , is defined over  $\mathbf{R}$  and is a Cartan involution. We send  $\theta_G$  to  $\theta'_G$ .

To show that the diagram is commutative, let  $T \in V^s(\mathbf{R})$  and let  $\theta_T$  be the associated Cartan involution of  $H$ , the adjoint group of  $\mathfrak{h}$ . Let  $T' \in V^s(\mathbf{C}) = (V')^s(\mathbf{R})$  be the image of  $T$  under the natural map. It follows from the definitions that  $\theta'_T$  (where  $\theta'_T$  is given by the same formula as in the previous paragraph) satisfies the conditions characterizing  $\theta_{T'}$ . This completes the proof.  $\square$

One possible use of the first part of Proposition 2.8 is the case where we start with a stably graded Lie algebra  $\mathfrak{h}_0$  over  $\mathbf{Q}$ , and take  $\mathfrak{h} = (\text{Res}_{K/\mathbf{Q}} \mathfrak{h}_0)_{\mathbf{R}}$ , for a number field  $K/\mathbf{Q}$ . We find that the reduction covariant of  $V^s(\mathbf{R}) = V^s_0(K \otimes_{\mathbf{Q}} \mathbf{R})$  is the product (over the set of infinite places  $v$  of  $K$ ) of the reduction covariants for the stably graded Lie algebras  $\text{Res}_{K_v/\mathbf{R}} \mathfrak{h}_{0,K_v}$ . One possible use of the second part is in computing the reduction covariant of  $V^s(\mathbf{R})$  explicitly. For example, if we start with the stable  $\mathbf{Z}/3\mathbf{Z}$ -grading of the exceptional Lie algebra  $\mathfrak{g}_2$ , then  $V$  is (close to) the space of binary cubic forms. In [Stoll and Cremona 2003], several reduction covariants on the space of binary cubic forms are considered, but it is shown that there is a unique one, namely the Julia invariant, which is compatible with extension of scalars from  $\mathbf{R}$  to  $\mathbf{C}$  (see [Stoll and Cremona 2003, Proposition 3.4]). This characterisation may be used to relate the reduction covariant  $\mathcal{R}$  we construct in this case to the Julia invariant.

### 3. Example: the stable $\mathbf{Z}/2\mathbf{Z}$ -grading of $\mathfrak{sl}_{2g+1}$

The stable  $\mathbf{Z}/m\mathbf{Z}$ -gradings of semisimple Lie algebras over  $\mathbf{C}$  have been classified [Reeder et al. 2012]. The first case is when  $m = 2$ ; then each semisimple Lie algebra over  $\mathbf{C}$  has a unique stable  $\mathbf{Z}/2\mathbf{Z}$ -grading, up to isomorphism.



show that if  $\theta_H = \theta_{H_0}$ , then  $H = H_0$ . However, if  $\theta_H = \theta_{H_0}$  then  $-H^{-1}{}^tX H = -{}^tX$  for all  $X \in \mathfrak{g}$ , so  $H$  is scalar (by Schur's lemma). Since  $H$  is positive definite and  $\det(H) = 1$ , this forces  $H = H_0$ .

Since the Lie bracket on  $\mathfrak{sl}_{2g+1}$  is given by  $[X, Y] = XY - YX$ , the second part of the proposition is asking for a unique  $H$  such that  $[T, \theta_H(T)] = 0$ . The existence and uniqueness therefore follows from Theorem 2.7.  $\square$

To complete Proposition 3.1, we explain how to compute  $H$  explicitly in terms of  $T$ . Supposing that  $H$  exists, we extend it to a Hermitian inner product on  $\mathbf{C}^{2g+1}$ . Since the characteristic polynomial of  $T$  has no repeated roots,  $T$  is diagonalisable, and we can find  $P \in \mathrm{GL}_{2g+1}(\mathbf{C})$  such that  $P^{-1}TP$  is diagonal. Since  $T$  is normal with respect to  $H$ , its eigenvectors are orthogonal and so  $D = {}^tPH\bar{P}$  is also diagonal, with positive real diagonal entries. Since  $T$  is also self-adjoint with respect to  $J$ ,  ${}^tPJP$  is also diagonal, and thus  ${}^tPH\bar{P}$ ,  ${}^tPJP$  commute. Starting with the identity  $H = JH^{-1}J$ , we get

$${}^tPH\bar{P} = {}^tPJH^{-1}J\bar{P} = {}^tPJP P^{-1}H^{-1}{}^t\bar{P}^{-1}{}^t\bar{P}J\bar{P} = {}^tPJP({}^t\bar{P}HP)^{-1}{}^t\bar{P}J\bar{P},$$

hence

$$D^2 = {}^tPH\bar{P}{}^t\bar{P}HP = {}^tPJP{}^t\bar{P}J\bar{P}.$$

This characterizes  $H$  uniquely as

$$H = {}^tP^{-1}({}^tPJP{}^t\bar{P}J\bar{P})^{1/2}{}^t\bar{P}^{-1}, \quad (3-1)$$

where  $P \in \mathrm{GL}_{2g+1}(\mathbf{C})$  is such that  $P^{-1}TP$  is diagonal.

#### 4. A reduction algorithm for $\mathrm{SO}(J)$

In this section, we will describe a reduction algorithm for the symmetric space  $X_G$  associated to the group  $G = \mathrm{SO}(J)$  introduced in §3. All of the action takes place on the group  $G$ : the ambient grading plays no role. To orient the reader, we note that we will have to consider three symmetric bilinear forms on  $\mathbf{R}^{2g+1}$  simultaneously. First, the form  $J$  defining the group  $G$ ; second, the standard inner product  $H_0$  on  $\mathbf{R}^{2g+1}$ , which defines a base point in  $X_G$ ; and third, a second inner product  $H$ , compatible with  $J$ , which we hope to bring closer to  $H_0$  using the action of the group  $G(\mathbf{Z})$ .

We continue to define

$$G = \mathrm{SO}(J) = \{x \in \mathrm{SL}_{2g+1} \mid {}^txJx = J\},$$

which we think of as a group scheme over  $\mathbf{Z}$ . We write  $A, N \subset G$  for the subgroups consisting of the diagonal and unipotent upper-triangular matrices, respectively. Then  $G_{\mathbf{Q}}$  is reductive, and  $A_{\mathbf{Q}}, A_{\mathbf{Q}}N_{\mathbf{Q}}$  are a maximal torus and Borel subgroup.

Let  $H_0$  denote the inner product on  $\mathbf{R}^{2g+1}$  with respect to which  $e_{-g}, \dots, e_g$  is an orthonormal basis. We define  $K \subset G(\mathbf{R})$  to be the subgroup of matrices that preserve  $H_0$ .

**Proposition 4.1.** (1)  $H_0$  is compatible with  $J$ , and  $K$  is a maximal compact subgroup of  $G(\mathbf{R})$ .

(2) The product map  $K \times A(\mathbf{R})^0 \times N(\mathbf{R}) \rightarrow G(\mathbf{R})$ ,  $(k, a, n) \mapsto kan$ , is a diffeomorphism.

(3) If  $H$  is an inner product which is compatible with  $J$ , then we can find a unique pair  $(a, n) \in A(\mathbf{R})^0 \times N(\mathbf{R})$  such that  $H = {}^t(an)H_0an$ .

*Proof.* Looking at Proposition 3.1 we see that  $H_0$  is compatible with  $J$  and  $\theta_0(x) = H_0^{-1}{}^t x^{-1} H_0 = {}^t x^{-1}$  is a Cartan involution of  $G_{\mathbf{R}}$ . Therefore  $K = G(\mathbf{R})^{\theta_0}$  is a maximal compact subgroup of  $G(\mathbf{R})$ . The second part of the proposition is a statement of the Iwasawa decomposition of  $G(\mathbf{R})$ , determined by the data of  $\theta_0$ ,  $A$ , and  $N$  [Knapp 2002, Theorem 7.31]. The third part of the proposition follows from the uniqueness of the Iwasawa decomposition and the fact that  $G(\mathbf{R})$  acts transitively on  $X_G$  with  $\text{Stab}_{G(\mathbf{R})}(\theta_0) = K$ .  $\square$

The components of the Iwasawa decomposition can be computed using the Gram–Schmidt process. Let  $e_{-g}^*, \dots, e_g^*$  denote the result of carrying out the Gram–Schmidt orthogonalization process on the basis  $e_{-g}, \dots, e_g$  with respect to the inner product defined by  $H$ . Thus we have formulae

$$e_{-g} = e_{-g}^*, \dots, e_j = e_j^* + \sum_{i=-g}^{j-1} \mu_{i,j} e_i^*, \dots, e_g = e_g^* + \sum_{i=-g}^{g-1} \mu_{i,g} e_i^*.$$

with

$$\mu_{i,j} = (e_j, e_i^*)_H / (e_i^*, e_i^*)_H.$$

In particular, we take  $\mu_{j,j} = 1$  and  $\mu_{i,j} = 0$  if  $i > j$ .

**Lemma 4.2.** Let  $n = n_H = (\mu_{i,j})_{-g \leq i, j \leq g}$  and  $a = a_H = \text{diag}(\|e_i^*\|_H)_{-g \leq i \leq g}$ . Then  $a \in A(\mathbf{R})^0$ ,  $n \in N(\mathbf{R})$ , and  $H = {}^t(an)an$ .

*Proof.* Let  $\theta_1$  denote the Cartan involution  $\theta_1 : \text{SL}_{2g+1} \rightarrow \text{SL}_{2g+1}$ ,  $g \mapsto {}^t g^{-1}$ . Let  $K_1 = \text{SL}_{2g+1}(\mathbf{R})^{\theta_1}$  and let  $A_1, N_1$  be the subgroups of diagonal and unipotent upper-triangular matrices in  $\text{SL}_{2g+1}$ , respectively. The Iwasawa decomposition for  $\text{SL}_{2g+1}$  is the statement that the product map

$$K_1 \times A_1(\mathbf{R})^0 \times N_1(\mathbf{R}) \rightarrow \text{SL}_{2g+1}(\mathbf{R})$$

is a diffeomorphism. It is a standard fact that the Gram–Schmidt process gives the Iwasawa decomposition for  $\text{SL}_{2g+1}$ , in the sense that  $H = {}^t(an)an$  and that these are the unique elements  $a \in A_1(\mathbf{R})^0$ ,  $n \in N_1(\mathbf{R})$  with this property. We need to explain why the assumption that  $H, J$  are compatible implies that in fact  $a, n$  lie in  $G(\mathbf{R})$ . However, we have  $K \leq K_1$ ,  $A \leq A_1$ , and  $N \leq N_1$ , by construction, so the existence of the Iwasawa decomposition for  $G$  and the uniqueness for  $\text{SL}_{2g+1}$  implies that the Gram–Schmidt process for  $\text{SL}_{2g+1}$  must be compatible with the Iwasawa decomposition for  $G$ .  $\square$

**Lemma 4.3.** For any  $n = (n_{ij}) \in N(\mathbf{R})$ , there exists  $m \in N(\mathbf{Z})$  satisfying the following conditions:

- (1)  $|(nm)_{ij}| \leq 1/2$  for all  $-g \leq i < j$ ,  $j = -g, \dots, -1$ .
- (2)  $|(nm)_{i,0}| \leq 1$  for all  $-g \leq i \leq -1$ .
- (3)  $|(nm)_{i,j}| \leq 1/2$  for all  $-g \leq i < -j$ ,  $j = 1, \dots, g$ .

*Proof.* Right multiplication by  $m$  corresponds to performing column operations on  $n$ . We can check that the following column operations on  $n$  are induced by elements of  $N(\mathbf{Z})$ :

- $A(i, j, q)$ : For  $q \in \mathbf{Z}$ ,  $-g \leq j \leq -1$ , and  $-g \leq i < j$ , add  $q$  times column  $i$  to column  $j$  and  $-q$  times column  $-j$  to column  $-i$ .
- $B(i, q)$ :  $q \in 2\mathbf{Z}$ ,  $-g \leq i \leq -1$ , add  $q$  times column  $i$  to column 0, and add  $-q$  times column 0 and  $-q^2/2$  times column  $i$  to column  $-i$ .
- $C(i, j, q)$ :  $q \in \mathbf{Z}$ ,  $1 \leq j \leq g$ , and  $-g \leq i \leq -j$ , add  $q$  times column  $i$  to column  $j$  and  $-q$  times column  $-j$  to column  $-i$ .

We therefore carry out column operations as follows in order to satisfy the conditions of the lemma (noting that the order of operations is chosen so that once we have forced a given  $n_{ij}$  to satisfy the conditions of the lemma, its value will not be changed by later operations):

- (1) For each  $j = -g, \dots, -1$ , then for each  $i = j - 1, j - 2, \dots, -g$ , let  $q$  denote the closest integer to  $n_{ij}$  and do  $A(i, j, -q)$ .
- (2) For each  $i = -1, \dots, -g$ , let  $q$  denote the closest even integer to  $n_{i0}$  and do  $B(i, -q)$ .
- (3) For each  $j = 1, \dots, g$ , then for each  $i = -j - 1, \dots, -g$ , let  $q$  denote the closest integer to  $n_{ij}$  and do  $C(i, j, -q)$ . □

The following definition is the analogue in our context of [Lenstra et al. 1982, (1.4), (1.5)].

**Definition 4.4.** Let  $\delta \in (1/2, 1)$ , and let  $H$  be an inner product on  $\mathbf{R}^{2g+1}$  compatible with  $J$ . We say that  $H$  is  $\delta$ -reduced if the following conditions are satisfied:

- (1)  $n_H$  satisfies the conditions of Lemma 4.3.
- (2) For each  $i = -g + 1, \dots, -1$ , we have  $\|e_i^* + \mu_{i-1,i} e_{i-1}^*\|_H^2 \geq \delta \|e_{i-1}^*\|_H^2$ .
- (3)  $\|e_1^* + \mu_{0,1} e_0^* + \mu_{-1,1} e_{-1}^*\|_H^2 \geq \delta^2 \|e_{-1}^*\|_H^2$ .

**Remark 4.5.** The above conditions may be reformulated in terms of the matrices  $n_H, a_H$  as follows (writing  $a_H = \text{diag}(a_{-g}, \dots, a_g)$ ):

- (1)  $n_H$  satisfies the conditions of Lemma 4.3.
- (2) For each  $i = -g + 1, \dots, -1$ , we have  $a_i^2 + \mu_{i-1,i}^2 a_{i-1}^2 \geq \delta a_{i-1}^2$  (as the  $e_j^*$  are pairwise orthogonal).
- (3)  $a_{-1}^{-2} + \frac{1}{2} \mu_{-1,0}^2 \geq \delta$  (noting that as  $n_H, a_H \in G(\mathbf{R})$ , we have the relations  $a_{-1} a_1 = a_0 = 1, \mu_{0,1} = -\mu_{-1,0}$ , and  $\mu_{-1,1} = -\mu_{-1,0}^2/2$ ).

We note that these conditions involve only about half the entries of the matrices  $n_H, a_H$ . However, because these matrices lie in the group  $\text{SO}_{2g+1}(\mathbf{R})$ , these entries determine the remaining ones.

The following lemma shows that if  $H$  is  $\delta$ -reduced, then it lies in a Siegel set. We recall (see [Borel 2019, Theorem 15.4]) that Siegel sets are fundamental sets for the action of the arithmetic group  $G(\mathbf{Z})$ , in the sense defined in the introduction to this paper. This lemma can be used to show that if  $H$  is  $\delta$ -reduced, then it has other desirable properties. For example, arguing as in the proof of [Lenstra et al. 1982, Proposition 1.6], one can show that there is a constant  $c = c_{g,\delta} > 0$  such that if  $H$  is  $\delta$ -reduced, then  $\prod_{j=-g}^g \|e_j\|_H^2 \leq c$ . (We thank the referee for this remark.)

**Lemma 4.6.** *If  $H$  is  $\delta$ -reduced, then  $a_H n_H$  lies in the Siegel set  $\mathfrak{S}_\delta = K A_\delta N_c$  defined as follows:*

$$A_\delta = \{a = (a_{-g}, \dots, a_g) \in A(\mathbf{R})^0 \mid \forall i = -g, \dots, -2, a_i/a_{i+1} \leq (\delta - 1/4)^{-1/2}; a_{-1} \leq (\delta - 1/2)^{-1/2}\},$$

$$N_c = \{n \in N(\mathbf{R}) \mid \forall j = -g, \dots, -1, -g \leq i < j, \max(|n_{ij}|, |n_{i,-j}|) \leq 1/2; \forall i = -g, \dots, -1, |n_{i0}| \leq 1\}.$$

*Proof.* Since  $n_H$  lies in  $N_c$  by definition of being  $\delta$ -reduced, we just need to check that  $a_H$  satisfies the required inequalities. Re-arranging gives

$$a_{i+1}^2/a_i^2 \geq \delta - \mu_{i,i+1}^2 \geq \delta - 1/4$$

for each  $i = -g, \dots, -2$ , and

$$a_1^2 \geq \delta - \mu_{-1,0}^2/2 \geq \delta - 1/2,$$

as required. □

The Weyl group  $W(G, A)$  is generated by its simple reflections (with respect to the choice of positive roots determined by  $N$ ). These simple reflections can be represented by the following elements  $s_{-g}, \dots, s_{-1}$  of  $G(\mathbf{Z})$ , which we define by their action on basis vectors:

- For each  $i = -g, \dots, -2$ ,  $s_i$  sends  $e_i$  to  $e_{i+1}$ ,  $e_{i+1}$  to  $e_i$ ,  $e_{-i}$  to  $e_{-(i+1)}$ ,  $e_{-(i+1)}$  to  $e_{-i}$ , and fixes the remaining basis vectors.
- $s_{-1}$  sends  $e_{-1}$  to  $e_1$ ,  $e_1$  to  $e_{-1}$ ,  $e_0$  to  $-e_0$ , and fixes the remaining basis vectors.

Here finally is an algorithm which, starting with any  $H$  as above, finds  $\gamma \in G(\mathbf{Z})$  such that  ${}^t\gamma H \gamma$  is  $\delta$ -reduced:

- (1) Let  $\gamma_1 = 1$ ,  $H_1 = H$ .
- (2) Set  $H_1 := {}^t\gamma_1 H \gamma_1$ . Compute the matrices  $n_{H_1} = (\mu_{i,j})$ ,  $a_{H_1} = \text{diag}(a_{-g}, \dots, a_g)$  using Gram–Schmidt.
- (3) If  $n_{H_1}$  satisfies the conditions of Lemma 4.3, then proceed to Step 4. Else, find  $\gamma_n$  such that  $n_{H_1} \gamma_n$  satisfies the conditions of Lemma 4.3, set  $\gamma_1 := \gamma_1 \gamma_n$ , and go to Step 2.
- (4) For each  $i = -g, \dots, -2$ : if  $a_{i+1}^2 + \mu_{i,i+1}^2 a_i^2 < \delta a_i^2$ , set  $\gamma_1 := \gamma_1 s_i$  and go to Step 2.
- (5) If  $a_{-1}^{-2} + \frac{1}{2} \mu_{-1,0}^2 < \delta$ , set  $\gamma_1 := \gamma_1 s_{-1}$  and go to Step 2.
- (6) Return  $\gamma_1$ .

In practice, it is more efficient to run Gram–Schmidt once (for the matrix  $H$ ) and then to update the matrices  $n_{H_1}$ ,  $a_{H_1}$  at each step. Explicit formulae describing how to do this are given in [Romano and Thorne 2025].

**Proposition 4.7.** *The above algorithm always terminates.*

*Proof.* It suffices to show that the simple reflections  $s_i$  are applied only finitely many times. At each instance of Step 2 we are given a basis  $f_i = \gamma_1 e_i$  of  $\mathbf{Z}^{2g+1}$ , to which we associate the flag  $F_i = \bigoplus_{k=-g}^i \mathbf{Z} f_k$ ,  $i = -g, \dots, g$ . If  $i = -g, \dots, -2$ , then acting by  $s_i$  changes  $F_i$  and  $F_{-(i+1)}$  but leaves the remaining  $F_j$

unchanged. Acting by  $s_{-1}$  changes  $F_{-1}$  and  $F_0$  and leaves the remaining  $F_j$  unchanged. In particular, among  $F_{-g}, \dots, F_{-1}$ ,  $s_i$  changes only  $F_i$ .

The inner product  $H$  on  $\mathbf{R}^{2g+1}$  determines one on  $\wedge^i \mathbf{R}^{2g+1}$  for each  $i = 1, \dots, 2g + 1$  by the usual formula  $(x_1 \wedge \dots \wedge x_i, y_1 \wedge \dots \wedge y_i)_H = \det((x_j, y_k)_H)$ . Since  $\wedge^i \mathbf{Z}^{2g+1}$  contains finitely many vectors of bounded norm, it suffices to show that applying the simple reflection  $s_i$  decreases the squared norm of the vector (which, up to sign, depends only on  $F_i$ )  $f_{-g} \wedge \dots \wedge f_i \in \wedge^{i+g+1} \mathbf{Z}^{2g+1}$ . A calculation shows that this squared norm is multiplied by a scalar which is strictly less than  $\delta$ . As  $\delta < 1$ , this completes the proof.  $\square$

### 5. Example: Reducing a self-adjoint linear operator

We now show how to combine the theory of the previous two sections in an example. Take  $g = 3$ , and consider the group  $G = \text{SO}(J) \subset \text{SL}_7$  and representation  $V \subset \mathfrak{sl}_7$  associated to the  $\mathbf{Z}/2\mathbf{Z}$ -grading of  $\mathfrak{sl}_7$  defined in §3. We consider the genus-3 hyperelliptic curve

$$C_f : y^2 = f(x) = x^7 - x^5 - 2x^4 - x^3 + 5x - 5.$$

This curve has the integral point  $P = (14, 10237)$ . Associated to  $P$  is the matrix

$$T = \begin{pmatrix} -14 & 1 & 0 & 0 & 0 & 0 & 0 \\ -195 & 0 & 1 & 0 & 0 & 0 & 0 \\ -2728 & 0 & 7 & 0 & -1 & 0 & 0 \\ -10237 & 0 & 0 & 14 & 0 & 0 & 0 \\ 19095 & -6 & -48 & 0 & 7 & 1 & 0 \\ 1546 & -26 & -6 & 0 & 0 & 0 & 1 \\ 390 & 1546 & 19095 & -10237 & -2728 & -195 & -14 \end{pmatrix} \in V(\mathbf{Z})$$

of characteristic polynomial  $f(x)$ , which we obtain, say, from the subregular Slodowy slice studied in [Thorne 2013]. We compute the reduction covariant  $H = \mathcal{R}(T) \in X_{\text{SO}(J)}$  using the formula (3-1). We obtain numerically

$$H = \begin{pmatrix} 3.74708 & 53.7691 & 750.242 & 2813.43 & -5244.78 & -421.526 & -47.2448 \\ 53.7691 & 776.143 & 10830.1 & 40612.6 & -75708.6 & -6080.03 & -681.676 \\ 750.242 & 10830.1 & 151130. & 566729. & -1.05648 \times 10^6 & -84842.6 & -9520.71 \\ 2813.43 & 40612.6 & 566729. & 2.12521 \times 10^6 & -3.96175 \times 10^6 & -318157. & -35704.6 \\ -5244.78 & -75708.6 & -1.05648 \times 10^6 & -3.96175 \times 10^6 & 7.38537 \times 10^6 & 593097. & 66564.2 \\ -421.526 & -6080.03 & -84842.6 & -318157. & 593097. & 47660.8 & 5338.34 \\ -47.2448 & -681.676 & -9520.71 & -35704.6 & 66564.2 & 5338.34 & 660.273 \end{pmatrix}.$$

We then apply the algorithm of §4 to  $H$  with  $\delta = 0.9$  to obtain an element  $\gamma_1 \in G(\mathbf{Z})$  such that  ${}^t\gamma_1 H \gamma_1$  is  $\delta$ -reduced. The resulting matrix is

$$\gamma_1 = \begin{pmatrix} -2 & -1 & -15 & 2 & -3 & -5 & 26 \\ 0 & -8 & -117 & 12 & 0 & 9 & 203 \\ -8 & -104 & -1462 & 180 & -16 & 184 & 2557 \\ 4 & 56 & 784 & -97 & 8 & -98 & -1372 \\ 1 & 15 & 209 & -26 & 2 & -26 & -366 \\ 0 & 1 & 15 & -2 & 0 & -2 & -26 \\ 0 & 0 & 1 & 0 & 0 & 0 & -2 \end{pmatrix},$$

yielding

$$\gamma_1^{-1}T\gamma_1 = \begin{pmatrix} 0 & 0 & -1 & 2 & 2 & -2 & 3 \\ 1 & 0 & 1 & 0 & 0 & 0 & -2 \\ 0 & 1 & 1 & -2 & 0 & 0 & 2 \\ 0 & 0 & 1 & -2 & -2 & 0 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

**Remark 5.1.** Since the lower left-hand  $3 \times 3$  submatrix of  $\gamma_1^{-1}T\gamma_1$  is 0, we see that the orbit of  $T$  is distinguished, in the sense of [Bhargava and Gross 2013]. It follows that the divisor class of  $P - P_\infty$  is divisible by 2 in  $J_f(\mathbf{Q})$  (where  $P_\infty$  is the point at infinity of  $C_f$  and  $J_f$  is the Jacobian of  $C_f$ ). This could also be checked using the usual theory of 2-descent (see [Schaefer 1995], for example) by noting that the class of  $14 - x$  in the group  $L_f^\times / (L_f^\times)^2$  (where  $L_f = \mathbf{Q}[x]/(f(x))$ ) is trivial.

## References

- [Adams and Taïbi 2018] J. Adams and O. Taïbi, “Galois and Cartan cohomology of real groups”, *Duke Math. J.* **167**:6 (2018), 1057–1097. [MR](#)
- [Bhargava and Gross 2013] M. Bhargava and B. H. Gross, “The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point”, pp. 23–91 in *Automorphic representations and L-functions* (Mumbai, 2012), edited by D. Prasad et al., Tata Inst. Fund. Res. Stud. Math. **22**, Tata Inst. Fund. Res., Mumbai, 2013. [MR](#)
- [Borel 2019] A. Borel, *Introduction to arithmetic groups*, Univ. Lect. Ser. **73**, Amer. Math. Soc., Providence, RI, 2019. [MR](#)
- [Borel and Harish-Chandra 1962] A. Borel and Harish-Chandra, “Arithmetic subgroups of algebraic groups”, *Ann. of Math. (2)* **75** (1962), 485–535. [MR](#)
- [Cremona et al. 2010] J. E. Cremona, T. A. Fisher, and M. Stoll, “Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves”, *Algebra Number Theory* **4**:6 (2010), 763–820. [MR](#)
- [Fisher 2013] T. Fisher, “Minimisation and reduction of 5-coverings of elliptic curves”, *Algebra Number Theory* **7**:5 (2013), 1179–1205. [MR](#)
- [Knapp 2002] A. W. Knap, *Lie groups beyond an introduction*, 2nd ed., Progr. Math. **140**, Birkhäuser, Boston, MA, 2002. [MR](#)
- [Laga 2022] J. Laga, “The average size of the 2-Selmer group of a family of non-hyperelliptic curves of genus 3”, *Algebra Number Theory* **16**:5 (2022), 1161–1212. [MR](#)
- [Lenstra et al. 1982] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, “Factoring polynomials with rational coefficients”, *Math. Ann.* **261**:4 (1982), 515–534. [MR](#)
- [Mostow 1955] G. D. Mostow, “Self-adjoint groups”, *Ann. of Math. (2)* **62** (1955), 44–55. [MR](#)
- [Reeder et al. 2012] M. Reeder, P. Levy, J.-K. Yu, and B. H. Gross, “Gradings of positive rank on simple Lie algebras”, *Transform. Groups* **17**:4 (2012), 1123–1190. [MR](#)
- [Romano and Thorne 2025] B. Romano and J. A. Thorne, “An LLL algorithm with symmetries”, *Int. J. Number Theory* (online publication January 2025).
- [Schaefer 1995] E. F. Schaefer, “2-descent on the Jacobians of hyperelliptic curves”, *J. Number Theory* **51**:2 (1995), 219–232. [MR](#)
- [Shankar 2019] A. N. Shankar, “2-Selmer groups of hyperelliptic curves with marked points”, *Trans. Amer. Math. Soc.* **372**:1 (2019), 267–304. [MR](#)
- [Stoll and Cremona 2003] M. Stoll and J. E. Cremona, “On the reduction theory of binary forms”, *J. Reine Angew. Math.* **565** (2003), 79–99. [MR](#)
- [Thorne 2013] J. A. Thorne, “Vinberg’s representations and arithmetic invariant theory”, *Algebra Number Theory* **7**:9 (2013), 2331–2368. [MR](#)

[Thorne 2015] J. A. Thorne, “ $E_6$  and the arithmetic of a family of non-hyperelliptic curves of genus 3”, *Forum Math. Pi* **3** (2015), art. id. e1. [MR](#)

[Vinberg 1976] È. B. Vinberg, “The Weyl group of a graded Lie algebra”, *Izv. Akad. Nauk SSSR Ser. Mat.* **40**:3 (1976), 488–526. In Russian; translated in *Math. USSR-Izv.* **10** (1976), 463–495. [MR](#)

Communicated by Melanie Matchett Wood

Received 2024-04-03    Revised 2024-12-13    Accepted 2025-01-20

[thorne@dpmms.cam.ac.uk](mailto:thorne@dpmms.cam.ac.uk)

*Department of Pure Mathematics and Mathematical Statistics,  
University of Cambridge, Cambridge CB3 0WB, United Kingdom*

# Algebra & Number Theory

[msp.org/ant](http://msp.org/ant)

## EDITORS

### MANAGING EDITOR

Antoine Chambert-Loir  
Université Paris-Diderot  
France

### EDITORIAL BOARD CHAIR

David Eisenbud  
University of California  
Berkeley, USA

## BOARD OF EDITORS

Jason P. Bell	University of Waterloo, Canada	Philippe Michel	École Polytechnique Fédérale de Lausanne
Bhargav Bhatt	University of Michigan, USA	Martin Olsson	University of California, Berkeley, USA
Frank Calegari	University of Chicago, USA	Irena Peeva	Cornell University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Saclay, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Samit Dasgupta	Duke University, USA	Bjorn Poonen	Massachusetts Institute of Technology, USA
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Gavril Farkas	Humboldt Universität zu Berlin, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	SUNY Buffalo, USA
Wee Teck Gan	National University of Singapore	Shunsuke Takagi	University of Tokyo, Japan
Andrew Granville	Université de Montréal, Canada	Pham Huu Tiep	Rutgers University, USA
Ben J. Green	University of Oxford, UK	Ravi Vakil	Stanford University, USA
Christopher Hacon	University of Utah, USA	Akshay Venkatesh	Institute for Advanced Study, USA
Roger Heath-Brown	Oxford University, UK	Melanie Matchett Wood	Harvard University, USA
János Kollár	Princeton University, USA	Shou-Wu Zhang	Princeton University, USA
Michael J. Larsen	Indiana University Bloomington, USA		

## PRODUCTION

[production@msp.org](mailto:production@msp.org)

Silvio Levy, Scientific Editor

---

See inside back cover or [msp.org/ant](http://msp.org/ant) for submission instructions.

---

The subscription price for 2026 is US \$590/year for the electronic version, and \$865/year (+\$75, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.


---

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 2000 Allston Way # 59, Berkeley, CA 94701-4004, is published continuously online.

---

ANT peer review and production are managed by EditFLOW<sup>®</sup> from MSP.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2026 Mathematical Sciences Publishers

# Algebra & Number Theory

Volume 20    No. 1    2026

---

The average Mordell–Weil rank of elliptic surfaces over number fields	1
REMKÉ KLOOSTERMAN	
Syntomic complex and $p$ -adic nearby cycles	17
ABHINANDAN	
The Brauer–Manin obstruction for nonisotrivial curves over global function fields	109
BRENDAN CREUTZ and JOSÉ FELIPE VOLOCH	
On the failure of the integral Tate conjecture for products with projective hypersurfaces	119
KEES KOK	
Malcev completions, Hodge theory, and motives	147
EMIL JACOBSEN	
Reduction theory for stably graded Lie algebras	195
JACK A. THORNE	
Remarks on Landau–Siegel zeros	209
DEBMALYA BASAK, JESSE THORNER and ALEXANDRU ZAHARESCU	