Graded Lie Algebras, Compactified Jacobians and Arithmetic Statistics

Jef Christine S Laga

Department of Pure Mathematics and Mathematical Statistics
University of Cambridge

This dissertation is submitted for the degree of
Doctor of Philosophy

Trinity Hall

November 2021

Declaration

This thesis is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the preface and specified in the text. It is not substantially the same as any work that has already been submitted before for any degree or other qualification except as declared in the preface and specified in the text.

Jef Christine S Laga
November 2021

Abstract

A simply laced Dynkin diagram gives rise to a family of curves over $\mathbb{Q}$ and a coregular representation, using deformations of simple singularities and Vinberg theory respectively. Thorne has conjectured and partially proven a strong link between the arithmetic of these curves and the rational orbits of these representations.

In this thesis, we complete Thorne's picture and show that 2-Selmer elements of the Jacobians of the smooth curves in each family can be parametrised by integral orbits of the corresponding representation. Using geometry-of-numbers techniques, we deduce statistical results on the arithmetic of these curves. We prove these results in a uniform manner. This recovers and generalises results of Bhargava, Gross, Ho, Shankar, Shankar and Wang.

The main innovations are an analysis of torsors on affine spaces using results of Colliot-Thélène and the Grothendieck–Serre conjecture, a study of geometric properties of compactified Jacobians using the Białynicki-Birula decomposition, and a general construction of integral orbit representatives.

Acknowledgements

It's a great pleasure to thank the many people that have shaped my thesis years in Cambridge. First and foremost, I would like to thank Jack Thorne for being a fantastic supervisor. His knowledge, precision and approach to mathematics are inspiring. Thank you in particular for carefully proofreading many drafts. Jack, it has been a wonderful privilege being your student.

I thank Alex Bartel, Tom Fisher, Davide Lombardo, Jesse Leo Kass, Bjorn Poonen, Beth Romano, Tony Scholl and Ari Shnidman for discussions related to the contents of this thesis, in person or via email. I thank the people from the CMS and DPMMS for creating a wonderful work environment and a friendly atmosphere, in particular thank you to Tessa Blackman, Vivien Gruar and Julia Blackwell. I would also like to thank my fellow PhD students for surviving many seminars, lunches and rounds of Durak together.

I thank my friends from The Origin and Flour Street for being wonderful housemates. I thank my friends and family from Belgium for always supporting me, even though some of them might be wondering what it is exactly that I'm doing every day. I wish I could share the true beauty of mathematics with them.

I would like to thank Lia for all the love and support throughout these years. Finally, I would like to thank my mother, for everything.

Table of contents

1 Introduction **1**

1.1 Context 1
1.2 Statement of results 3
1.3 Relation to other works 5
1.4 Method of proof 6
1.5 Other coregular representations 8
1.6 Organisation 8
1.7 Notation 9

2 Background **11**

2.1 The adjoint quotient of a Lie algebra 11
2.2 Vinberg theory 13
2.3 Stable gradings 14
2.4 Arithmetic Invariant Theory 16
2.5 The Grothendieck–Serre conjecture 16

3 Around Thorne's thesis **19**

3.1 A split stable $\mathbb{Z}/2\mathbb{Z}$-grading 19
3.2 Explicit determination of (G,V) 21
3.3 The component group of H^{θ} 22
3.4 The fundamental group of G 24
3.5 Regular nilpotent elements in V 24
3.6 Kostant sections 25
3.7 A family of curves 25
3.8 Universal centralisers 27
3.9 Monodromy of $J^{\mathrm{rs}}[2]$ 29

4 The mildly singular locus **33**
4.1 The discriminant locus . . . 33
4.2 Representation theory over B^1 . . . 34
4.3 Geometry over B^1 . . . 37
4.4 Summary of properties of B^1 . . . 39

5 The compactified Jacobian **41**
5.1 Generalities on sheaves . . . 41
5.2 The definition . . . 43
5.3 Basic properties of $\bar{J}$ . . . 45
5.4 The Białynicki-Birula decomposition of $\bar{J}$ . . . 46

6 Constructing orbits **51**
6.1 Torsors on open subsets of affine space . . . 51
6.2 A universal torsor . . . 55
6.3 Constructing orbits for 2-descent elements . . . 57
6.4 Constructing orbits for 2-Selmer elements . . . 58
6.5 Reducible orbits and marked points . . . 59

7 Integral representatives **61**
7.1 Integral structures . . . 61
7.2 Spreading out . . . 62
7.3 Some stacks . . . 65
7.4 Orbits of square-free discriminant . . . 68
7.5 Proof of Theorem 7.2.4 . . . 72
7.6 Orbits over $\mathbb{Z}$ . . . 74

8 Geometry-of-numbers **77**
8.1 Heights . . . 77
8.2 Measures on G . . . 78
8.3 Measures on V . . . 79
8.4 Fundamental sets . . . 80
8.5 Counting integral orbits of V . . . 81
8.6 First reductions . . . 82
8.7 Averaging and counting lattice points . . . 83
8.8 End of the proof of Proposition 8.5.2 . . . 88
8.9 Congruence conditions . . . 88

8.10 Estimates on reducibility and stabilisers 90
8.11 Cutting off the cusp 92

9 The average size of the 2-Selmer group 95
9.1 An upper bound 95
9.2 A conditional lower bound 98

References 101

Appendix A Cutting off the cusp for D_{2n} 107
A.1 Recollections on even orthogonal groups 107
A.2 An explicit model for the split stable involution of D_{2n} 109
A.3 Reducibility conditions 113
A.4 Bounding the remaining cusp integrals 116

Chapter 1

Introduction

1.1 Context

This thesis is a contribution to arithmetic statistics of algebraic curves. Arithmetic statistics is concerned with the study of number-theoretic objects in families. For example, given a family $\mathscr{F}$ of (smooth, projective, geometrically integral) curves over $\mathbb{Q}$, one may ask about the statistical behaviour of:

- the rational points $C(\mathbb{Q})$ of $C \in \mathscr{F}$;
- the Mordell–Weil group, i.e. the rational points $J(\mathbb{Q})$ of the Jacobian variety of C;
- the 2-Selmer group (or more generally m-Selmer group) $\mathrm{Sel}_2 J$ of J.

Typically, understanding Selmer groups yields information about the Mordell–Weil group of J, which in turn may tell us something about the rational points of C. See [5] for a survey of conjectures concerning elliptic curves and [64] for a remarkable set of heuristics modelling Selmer groups of abelian varieties.

Over the last twenty years, Bhargava and his collaborators have made spectacular progress in arithmetic statistics. One of their key ideas is that many arithmetic objects can be parametrised by rational or integral orbits of a representation (G,V). When the representation is coregular, meaning that the ring of invariants $\mathbb{Q}[V]^G$ is a polynomial ring, they have developed powerful geometry-of-numbers techniques to count integral orbits of V. Combining orbit parametrisations with these counting techniques has led to many striking results; see [16, 17, 14, 15, 9, 11] for some highlights and [41, 7] for surveys of these results.

This raises the question: how does one find such orbit parametrisations? Typically, one may find them using classical constructions in algebraic geometry, such as in the following primordial example:

Example 1.1.1 (2-Selmer groups of elliptic curves)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then every element of the* 2*-Selmer group* $\mathrm{Sel}_2 E$ *of E can be represented by the isomorphism class of a double cover $C \xrightarrow{2:1} S$ ramified at four points, where S is a conic and the curve C has $\mathbb{Q}_v$-points for every place v [31, §1.3]. Since S satisfies the Hasse principle and has points everywhere locally, we have $S \simeq \mathbb{P}^1_{\mathbb{Q}}$ and the curve C is defined by $z^2 = f(x,y)$ where $f \in \mathbb{Q}[x,y]$ is a binary quartic form. This induces a well-defined injection from* $\mathrm{Sel}_2 E$ *to the set of* $\mathrm{PGL}_2(\mathbb{Q})$*-orbits of binary quartic forms [16, Theorem 3.5].*

Example 1.1.1 goes back to Birch and Swinnerton-Dyer [19] and has been used by Bhargava and Shankar to compute the average size of the 2-Selmer group of elliptic curves [16]. See [13] for an exhaustive list of orbit parametrisations of genus-1 curves which are obtained using similar (but more difficult) algebro-geometric constructions. See also [9] for an orbit parametrisation of 2-Selmer groups of odd hyperelliptic curves using the geometry of pencils of quadrics [88]. Even though these considerations have been hugely successful, Wei Ho writes that 'Finding appropriate groups G and vector spaces V related to the Selmer elements is still a relatively ad hoc process' [41].

Gross [38] observed that most coregular representation employed in arithmetic statistics arise from *Vinberg theory*, that is the theory of graded Lie algebras. This suggests the possibility to take Vinberg theory as a starting point, and to attempt to naturally construct families of curves in this setting. This is exactly the perspective taken in Thorne's PhD thesis [83] in the case of 2-Selmer groups. Given a simply laced Dynkin diagram of type A, D, E, he *canonically* constructs a family of curves and a coregular representation whose rational orbits should be related to the arithmetic of the curves in the family. This construction unifies many orbit parametrisations in the literature and has already produced new results in arithmetic statistics; see [84, 71, 86]. However, to obtain all the expected consequences in arithmetic statistics, it remained to be shown that all elements of the 2-Selmer group give rise to rational orbits [83, Conjecture 4.16] and that such rational orbits admit integral representatives.

The main goal of this thesis is to resolve both these questions, and to do so in a uniform manner for all the ADE-families considered. By using geometry-of-numbers techniques developed by Bhargava and his collaborators, we obtain an upper bound on the average size of the 2-Selmer group of the Jacobians of the smooth curves in each family. This has consequences for the ranks of the Jacobians and the rational points of the curves in these families.

Type	Equation	m
A_{2g}	$y^2 = x^{2g+1} + p_2 x^{2g-1} + \cdots + p_{2g+1}$	1
A_{2g+1}	$y^2 = x^{2g+2} + p_2 x^{2g} + \cdots + p_{2g+2}$	2
$D_{2g+2}\,(g \geq 1)$	$y(xy + p_{2g+2}) = x^{2g+1} + p_2 x^{2g} + p_4 x^{2g-1} + \cdots + p_{4g+2}$	3
$D_{2g+1}\,(g \geq 2)$	$y(xy + p_{2g+1}) = x^{2g} + p_2 x^{2g-1} + p_4 x^{2g-2} + \cdots + p_{4g+2}$	2
E_6	$y^3 = x^4 + (p_2 x^2 + p_5 x + p_8)y + (p_6 x^2 + p_9 x + p_{12})$	1
E_7	$y^3 = x^3 y + p_{10} x^2 + x(p_2 y^2 + p_8 y^2 + p_{14}) + p_6 y^2 + p_{12} y + p_{18}$	2
E_8	$y^3 = x^5 + (p_2 x^3 + p_8 x^2 + p_{14} x + p_{20})y + (p_{12} x^3 + p_{18} x^2 + p_{24} x + p_{30})$	1

Table 1.1 Families of curves

1.2 Statement of results

Let D be a Dynkin diagram of type A_n, D_n or E_n and let $C \to B$ be the family of projective curves over $\mathbb{Q}$ with affine equation given by Table 1.1. For example, if $\mathsf{D} = A_{2g}$, then $B = \operatorname{Spec}\mathbb{Q}[p_2, \ldots, p_{2g+1}]$ and $C \to B$ is the family of all monic odd hyperelliptic curves of genus g. If $\mathsf{D} = E_7$, then $C \to B$ is the family of all plane quartic curves with a marked rational flex point. The family $C \to B$ is a semi-universal deformation of its central fibre (by setting all coefficients p_i equal to zero), which is a simple singularity of type D. (See Proposition 3.7.1.) We exclude the case $\mathsf{D} = A_1$.

Write $B^{\mathrm{rs}} \subset B$ for the locus above which $C \to B$ is smooth, the complement of a discriminant hypersurface. For every field $k/\mathbb{Q}$ and $b \in B^{\mathrm{rs}}(k)$, write J_b for the Jacobian of the smooth projective curve C_b, an abelian variety over k of dimension equal to the genus of C_b. Our first main theorem is an orbit parametrisation for elements of $J_b(k)/2J_b(k)$.

To each diagram D one may canonically associate a representation V of a reductive group $G/\mathbb{Q}$. This construction, due to Thorne [83], is recalled in §3.1 and is based on Vinberg's theory of graded Lie algebras. See §3.2 for an explicit description of G and V, although we will almost never use this description. The geometric quotient $V /\!\!/ G = \operatorname{Spec}\mathbb{Q}[V]^G$ (parametrising G-invariant polynomials of V) turns out to be isomorphic to B. For every field $k/\mathbb{Q}$ and $b \in B(k)$, write V_b for the subset of elements of V which map to b under the map $V \to V /\!\!/ G \simeq B$.

Theorem 1.2.1 (Theorem 6.3.2)**.** *For every field $k/\mathbb{Q}$ and element $b \in B^{\mathrm{rs}}(k)$, there exists an injection $\eta_b \colon J_b(k)/2J_b(k) \hookrightarrow G(k)\backslash V_b(k)$ compatible with base change.*

See Theorem 6.3.2 for a more precise formulation and an explicit construction of this injection. Using a local-global principle for G, one can also embed the 2-Selmer group of J_b inside the $G(\mathbb{Q})$-orbits of $V(\mathbb{Q})$. Recall that the 2-Selmer group of an abelian variety $A/\mathbb{Q}$ is a finite dimensional $\mathbb{F}_2$-vector space $\operatorname{Sel}_2 A$ defined by local conditions and fitting inside an exact sequence

$$0 \to A(\mathbb{Q})/2A(\mathbb{Q}) \to \mathrm{Sel}_2 A \to \text{Ш}(A/\mathbb{Q})[2] \to 0.$$

Theorem 1.2.2 (Corollary 6.4.2)**.** *For every $b \in B^{\mathrm{rs}}(\mathbb{Q})$, the injection η_b extends to an injection* $\mathrm{Sel}_2 J_b \hookrightarrow G(\mathbb{Q})\backslash V_b(\mathbb{Q})$.

If D is of type A_2, $C \to B$ is the family of elliptic curves in short Weierstrass form and we essentially recover the injection of Example 1.1.1. If D is of type A_{2g}, we recover the orbit parametrisation of Bhargava and Gross [9].

Crucially, we additionally show that the $G(\mathbb{Q})$-orbits corresponding to $\mathrm{Sel}_2 J_b$ using Theorem 1.2.2 have integral representatives away from small primes, see Corollary 7.6.1. Using geometry-of-numbers techniques to count integral orbits of V, Theorem 1.2.2 may thus be used to give an upper bound on the average size of the 2-Selmer group of $\mathrm{Sel}_2 J_b$. Using the identification $B = \mathrm{Spec}\,\mathbb{Q}[p_{d_1}, \dots, p_{d_r}]$ from Table 1.1, let $\mathscr{F}$ be the subset of elements $b = (p_{d_1}(b), \dots, p_{d_r}(b)) \in \mathbb{Z}^r$ with $b \in B^{\mathrm{rs}}(\mathbb{Q})$. We define the height of $b \in \mathscr{F}$ by the formula

$$\mathrm{ht}(b) \coloneqq \max\left(|p_{d_1}(b)|^{1/d_1}, \dots, |p_{d_r}(b)|^{1/d_r}\right).$$

Note that for any $X \in \mathbb{R}_{>0}$, the set $\{b \in \mathscr{F} \mid \mathrm{ht}(b) < X\}$ is finite. To state the next theorem, note that each curve C_b has points at infinity not lying in the affine patch of Table 1.1, and we call those points the *marked points*. Their cardinality m is displayed in Table 1.1.

Theorem 1.2.3 (Theorem 9.1.1)**.** *Then when ordered by height, the average size of the* 2*-Selmer group of J_b for $b \in \mathscr{F}$ is bounded above by* $3 \cdot 2^{m-1}$. *More precisely, we have*

$$\limsup_{X \to +\infty} \frac{\sum_{b \in \mathscr{F},\, \mathrm{ht}(b) < X} \#\mathrm{Sel}_2 J_b}{\#\{b \in \mathscr{F} \mid \mathrm{ht}(b) < X\}} \leq 3 \cdot 2^{m-1}.$$

The same result holds true even if we impose finitely many congruence conditions on $\mathscr{F}$. Assuming a certain plausible uniformity estimate, we show that the limit exists and the bound $3 \cdot 2^{m-1}$ is sharp, see §9.2 and the discussion at the end of §1.4. See §1.3 for a comparison of this theorem with previously obtained results.

Bhargava and Shankar observed that bounding the 2-Selmer group gives an upper bound on the average rank of elliptic curves. In our case we can bound the average of the Mordell–Weil rank $\mathrm{rk}(J_b)$ of J_b, the rank of the finitely generated abelian group $J_b(\mathbb{Q})$. Using the inequalities $2\,\mathrm{rk}(J_b) \leq 2^{\mathrm{rk}(J_b)} \leq \#\mathrm{Sel}_2 J_b$, we obtain:

Corollary 1.2.4. *Let m be the number of marked points of the family $C \to B$. Then when ordered by height, the average rank* $\mathrm{rk}(J_b)$ *where $b \in \mathscr{F}$ is bounded above by* $3 \cdot 2^{m-2}$.

Theorem 1.2.3 has a number of interesting consequences for the rational points of C_b, typically using various forms of the Chabauty–Coleman method. See for example [9, Corollary 1.4] and [65] for such results in the case $\mathsf{D} = A_{2g}$, and [48, Corollary 1.3 & Theorem 1.4] in the case $\mathsf{D} = E_6$. Theorem 1.2.3 should give similar such consequences for other D.

1.3 Relation to other works

Theorem 1.2.3 has been previously obtained for many D:

- A_2: Bhargava–Shankar [16], who even prove that the average exists and is exactly 3.
- A_{2g}: Bhargava–Gross [9].
- A_{2g+1}, $g \geq 2$: Shankar–Wang [75].
- D_{2g+1}, $g \geq 2$: Shankar [76].
- A_3, D_4: Bhargava–Ho [12, Theorem 1.1(c),(g)].
- E_6: Laga [48].

All these works combine geometry-of-numbers techniques with the orbit parametrisation of Theorem 1.2.2 to obtain Theorem 1.2.3 in their specific case, just as we do here. However, their construction of orbits (in other words, the proof of Theorem 1.2.2) and analysis of the representation (G,V) requires specific arguments in each case. One of the main points of this thesis is that we are able to prove Theorem 1.2.3 in a uniform way. Inspecting the above list, we see that the only cases not previously considered in the literature are $\mathsf{D} = D_{2g+2}$ with $g \geq 2$, E_7 and E_8.

We describe what is new in this thesis compared with Thorne's work. He has shown the analogue of Theorem 1.2.1 for the subset of $J_b(k)/2J_b(k)$ lying in the image of the Abel–Jacobi map $C_b(k) \to J_b(k)/2J_b(k)$ with respect to a fixed marked point [83, Theorem 4.15]. This allowed him to deduce arithmetic statistical results on the 2-*Selmer set* of the curve C_b (a pointed subset of $\mathrm{Sel}_2 J_b$) and the integral points of the affine curve C_b°, see [84, 71]. The first main innovation of this work is the construction of orbits associated to *all* elements of $J_b(k)/2J_b(k)$, as was conjectured in [83, Conjecture 4.16]. The second main innovation is an integral study of the representations (G,V). In particular, we show that orbits arising from Theorem 1.2.2 admit integral representatives away from small primes (Theorem 7.2.4). This technical result is essential for applying orbit-counting methods and allows us to obtain new results on the arithmetic of the curves C_b.

We briefly mention the relation to our previous work [48], which treats the case $\mathsf{D} = E_6$. The construction of orbits there relies on the isomorphism $G_{sc} \simeq \mathrm{Sp}_8$ (where G_{sc} is the simply connected cover of G) and the triviality of the Galois cohomology set $\mathrm{H}^1(k, \mathrm{Sp}_8)$ for every field k. However, this triviality fails to hold for general simply connected groups (for example, Spin groups), so the same argument does not work for all D. Indeed, the proof of Theorem 1.2.1 explained in §1.4 is completely different from the one given in [48].

1.4 Method of proof

We briefly describe the proof of Theorem 1.2.1, which is the first main novelty of this thesis. Thorne has shown that the stabiliser $Z_G(v)$ of an arbitrary element $v \in V_b(k)$ is canonically isomorphic to $J_b[2]$, the 2-torsion subgroup of the Jacobian of C_b. In fact, there always exists a distinguished orbit $\kappa_b \in G(k)\backslash V_b(k)$ and a well-known lemma in arithmetic invariant theory (Lemma 2.4.2) shows that by twisting κ_b the set $G(k)\backslash V_b(k)$ can be identified with the pointed kernel of the map on Galois cohomology $\mathrm{H}^1(k, Z_G(\kappa_b)) \to \mathrm{H}^1(k, G)$.

To prove Theorem 1.2.1, it therefore suffices to prove that the composition

$$J_b(k)/2J_b(k) \xrightarrow{\delta} \mathrm{H}^1(k, J_b[2]) \simeq \mathrm{H}^1(k, Z_G(\kappa_b)) \to \mathrm{H}^1(k, G), \tag{1.4.1}$$

where δ is the 2-descent map of J_b, is trivial. We solve this problem by considering it universally. More precisely, a 'categorified' version of (1.4.1) associates to every element $P \in J_b(k)$ a G-torsor $T_P \to \operatorname{Spec} k$ such that its isomorphism class $[T_P] \in \mathrm{H}^1(k, G)$ equals the image of P under (1.4.1). This process can be carried out in a relative setting: let J^{rs} be the relative Jacobian of the family of smooth curves $C|_{B^{\mathrm{rs}}} \to B^{\mathrm{rs}}$. Then we may construct a G-torsor $T \to J^{\mathrm{rs}}$ whose pullback along a point $P\colon \operatorname{Spec} k \to J^{\mathrm{rs}}$ is isomorphic to T_P. The crucial observation is that the geometry of the total space J^{rs} is very simple, despite the fibres of $J^{\mathrm{rs}} \to B^{\mathrm{rs}}$ being abelian varieties so arguably not so simple. For example, J^{rs} is a rational variety. This fact (or rather a similar, more precise statement), together with an analysis of G-torsors on affine spaces and progress on the Grothendieck–Serre conjecture on principal bundles, allows us to prove J^{rs} admits a Zariski open cover above which T is trivial. This implies that each T_P is trivial, proving the theorem.

To analyse the geometry of J^{rs}, we introduce a compactification of J^{rs} over the whole of B: there exists a projective scheme $\bar{J} \to B$ restricting to J^{rs} over B^{rs} called the *compactified Jacobian* of $C \to B$. The scheme $\bar{J}$ parametrises rank-1 torsion-free sheaves following Altman–Kleiman [1], with the caveat that in the reducible fibres of $C \to B$ we have to impose a stability condition in the sense of Esteves [36] to obtain a well-behaved moduli problem.

The main selling point of this thesis can be summarised as follows: geometric properties of $\bar{J}$ are very useful in the construction of orbits associated to elements of J^{rs}. For example, we show that even though the fibres of $\bar{J} \to B$ might be highly singular, $\bar{J}$ is a smooth and geometrically integral variety. Moreover, the Białynicki-Birula decomposition from geometric representation theory shows that $\bar{J}$ has a decomposition into affine cells, so has a very transparent geometry. The consequences for the geometry of J^{rs} are strong enough to carry out the strategy of the previous paragraph and consequently prove Theorem 1.2.1.

The second main innovation of this thesis is a uniform construction of integral representatives, and we again exploit the geometry of the compactified Jacobian. Constructing integral orbits has often been a subtle point in the past. We achieve this by deforming to the case of square-free discriminant and using a general result on extending reductive group schemes over open dense subschemes of regular arithmetic surfaces (Lemma 7.3.6). We are able to deform to this case using Bertini theorems over $\mathbb{Q}_p$ and $\mathbb{F}_p$ and the smoothness of $\bar{J}$. This smoothness is essential and follows from the fact that $C \to B$ is a semi-universal deformation of its central fibre. We expect that our methods will have applications to the construction of integral representatives in settings different to the one considered here.

We say a few words about counting integral orbits of V. The geometry-of-numbers methods developed by Bhargava and his collaborators are fairly robust, so this part of the argument is rather formal and requires little new input. We make two remarks. First of all, because we cannot prove a uniformity estimate like [16, Theorem 2.13], we only obtain an upper bound in our estimates on integral orbits. We expect that similar uniformity estimates hold in our case (see Conjecture 8.9.3), which implies using the so-called square-free sieve that the average size of the 2-Selmer group of J_b is in fact equal to $3 \cdot 2^{m-1}$, see Proposition 8.9.4. Secondly, for every pair (G, V) one needs to control orbits lying in the cuspidal region of the fundamental domain; this is called 'cutting off the cusp'. For every diagram D, this relies on combinatorial calculations in the associated root system, and they have appeared in the literature except in case D_{2g+2}. We handle this case explicitly with the same methods in an appendix chapter. This is the only part of the thesis where we rely on the previous works listed at the beginning of §1.3. It would be very interesting to find a less computational or even uniform proof for these calculations. This remark extends to other representations employed in arithmetic statistics, for example the ones used in [14, 15]. See [15, Table 2] for an example of the intricacies involved.

1.5 Other coregular representations

There are at least two ways in which coregular representations can arise from Vinberg theory that are not treated in this thesis. In both cases, we expect that our methods go a long way towards proving analogous results to Theorem 1.2.3.

Firstly, one may try to incorporate gradings on nonsimply laced Lie algebras (so of type B, C, F, G) into the picture. Again there will be families of curves, but the relevant Selmer groups may arise from a general isogeny, not just multiplication by an integer. Such gradings have already appeared in the literature, implicitly and explicitly: a $\mathbb{Z}/2\mathbb{Z}$-grading on G_2 has been used to study 2-Selmer groups of elliptic curves with a marked 3-torsion point [12, Theorem 1.1(f)]; a $\mathbb{Z}/3\mathbb{Z}$-grading on G_2 has been used to study 3-isogeny Selmer groups of the curves $y^2 = x^3 + k$ [8]; a $\mathbb{Z}/2\mathbb{Z}$-grading on F_4 has been used to study 2-Selmer groups of a family of Prym surfaces [47].

Secondly, although their occurrence is more sporadic, there are also interesting $\mathbb{Z}/m\mathbb{Z}$-gradings on simple Lie algebras for $m \geq 3$; see for example [72], where the authors calculate the average size of the 3-Selmer group of the family of odd genus-2 curves using a $\mathbb{Z}/3\mathbb{Z}$-grading on E_8.

We mention that there are also coregular representations used in arithmetic statistics that do not arise from Vinberg theory. The most important example is the representation $\mathrm{Sym}^2(n) \oplus \mathrm{Sym}^2(n)$ of SL_n, which is used in [11] to show that a positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ of fixed genus have no points over any odd degree extension. One feature that distinguishes this setting from ours is that their representation lacks a 'Kostant section', which is related to the fact that the curves they study do not come with specified marked points. We wonder if one can still interpret this representation in terms of Lie theory and study its arithmetic from this perspective.

1.6 Organisation

We now summarise the chapters of this thesis. In §2 we recall some background results in Vinberg theory and arithmetic invariant theory. In §3 we recall the constructions and main results of Thorne's thesis and introduce the Vinberg representation (G, V) and family of curves $C \to B$. In §4, we extend the results of Thorne's thesis from the smooth fibres of $C \to B$ to those fibres admitting at most one singular nodal point. In §5, we introduce and study compactified Jacobians of the family $C \to B$. In §6 we analyse torsors on affine spaces and use this and our results from the previous chapters to prove Theorems 1.2.1 and 1.2.2 on the construction of orbits. In §7 we prove that such orbits admit integral representatives away from small primes. In §8, we employ Bhargava's orbit-counting techniques and count integral orbits of the representation (G,V). We combine all the results from the previous chapters in §9 to obtain Theorem 1.2.3. In an appendix chapter, we perform some combinatorial calculations in the root system of type D_{2n} to complete the proof of Proposition 8.7.2 (cutting off the cusp) in this case. We note that the main novel contributions of this thesis lie in Chapters 4, 5, 6 and 7.

1.7 Notation

General

For a field k we write k^s for a fixed separable closure and $\Gamma_k = \mathrm{Gal}(k^s/k)$ for its absolute Galois group.

If X is a scheme over S and $T \to S$ a morphism we write X_T for the base change of X to T. If $T = \operatorname{Spec} A$ is an affine scheme we also write X_A for X_T.

If G is a smooth group scheme over S then we write $\mathrm{H}^1(S,G)$ for the set of isomorphism classes of étale sheaf torsors under G over S, which is a pointed set coming from nonabelian Čech cohomology. If $S = \operatorname{Spec} R$ we write $\mathrm{H}^1(R,G)$ for the same object. If k is a field then $\mathrm{H}^1(k,G)$ coincides with the first nonabelian Galois cohomology set of $G(k^s)$.

If $G \to S$ is a group scheme acting on $X \to S$ and $x \in X(T)$ is a T-valued point, we write $Z_G(x) \to T$ for the centraliser of x in G. It is defined by the following pullback square:

$$\begin{tikzcd} Z_G(x) \arrow[r] \arrow[d] & T \arrow[d] \\ G \times_S X \arrow[r] & X \times_S X \end{tikzcd}$$

Here $G \times_S X \to X \times_S X$ denotes the map $(g,x) \mapsto (g \cdot x, x)$ and $T \to X \times_S X$ denotes the composition of x with the diagonal $X \to X \times_S X$.

If V is a vector space over a field k we write $k[V]$ for the graded algebra $\mathrm{Sym}(V^\vee)$. Then V is naturally identified with the k-points of the scheme $\operatorname{Spec} k[V]$, and we call this latter scheme V as well. If G is a group scheme over k acting on V we write $V /\!\!/ G := \operatorname{Spec} k[V]^G$ for the *GIT quotient* of V by G.

Root lattices

We define a *lattice* to be a finitely generated free $\mathbb{Z}$-module Λ together with a symmetric and positive-definite bilinear form $(\cdot,\cdot)\colon \Lambda \times \Lambda \to \mathbb{Z}$. We write $\Lambda^\vee := \{\lambda \in \Lambda \otimes \mathbb{Q} \mid (\lambda, \Lambda) \subset \mathbb{Z}\}$

for the *dual lattice* of Λ, which is naturally identified with $\mathrm{Hom}(\Lambda, \mathbb{Z})$. We say Λ is a *root lattice* if (λ, λ) is an even integer for all $\lambda \in \Lambda$ and the set

$$\{\alpha \in \Lambda \mid (\alpha, \alpha) = 2\}$$

generates Λ. If $\Phi \subset \mathbb{R}^n$ is a simply laced root system then $\Lambda = \mathbb{Z}\Phi$ is a root lattice. In that case we define the type of Λ to be the Dynkin type of Φ.

If S is a scheme, an *étale sheaf of root lattices* Λ over S is defined as a locally constant étale sheaf of finite free $\mathbb{Z}$-modules together with a bilinear pairing $\Lambda \times \Lambda \to \mathbb{Z}$ (where $\mathbb{Z}$ denotes the constant étale sheaf on S) such that for every geometric point $\bar{s}$ of S the stalk $\Lambda_{\bar{s}}$ is a root lattice. In that case $\mathrm{Aut}(\Lambda)$ is a finite étale S-group.

Reductive groups and Lie algebras

A reductive group scheme over S is a smooth S-affine group scheme $G \to S$ whose geometric fibres are connected reductive groups. See [78] for the basics of reductive groups over a field and [30] for reductive group schemes over a general base. A reductive group is assumed to be connected.

If $G, H, \ldots$ are algebraic groups then we will use gothic letters $\mathfrak{g}, \mathfrak{h}, \ldots$ to denote their Lie algebras. If G is a reductive group with split maximal torus $T \subset G$, we shall write $\Phi_{\mathfrak{t}} \subset X^*(T)$ for the set of roots of T in $\mathfrak{g}$, and $\Phi_{\mathfrak{t}}^{\vee} \subset X_*(T)$ for its set of coroots. The map $\alpha \in \Phi_{\mathfrak{t}} \mapsto d\alpha \in \mathrm{Hom}(\mathfrak{t}, k)$ identifies $\Phi_{\mathfrak{t}}$ with the set of roots of $\mathfrak{t}$ in $\mathfrak{g}$, and we will use this identification without further comment.

If x is an element of a Lie algebra $\mathfrak{g}$ then we write $\mathfrak{z}_{\mathfrak{g}}(x)$ for the centraliser of x in $\mathfrak{g}$, a subalgebra of $\mathfrak{g}$. We note that if G is an algebraic group over a field k and $x \in \mathfrak{g}$ any element, then the inclusion $\mathrm{Lie}\, Z_G(x) \subset \mathfrak{z}_{\mathfrak{g}}(x)$ is an equality if the characteristic of k is zero or if x is semisimple [42, Proposition 1.10].

Chapter 2

Background

2.1 The adjoint quotient of a Lie algebra

To motivate the results in Vinberg theory, we first recall some classical results in the invariant theory of Lie algebras.

Let H be a connected reductive group over a field k of characteristic zero with Lie algebra $\mathfrak{h}$. The group H acts on $\mathfrak{h}$ via the adjoint representation. Let $p\colon \mathfrak{h} \to \mathfrak{h} /\!\!/ H = \operatorname{Spec} k[\mathfrak{h}]^H$ be the so-called *adjoint quotient* induced by the inclusion $k[\mathfrak{h}]^H \subset k[\mathfrak{h}]$. We interpret $\mathfrak{h} /\!\!/ H$ as the space of invariants of the H-action on $\mathfrak{h}$ and p as the morphism of taking invariants. Recall that an element $x \in \mathfrak{h}$ is said to be *regular* if $\dim \mathfrak{z}_{\mathfrak{h}}(x)$ is minimal among elements of $\mathfrak{h}$; this minimal value equals the rank of H. The subset of regular elements defines an open subscheme $\mathfrak{h}^{reg} \subset \mathfrak{h}$. The following classical proposition summarises the invariant theory of $\mathfrak{h}$.

Proposition 2.1.1.

- *Every semisimple element of $\mathfrak{h}$ is contained in a Cartan subalgebra, and if k is algebraically closed every two Cartan subalgebras are $H(k)$-conjugate.*
- *Let $\mathfrak{c} \subset \mathfrak{h}$ be a Cartan subalgebra and let $W = N_H(\mathfrak{c})/Z_H(\mathfrak{c})$. Then the inclusion $\mathfrak{c} \subset \mathfrak{h}$ induces an isomorphism (the Chevalley isomorphism)*

$$\mathfrak{c} /\!\!/ W \simeq \mathfrak{h} /\!\!/ H.$$

  Since W is a finite reflection group, this quotient is isomorphic to affine space.
- *If k is algebraically closed and $b \in (\mathfrak{h} /\!\!/ H)(k)$, the fibre $p^{-1}(b)$ contains a unique open $H(k)$-orbit (consisting of the regular elements with invariants b) and a unique closed $H(k)$-orbit (consisting of the semisimple elements with invariants b).*

We will often use induction arguments to reduce a statement for $\mathfrak{h}$ to a reductive Lie algebra of smaller rank. To this end, the following lemma will be helpful. We suppose for this lemma that H is split and $T \subset H$ is a split maximal torus. This determines a root datum $(X^*(T), \Phi_{\mathfrak{t}}, X_*(T), \Phi_{\mathfrak{t}}^{\vee})$ (in the sense of [78, §7.4]) and a Weyl group $W = N_G(T)/T$.

Lemma 2.1.2. *Let $x \in \mathfrak{t}$ be a semisimple element. Then the centraliser $Z_H(x)$ is a (connected) reductive group. Moreover, let*

$$\Phi_{\mathfrak{t}}(x) = \{\alpha \in \Phi_{\mathfrak{t}} \mid \alpha(x) = 0\} \quad \textit{and} \quad \Phi_{\mathfrak{t}}^{\vee}(x) = \{\alpha^{\vee} \in \Phi_{\mathfrak{t}}^{\vee} \mid \alpha \in \Phi_{\mathfrak{t}}(x)\}.$$

Let $W_x = Z_W(x)$. Then the root datum of $Z_H(x)$ is $(X^*(T), \Phi_{\mathfrak{t}}(x), X_*(T), \Phi_{\mathfrak{t}}^{\vee}(x))$, and the Weyl group of $Z_H(x)$ with respect to T is isomorphic to W_x.

Proof. The centraliser $Z_H(x)$ is connected by [81, Theorem 3.14]. The fact that it is reductive and has the above root datum follows from [81, Lemma 3.7]. The claim about the Weyl group of $Z_H(x)$ follows from [81, Lemma 3.7(c)], again using the fact that $Z_H(x)$ is connected. □

Let $\mathfrak{c} \subset \mathfrak{h}$ a Cartan subalgebra. The *discriminant polynomial* $\Delta \in k[\mathfrak{h}]^H$ is the image of the product of all the roots $\prod \alpha \in k[\mathfrak{c}]^W$ with respect to $\mathfrak{c}$ under the Chevalley isomorphism $k[\mathfrak{c}]^W \xrightarrow{\sim} k[\mathfrak{h}]^H$; it is independent of the choice of $\mathfrak{c}$. For $x \in \mathfrak{h}$ we have $\Delta(x) \neq 0$ if and only if x is regular semisimple. The *discriminant locus* (or discriminant divisor) $D \subset \mathfrak{h} /\!\!/ H$ is the zero locus of Δ. This subscheme will play a fundamental role later in this thesis (in particular in Chapter 4).

The next lemma says that the étale local structure of $\mathfrak{h} /\!\!/ H$ and D near a point is determined by the centraliser of a semisimple lift of that point.

Lemma 2.1.3. *Let $x \in \mathfrak{h}$ be a semisimple element with centraliser $\mathfrak{z}_{\mathfrak{h}}(x)$. Let $\mathfrak{c} \subset \mathfrak{h}$ be a Cartan subalgebra containing x. Let W and W_x be the respective Weyl groups of $\mathfrak{h}$ and $\mathfrak{z}_{\mathfrak{h}}(x)$ with respect to $\mathfrak{c}$. Consider the diagram:*

$$\begin{tikzcd} \mathfrak{c} \arrow[d, "\phi_x"'] \arrow[dr, "\phi"] & \\ \mathfrak{c} /\!\!/ W_x \arrow[r, "\psi"] & \mathfrak{c} /\!\!/ W \end{tikzcd}$$

Then ψ is étale at $\phi_x(x)$. Moreover, if D and D_x denote the discriminant divisors of $\mathfrak{h}$ and $\mathfrak{z}_{\mathfrak{h}}(x)$ respectively, then $\psi^*D = D_x + R$, where R is a divisor of $\mathfrak{c} /\!\!/ W_x$ not containing $\phi_x(x)$ in its support.

Proof. We may assume that k is algebraically closed and that $\mathfrak{h}$ is split. Since ϕ and ϕ_x are finite and faithfully flat (they are even Galois with Galois group W and W_x), the map ψ

is finite and faithfully flat. The fact that ψ is étale at $\phi_x(x)$ follows from the fact that the stabiliser of the W-action on x is precisely W_x (Lemma 2.1.2).

To prove the claim about the discriminant divisors, let $\Delta = \prod_{\alpha\in\Phi_{\mathfrak{c}}} \alpha \in k[\mathfrak{c}]^W$ and $\Delta_x = \prod_{\alpha\in\Phi_{\mathfrak{c}}(x)} \alpha \in k[\mathfrak{c}]^{W_x}$ denote the respective discriminant polynomials. By definition of $\Phi_{\mathfrak{c}}(x)$, $\Delta = \Delta_x \cdot \mathscr{R}$ as elements of $k[\mathfrak{c}]^{W_x}$, where $\mathscr{R} \in k[\mathfrak{c}]^{W_x}$ is a polynomial that does not vanish at x. Since D and D_x are the zero loci of Δ and Δ_x respectively, this proves the claim. □

2.2 Vinberg theory

We keep the notations from §2.1. Let $m \geq 1$ be an integer. A *$\mathbb{Z}/m\mathbb{Z}$-grading* on $\mathfrak{h}$ is, by definition, a direct sum decomposition

$$\mathfrak{h} = \bigoplus_{i\in\mathbb{Z}/m\mathbb{Z}} \mathfrak{h}(i)$$

into linear subspaces satisfying $[\mathfrak{h}(i), \mathfrak{h}(j)] \subset \mathfrak{h}(i+j)$. Given a $\mathbb{Z}/m\mathbb{Z}$-grading on $\mathfrak{h}$, let $\mathfrak{g} = \mathfrak{h}(0)$ and $V = \mathfrak{h}(1)$. Then $\mathfrak{g}$ is a subalgebra of $\mathfrak{h}$ and the restriction of the adjoint representation induces an action of $\mathfrak{g}$ on V. If $\zeta \in k$ is a primitive m-th root of unity, giving a $\mathbb{Z}/m\mathbb{Z}$-grading amounts to giving, by considering ζ^i-eigenspaces, an automorphism θ of $\mathfrak{h}$ of order dividing m. In general when no such ζ exists or is fixed, giving a $\mathbb{Z}/m\mathbb{Z}$-grading amounts to giving a homomorphism $\mu_m \to \mathrm{Aut}(\mathfrak{h})$ of group schemes over k.

Let $\mu_m \to \mathrm{Aut}(H)$ be a morphism of group schemes. The composition $\mu_m \to \mathrm{Aut}(H) \to \mathrm{Aut}(\mathfrak{h})$ determines a $\mathbb{Z}/m\mathbb{Z}$-grading on $\mathfrak{h}$. If G is the identity component of the centraliser of μ_m in H, then G has Lie algebra $\mathfrak{g}$ and acts on $V = \mathfrak{h}(1)$ by restriction of the adjoint action. The pair (G,V) is called a *Vinberg representation*, and its study is dubbed *Vinberg theory* [87]. If $\mathfrak{h}$ is a semisimple $\mathbb{Z}/m\mathbb{Z}$-graded Lie algebra, a natural choice for H is the adjoint group $\mathrm{Aut}(\mathfrak{h})^\circ$ of $\mathfrak{h}$: this is the unique (up to nonunique isomorphism) connected semisimple group with trivial centre and Lie algebra $\mathfrak{h}$.

We now summarise some of the highlights of Vinberg theory, referring to [60, 51] for proofs. We call an element $x \in V$ semisimple, nilpotent or regular if it is so when considered as an element of $\mathfrak{h}$. We call a subspace $\mathfrak{c} \subset V$ that consists of semisimple elements, that satisfies $[\mathfrak{c}, \mathfrak{c}] = 0$, and is maximal with these properties (among subspaces of V) a *Cartan subspace*.

Lemma 2.2.1. *If $x \in V$ has Jordan decomposition $x = x_s + x_n$ where x_s, x_n are commuting elements that are semisimple and nilpotent respectively, then $x_s, x_n \in V$.*

Proposition 2.2.2. *Every semisimple $x \in V$ is contained in a Cartan subspace of V. Every two Cartan subspaces are $G(k^s)$-conjugate.*

We call a triple (e,h,f) an $\mathfrak{sl}_2$-*triple* of $\mathfrak{h}$ if e,h,f are nonzero elements of $\mathfrak{h}$ satisfying the following relations:

$$[h,e] = 2e, \quad [h,f] = -2f, \quad [e,f] = h.$$

The classical Jacobson–Mozorov lemma states that every nilpotent element in $\mathfrak{h}$ can be completed to an $\mathfrak{sl}_2$-triple. If $\mathfrak{h}$ is $\mathbb{Z}/m\mathbb{Z}$-graded, we say an $\mathfrak{sl}_2$-triple is *normal* if $e \in \mathfrak{h}(1)$, $h \in \mathfrak{h}(0)$ and $f \in \mathfrak{h}(-1)$.

Lemma 2.2.3. *Let $e \in \mathfrak{h}(1)$ be a nilpotent element. Then there exists an $\mathfrak{sl}_2$-triple (e,h,f) with $h \in \mathfrak{h}(0)$ and $f \in \mathfrak{h}(-1)$.*

Proof. See [46, Proposition 4], which only treats the case $m = 2$ but whose proof works for any m. (We will only need the $m = 2$ case in this thesis.) □

The next proposition describes the basic geometric invariant theory of the representation (G,V). Let $\pi\colon V \to V /\!\!/ G = \operatorname{Spec} k[V]^G$ be the graded analogue of the adjoint quotient from §2.1.

Proposition 2.2.4.

- *Let $\mathfrak{c} \subset V$ be a Cartan subspace and $W(\mathfrak{c}) = N_G(\mathfrak{c})/Z_G(\mathfrak{c})$. Then the inclusion $\mathfrak{c} \subset V$ induces an isomorphism*

  $$\mathfrak{c} /\!\!/ W(\mathfrak{c}) \simeq V /\!\!/ G.$$

  The group $W(\mathfrak{c})$ is a finite pseudo-reflection group, so the quotient is isomorphic to affine space.

- *If k is algebraically closed and $b \in (V /\!\!/ G)(k)$, then the fibre $\pi^{-1}(b)$ contains a unique closed $G(k)$-orbit, the set of semisimple elements with invariants b.*

Remark 2.2.5. *In contrast to the $m = 1$ case, it is not true in general that two regular element $x,y \in V(k)$ with the same invariants (that is, with the same image in $V /\!\!/ G$) are $G(k^s)$-conjugate. Indeed, it follows from Proposition 3.5.1 below that the $\mathbb{Z}/2\mathbb{Z}$-gradings introduced in §3.1 can have multiple $G(k^s)$-orbits of regular nilpotent elements.*

2.3 Stable gradings

We keep the notations of §2.1 and §2.2. Of particular interest to us are the stable gradings.

Definition 2.3.1. *Suppose that k is algebraically closed. We say a vector $v \in V$ is* stable *(in the sense of geometric invariant theory) if the G-orbit of v is closed and its stabiliser $Z_G(v)$ is finite. We say (G,V) is* stable *if V contains stable vectors. If k is not necessarily algebraically closed, we say (G,V) is stable if (G_{k^s}, V_{k^s}) is.*

Stable gradings of simple Lie algebras over an algebraically closed field of characteristic zero have been classified [68, §7.1, §7.2] in terms of regular elliptic conjugacy classes of (twisted) Weyl groups. In the case of involutions, this classification takes the simple form of Lemma 2.3.2, see [83, Lemma 2.6] for a proof. We say two involutions $\theta, \theta' \colon H \to H$ are $H(k)$-conjugate if there exists an $h \in H(k)$ such that $\theta' = h\theta h^{-1}$.

Lemma 2.3.2. *Suppose that k is algebraically closed. Then there exists a unique $H(k)$-conjugacy class of stable involutions.*

For example, if H is a torus then the only stable involution is given by the inversion map $h \mapsto h^{-1}$.

One of the main advantages of stable gradings is that they have a particularly good invariant theory. The next proposition describes this more precisely in the case of $\mathbb{Z}/2\mathbb{Z}$-gradings. In particular, it shows that regular semisimple orbits over algebraically closed fields are well understood. We refer to [83, §2] for precise references.

Proposition 2.3.3. *Suppose that $\theta \colon H \to H$ a stable involution, with associated Vinberg representation (G,V). The following properties are satisfied:*

1. *Let $\mathfrak{c} \subset V$ be a Cartan subspace and $W(\mathfrak{c}) = N_G(\mathfrak{c})/Z_G(\mathfrak{c})$. Then $\mathfrak{c}$ is a Cartan subalgebra of $\mathfrak{h}$ and the map $N_G(\mathfrak{c}) \to W_{\mathfrak{c}} := N_H(\mathfrak{c})/Z_H(\mathfrak{c})$ is surjective. Consequently, the inclusions $\mathfrak{c} \subset V \subset \mathfrak{h}$ induce isomorphisms*
$$\mathfrak{c} /\!\!/ W_{\mathfrak{c}} \simeq V /\!\!/ G \simeq \mathfrak{h} /\!\!/ H.$$
In particular, the quotient is isomorphic to affine space.

2. *Suppose that k is algebraically closed and let $x, y \in V(k)$ 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. *Let $\Delta \in \mathbb{Q}[V]^G$ be the restriction of the Lie algebra discriminant of $\mathfrak{h}$ to the subspace V and suppose that k is algebraically closed. Then for all $x \in V(k)$, x is regular semisimple if and only if $\Delta(x) \neq 0$, if and only if x is stable in the sense of Definition 2.3.1.*

2.4 Arithmetic Invariant Theory

Let k be a field with separable closure k^s. Let G/k be a smooth algebraic group acting on a k-vector space V. In general, a fixed $G(k^s)$-orbit in $V(k^s)$ might break up into multiple $G(k)$-orbits, and the study of this phenomenon is referred to as arithmetic invariant theory [10]. We recall its relation to Galois cohomology, which lies at the basis of the orbit parametrisations in this thesis.

Lemma 2.4.1. *Suppose that G acts on a k-scheme X. Suppose that the k-point $e \in X(k)$ has smooth stabiliser $Z_G(e)$ and that the action of $G(k^s)$ on $X(k^s)$ is transitive. Then there is a natural bijection*

$$G(k)\backslash X(k) \overset{1:1}{\longleftrightarrow} \ker(\mathrm{H}^1(k, Z_G(e)) \to \mathrm{H}^1(k, G)).$$

Proof. This is [10, Proposition 1]. The bijection is explicitly constructed as follows: if $x \in X(k)$, transitivity ensures that there exists an element $g \in G(k^s)$ with $x = g \cdot e$. For every element $\sigma \in \Gamma_k = \mathrm{Gal}(k^s/k)$, we again have $x = \sigma(g) \cdot e$, so the map $\sigma \mapsto g^{-1}\sigma(g)$ defines a 1-cocycle with values in $Z_G(e)$ which is trivial in $\mathrm{H}^1(k, G)$. □

In fact, we will need a relative version of Lemma 2.4.1 which is valid over any base scheme.

Lemma 2.4.2. *Let $G \to S$ be a smooth affine group scheme acting on an S-scheme X. Let $e \in X(S)$ be an S-point and suppose that the action map $m\colon G \to X, g \mapsto g \cdot e$ is smooth and surjective. Then the assignment $x \mapsto$ 'isomorphism class of the $Z_G(e)$-torsor $m^{-1}(x)$' induces a bijection between the set of $G(S)$-orbits of $X(S)$ and the kernel of the map of pointed sets $\mathrm{H}^1(S, Z_G(e)) \to \mathrm{H}^1(S, G)$.*

Proof. This is [30, Exercise 2.4.11]: the conditions imply that $X \simeq G/Z_G(e)$ and since G and $Z_G(e)$ (the fibre above e of the smooth map m) are S-smooth we can replace fppf cohomology by étale cohomology. □

2.5 The Grothendieck–Serre conjecture

We discuss some general results concerning principal bundles over reductive group schemes which will be useful in §6. Recall from [30, Definition 3.1.1] that a reductive group scheme over S is a smooth S-affine group scheme $G \to S$ whose geometric fibres are connected reductive groups.

Definition 2.5.1. *Let R be a regular local ring with fraction field K and let $G \to \operatorname{Spec} R$ be a reductive group scheme. We say that the* Grothendieck–Serre conjecture holds for R and G *if the restriction map*

$$\mathrm{H}^1(R,G) \to \mathrm{H}^1(K,G)$$

is injective.

Note that the injectivity $\mathrm{H}^1(R,G) \to \mathrm{H}^1(K,G)$ is stronger than requiring that this map has trivial kernel, since this is merely a map of pointed sets. It is conjectured that the Grothendieck-Serre conjecture holds for every reductive group scheme over every regular local ring; see [59] for a survey and [25, §1.4] for a short summary of known results. Below we will single out the known cases that we will need.

Lemma 2.5.2. *Let X be a regular integral scheme with function field K. Let G be a reductive X-group scheme. Suppose that the Grothendieck-Serre conjecture holds for all local rings of X and G. Then every two G-torsors over X that are generically isomorphic (that is, isomorphic over K) are Zariski locally isomorphic (that is, isomorphic after restricting to a Zariski open cover).*

Proof. Let T, T' be two G-torsors over X which are generically isomorphic and let $x \in X$. We need to prove that x has an open neighbourhood over which T and T' are isomorphic. Since the Grothendieck-Serre conjecture holds for the local ring $\mathscr{O}_{X,x}$, the torsors T and T' are isomorphic when restricted to $\operatorname{Spec} \mathscr{O}_{X,x}$. The result follows from spreading out this isomorphism. □

Proposition 2.5.3. *Let R be a regular local ring and G a reductive R-group. Suppose that at least one of the following is satisfied:*

- *R is a discrete valuation ring;*
- *R contains an infinite field.*

Then the Grothendieck-Serre conjecture holds for R and G.

Proof. The case of a discrete valuation ring was proved by Nisnevich [56], with corrections by Guo [40]. The case where R contains an infinite field was proved by Fedorov and Panin [37]. □

The conjecture is known in many other cases; see [25] for a recent general result when R is of mixed characteristic and [58] for the case where R contains a finite field.

Corollary 2.5.4. *Let X be a regular integral scheme and G a reductive X-group. Suppose that at least one of the following conditions is satisfied:*

- *X is a Dedekind scheme;*
- *X has a map to the spectrum of an infinite field.*

Then every two G-torsors over X that are generically isomorphic are Zariski locally isomorphic.

Proof. Combine Lemma 2.5.2 and Proposition 2.5.3. $\square$

Chapter 3

Around Thorne's thesis

In the remainder of this thesis we will focus on a particular Vinberg representation. Given a Dynkin diagram of type A, D, E, we will canonically construct a stable $\mathbb{Z}/2\mathbb{Z}$-grading on the Lie algebra of the corresponding type following a construction of Thorne's thesis [83, §2]. We then recall and extend some of its basic properties in §3.2–3.6. In §3.7 we introduce the corresponding family of curves $C \to B$ and in §3.8 we recall the relation between stabilisers in V with the 2-torsion in the Jacobians of smooth fibres of $C \to B$. We do not claim any originality in this chapter, except maybe for some of the calculations in §3.9.

3.1 A split stable $\mathbb{Z}/2\mathbb{Z}$-grading

Let H be a split adjoint simple group of type A, D, E over $\mathbb{Q}$ with Dynkin diagram D. We have an exact sequence

$$1 \to H \to \mathrm{Aut}(H) \to \mathrm{Aut}(\mathsf{D}) \to 1. \tag{3.1.1}$$

Assume that H is equipped with a pinning $(T, P, \{X_\alpha\})$. By definition, this means that:

- $T \subset H$ is a split maximal torus (which determines a root system $\Phi_H := \Phi_{\mathfrak{t}}$);
- $P \subset H$ is a Borel subgroup containing T (which determines a root basis $S_H \subset \Phi_H$);
- X_α is a generator for each root space $\mathfrak{h}_\alpha$ for $\alpha \in S_H$.

The subgroup $\mathrm{Aut}((H, T, P, \{X_\alpha\})) \subset \mathrm{Aut}(H)$ of elements preserving the pinning determines a splitting of the sequence (3.1.1).

On the other hand, if $W = N_H(T)/T$ denotes the Weyl group of Φ_H, we have an exact sequence

$$1 \to W \to \mathrm{Aut}(\Phi_H) \to \mathrm{Aut}(\mathsf{D}) \to 1. \tag{3.1.2}$$

We define $\vartheta \in \mathrm{Aut}(H)$ as the unique element of $\mathrm{Aut}((H,T,P,\{X_\alpha\}))$ whose image in $\mathrm{Aut}(\mathsf{D})$ under (3.1.1) coincides with the image of $-1 \in \mathrm{Aut}(\Phi_H)$ in $\mathrm{Aut}(\mathsf{D})$ under (3.1.2). Note that $\vartheta = 1$ if and only if $-1 \in W$.

Write $\check{\rho} \in X_*(T)$ for the sum of the fundamental coweights with respect to S_H, characterised by the property that $(\alpha \circ \check{\rho})(t) = t$ for all $\alpha \in S_H$. Let

$$\theta := \vartheta \circ \mathrm{Ad}(\check{\rho}(-1)) = \mathrm{Ad}(\check{\rho}(-1)) \circ \vartheta.$$

Then θ defines an involution of $\mathfrak{h}$ and thus by considering (± 1)-eigenspaces it determines a $\mathbb{Z}/2\mathbb{Z}$-grading

$$\mathfrak{h} = \mathfrak{h}(0) \oplus \mathfrak{h}(1).$$

Let $G := (H^\theta)^\circ$ be the identity component of the centraliser of θ in H and let $V := \mathfrak{h}(1)$. The space V defines a representation of G by restricting the adjoint representation. If we write $\mathfrak{g}$ for the Lie algebra of G then V is a Lie algebra representation of $\mathfrak{g} = \mathfrak{h}(0)$. The Vinberg representation (G,V) is a central object of study of this thesis. Its relevance can be summarised in the following proposition, proved in [85, Proposition 1.9].

Proposition 3.1.1. *Up to $H(\mathbb{Q})$-conjugacy, θ is the unique involution of H that satisfies the following two properties:*

1. *θ is a stable involution (Definition 2.3.1);*

2. *The reductive group G is split over $\mathbb{Q}$.*

The first property of Proposition 3.1.1 is geometric: it characterises the $H(\bar{\mathbb{Q}})$-conjugacy class of θ. The second property is arithmetic, and it is equivalent to requiring the existence of a regular nilpotent in $V(\mathbb{Q})$. (For the last claim, see [83, Corollary 2.15].) Note that in our construction of θ the element $E = \sum_{\alpha \in S_H} X_\alpha$ is a regular nilpotent in $V(\mathbb{Q})$.

Write $B := V /\!\!/ G = \mathrm{Spec}\, \mathbb{Q}[V]^G$ and $\pi\colon V \to B$ for the natural quotient map. We have a $\mathbb{G}_m$-action on V given by $\lambda \cdot v = \lambda v$ and there is a unique $\mathbb{G}_m$-action on B such that π is $\mathbb{G}_m$-equivariant. The invariant theory of the pair (G,V) is summarised in Proposition 2.3.3. We additionally record the following fact concerning the smooth locus of π.

Lemma 3.1.2. *Let $x \in V$ and let $d\pi_x$ be the induced map on tangent spaces $T_xV \to T_{\pi(x)}B$. Then $d\pi_x$ is surjective if and only if x is regular. Consequently, the smooth locus of π coincides with $V^{reg} := V \cap \mathfrak{h}^{reg}$.*

Proof. This follows from the proof of [83, Proposition 3.10]; we include the argument for completeness. Let $p\colon \mathfrak{h} \to B$ be the invariant map of $\mathfrak{h}$ and let $dp_x\colon T_x\mathfrak{h} \to T_{\pi(x)}B$ the induced map on tangent spaces. Under the canonical isomorphism of vector spaces $T_x\mathfrak{h} \simeq \mathfrak{h}$, we claim that $dp_x(\mathfrak{g}) = 0$. This is true if x is regular. Indeed, we then have $\mathfrak{g} = [x,V] \subset [x,\mathfrak{h}]$ (compare dimensions, see [83, Lemma 2.21]). So $\mathfrak{g}$ is contained in the tangent space to the orbit $H \cdot x$, hence maps to zero under dp_x. Since the regular elements are dense in V, it follows that $dp_x(\mathfrak{g}) = 0$ for all $x \in V$.

Therefore $d\pi_x$ is surjective if and only if dp_x is surjective. The latter is true if and only if x is regular, by a result of Kostant [45, Theorem 9]. This is equivalent to the smoothness of π at x [23, §2.2, Proposition 8]. □

3.2 Explicit determination of (G,V)

Using the results of [67] applied to the Kac diagram of θ [68, §7.1, §7.2], one may calculate the isomorphism class of the split group G and the representation V explicitly. These results are summarised in Table 3.1, where we have used the following notation:

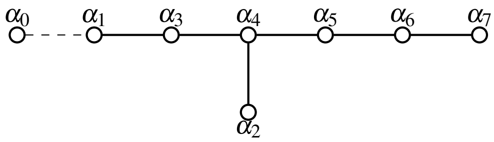
- If G is defined as a subgroup of GL_n, then (n) denotes the representation of G corresponding to this embedding.
- In case D_{2r}, $\Delta(\mu_2)$ denotes the image of μ_2 diagonally embedded in the centre $\mu_2 \times \mu_2$ of $\mathrm{SO}_{2r} \times \mathrm{SO}_{2r}$.
- In case E_6, $\wedge^4_0(8)$ denotes the unique 42-dimensional subrepresentation of the PSp_8-representation $\wedge^4(8)$.
- In case E_8, Spin_{16}/μ_2 denotes a μ_2-quotient of Spin_{16} that is not isomorphic to SO_{16}; it does not seem to have a more succinct name.

We will only need these explicit identifications in the proof of Proposition 8.7.2. Moreover we will calculate the component group of H^θ and the centre of G more uniformly in §3.3 and §3.4.

We treat the E_7 case as an example. The extended Dynkin diagram is given by:

Type	G	V	$\pi_0(H^\theta)$
A_{2r}	SO_{2r+1}.	$\mathrm{Sym}^2(2r+1)$	1
A_{2r+1}	PSO_{2r+2}	$\mathrm{Sym}^2(2r+2)$	$\mathbb{Z}/2\mathbb{Z}$
D_{2r}	$(\mathrm{SO}_{2r}\times \mathrm{SO}_{2r})/\Delta(\mu_2)$	$(2r)\boxtimes(2r)$	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$
D_{2r+1}	$\mathrm{SO}_{2r+1}\times \mathrm{SO}_{2r+1}$	$(2r+1)\boxtimes(2r+1)$	$\mathbb{Z}/2\mathbb{Z}$
E_6	PSp_8	$\wedge^4_0(8)$	1
E_7	SL_8/μ_4	$\wedge^4(8)$	$\mathbb{Z}/2\mathbb{Z}$
E_8	Spin_{16}/μ_2	half spin	1

Table 3.1 Short description of each representation



The normalised Kac coordinates of θ (given in [68, §7.1, Table 4]) are everywhere zero, except at the bottom node α_2, which has coordinate 1. We may now apply the results of [67, §2.4]. Since the Kac coordinates are invariant under the automorphism of the extended diagram, the component group of H^θ is of order 2. Since the highest root has coordinate 2 at α_2, the centre of G is of order 2. If we delete the node α_2, we obtain a diagram of type A_7, so G semisimple is of type A_7. Since G is split, it follows that $G \simeq \mathrm{SL}_8/\mu_4$. Moreover, the representation V has highest weight the fundamental weight corresponding to α_4, so is isomorphic to $\wedge^4(8)$, where (8) denotes the defining representation of SL_8.

3.3 The component group of H^θ

The group H^θ is typically disconnected, and we have a tautological exact sequence

$$1 \to G \to H^\theta \to \pi_0(H^\theta) \to 1.$$

The component group $\pi_0(H^\theta)$ is a finite étale group scheme over $\mathbb{Q}$. We will show that $\pi_0(H^\theta)$ is split and describe it in two different ways, which will be useful in the proof of Proposition 6.5.1.

Firstly, we use Weyl groups. Recall that $W_H = N_H(T)/T$ denotes the Weyl group of H. We know that $T^\theta = T^\vartheta$ is a maximal torus of G, and moreover the centraliser $Z_H(T^\theta)$ of T^θ equals T; these claims can be verified explicitly or follow from [69, Lemmas 5.1 and 5.3]. It follows that $N_H(T^\theta) \subset N_H(T)$, so $W_{H^\theta} := N_{H^\theta}(T^\theta)/T^\theta$ is naturally a subgroup of W_H. Let $W_G := N_G(T^\theta)/T^\theta$ be the Weyl group of G, a normal subgroup of W_{H^θ}. We have inclusions $W_G \subset W_{H^\theta} \subset W_H$.

Lemma 3.3.1. *The inclusion $N_{H^\theta}(T^\theta) \subset H^\theta$ induces an isomorphism $W_{H^\theta}/W_G \simeq \pi_0(H^\theta)$.*

Proof. This is implicit in the proof of [67, Lemma 3.9]; we sketch the details. It suffices to prove that $H^\theta = G \cdot N_{H^\theta}(T^\theta)$. This can be checked on geometric points, so let $k/\mathbb{Q}$ be an algebraically closed field and $h \in H^\theta(k)$. The conjugate subgroup $\mathrm{Ad}(h) \cdot T^\theta$ is a maximal torus of G_k. Since G_k is reductive, $G(k)$ acts transitively on its maximal tori, so $\mathrm{Ad}(h) \cdot T^\theta = \mathrm{Ad}(g) \cdot T^\theta$ for some $g \in G$. We see that $g^{-1}h \in N_{H^\theta}(T^\theta)$, as claimed. □

Corollary 3.3.2. *The finite étale $\mathbb{Q}$-group $\pi_0(H^\theta)$ is constant (in other words, has trivial Galois action) and the map $H^\theta(\mathbb{Q}) \to \pi_0(H^\theta)$ is surjective.*

Proof. It suffices to prove the latter claim. Since T is a maximal torus of H, W_H is a constant group scheme, so its subgroup W_{H^θ} is constant too. By Lemma 3.3.1 it suffices to show that $N_{H^\theta}(T^\theta)(\mathbb{Q}) \to W_{H^\theta}$ is surjective. This follows from Hilbert's theorem 90 since the torus T^θ is $\mathbb{Q}$-split. □

Remark 3.3.3. *If θ is inner, it is possible to describe a complement of W_G in W_{H^θ}, see [67, Remarks after Proposition 2.1]. It seems likely that one can give a similar description in the general case using twisted root systems, but we will not need this in what follows.*

For the second description, choose a Cartan subspace $\mathfrak{c} \subset V$ and let $C \subset H$ be the maximal torus with Lie algebra $\mathfrak{c}$. Since θ acts as -1 on $\mathfrak{c}$ it acts via inversion on C hence $C[2] \subset H^\theta$. The next lemma is [46, Proposition 1]:

Lemma 3.3.4. *We have $H^\theta = G \cdot C[2]$. In other words, the inclusion $C[2] \subset H^\theta$ induces a surjection $C[2] \twoheadrightarrow \pi_0(H^\theta)$.*

Lemma 3.3.4 allows us to give an explicit description of $\pi_0(H^\theta)$.

Corollary 3.3.5. *Let $H_{sc} \to H$ be the simply connected cover of H and let $\pi_1(H)$ denote the centre of H_{sc}. Then there is an isomorphism $\pi_0(H^\theta) \simeq \pi_1(H)/2\pi_1(H)$.*

Proof. Let $C \subset H$ be a maximal torus whose Lie algebra is a Cartan subspace of V. (Such a torus certainly exists: take the centraliser of a regular semisimple element of V.) Let $C_{sc} \subset H_{sc}$ be its preimage in H_{sc}. We have an exact sequence

$$1 \to \pi_1(H) \to C_{sc} \to C \to 1. \tag{3.3.1}$$

Examining the long exact sequence associated to the 2-torsion of (3.3.1) shows that we have an isomorphism

$$\frac{C[2]}{\mathrm{image}(C_{sc}[2] \to C[2])} \simeq \pi_1(H)/2\pi_1(H).$$

We claim that the left-hand-side is isomorphic to $\pi_0(H^\theta)$. Indeed, the involution $\theta\colon H \to H$ uniquely extends to an involution of H_{sc}, still denoted by θ, and a theorem of Steinberg [80, Theorem 8.1] shows that H_{sc}^θ is connected. It follows that the induced map $H_{sc}^\theta \to H^\theta$ surjects onto G. Therefore the kernel of the natural map $C[2] \to \pi_0(H^\theta)$ (which is surjective by Lemma 3.3.4) agrees with the image of the map $C_{sc}[2] \to C[2]$, as claimed. □

3.4 The fundamental group of G

Proposition 3.4.1. *The group G is semisimple and its fundamental group has order* $2\#\pi_0(H^\theta)$.

Proof. Let $H_{sc} \to H$ be the simply connected cover of H and let $\pi_1(H)$ denote the centre of H_{sc}. By a previously invoked theorem of Steinberg [80, Theorem 8.1], H_{sc}^θ is connected. Therefore the induced map on θ-fixed points $H_{sc}^\theta \to G$ is surjective with kernel $\pi_1(H)[2]$. Moreover $\pi_1(H)[2]$ has cardinality $\#\pi_0(H^\theta)$ by Corollary 3.3.5. Hence it suffices to prove that H_{sc}^θ is semisimple and its fundamental group is of order 2. This is a result of Kaletha, see [85, Proposition A.1]. □

3.5 Regular nilpotent elements in V

The next proposition describes the set of regular nilpotent elements in V [83, Lemma 2.14].

Proposition 3.5.1. *For every field $k/\mathbb{Q}$, the group $H^\theta(k)$ acts simply transitively on the set of regular nilpotent elements of $V(k)$.*

Corollary 3.5.2. *Let $k/\mathbb{Q}$ be a field and $E \in V(k)$ a regular nilpotent. (For example, $E = \sum_{\alpha\in S_H} X_\alpha$.) Then the map $h \mapsto h \cdot E$ induces a bijection between $\pi_0(H^\theta)$ and the set of $G(k)$-orbits of regular nilpotent elements in $V(k)$.*

Proof. Follows from Proposition 3.5.1 and the fact that $H^\theta(k) \to \pi_0(H^\theta)$ is surjective (Corollary 3.3.2). □

We see in particular that if H^θ is disconnected then there are multiple G-orbits of regular nilpotent elements in V. To state the next result, recall from §2.2 the notion of a normal $\mathfrak{sl}_2$-triple.

Corollary 3.5.3. *Let $k/\mathbb{Q}$ be a field and $E \in V(k)$ a regular nilpotent element. Then E is contained in a unique normal $\mathfrak{sl}_2$-triple.*

Proof. Proposition 3.5.1 shows that the stabiliser $Z_G(E)$ is trivial. Therefore the corollary follows from [83, Lemma 2.17]. □

3.6 Kostant sections

We describe sections of the GIT quotient $\pi\colon V \to B$ whose remarkable construction is originally due to Kostant. Let $E \in V(\mathbb{Q})$ be a regular nilpotent element and let (E,X,F) be the unique normal $\mathfrak{sl}_2$-triple containing E using Corollary 3.5.3. We define the affine linear subspace $\kappa := \big(E + \mathfrak{z}_{\mathfrak{h}}(F)\big) \cap V \subset V$. We call κ the *Kostant section* associated to E, or simply a Kostant section.

Proposition 3.6.1. *1. The composition $\kappa \hookrightarrow V \to B$ is an isomorphism.*

2. κ is contained in the open subscheme of regular elements of V.

3. The morphism $G \times \kappa \to V, (g,v) \mapsto g \cdot v$ is étale.

Proof. Parts 1 and 2 are [83, Lemma 3.5]; the last part is [83, Proposition 3.4], together with the fact that $G \times \kappa$ and V have the same dimension (apply [83, Lemma 2.21] to $x = 0$). □

Every Kostant section κ determines a morphism $B \to V$ that is a section of the quotient map $\pi\colon V \to B$, and we denote this section by κ too. For any $b \in B(k)$ we write κ_b for the fibre of κ over b.

Definition 3.6.2. *Let $k/\mathbb{Q}$ be a field and $v \in V(k)$. We say v is k-*reducible *if v is not regular semisimple or v is $G(k)$-conjugate to κ_b for some Kostant section κ and where $b = \pi(v)$. Otherwise, we call v k-*irreducible.

3.7 A family of curves

If $k/\mathbb{Q}$ is a field, an element $v \in \mathfrak{h}(k)$ is called *subregular* if $\dim \mathfrak{z}_{\mathfrak{h}}(x) = r+2$, where r is the rank of $\mathfrak{h}$. By [83, Proposition 2.27], the vector space V contains subregular nilpotent elements; let $e \in V(\mathbb{Q})$ be such an element and let (e,x,f) be a normal $\mathfrak{sl}_2$-triple extending it, using Lemma 2.2.3.

Slodowy [77] has shown that the restriction of the invariant map $(e + \mathfrak{z}_{\mathfrak{h}}(f)) \to B$ is a family of surfaces. Moreover, he has shown that this family is a semi-universal deformation of its central fibre, which is a simple surface singularity of the type corresponding to that of H. Proposition 3.7.1 is a $\mathbb{Z}/2\mathbb{Z}$-graded analogue of Slodowy's result, due to Thorne. Define $C^\circ := (e + \mathfrak{z}_{\mathfrak{h}}(f)) \cap V$. Restricting the invariant map $\pi\colon V \to B$ to C° defines a morphism $\varphi\colon C^\circ \to B$.

Proposition 3.7.1. *1. The geometric fibres of φ are reduced connected curves.*

2. *The central fibre $C_0^\circ = \varphi^{-1}(0)$ has a unique singular point which is a simple singularity of type A_r, D_r, E_r, corresponding to that of H.*

3. *We can choose coordinates $p_{d_1}, \dots, p_{d_r}$ on B and $(x, y, p_{d_1}, \dots, p_{d_{r-1}})$ on C° such that $C^\circ \to B$ is given by the affine equation of Table 1.1.*

4. *The formal completion of $C^\circ \to B$ along its central fibre defines a morphism of formal schemes $\widehat{C^\circ} \to \widehat{B}$ which is a semi-universal deformation of its central fibre.*

5. *The morphism φ is faithfully flat. It is smooth at $x \in C^\circ$ if and only if x is a regular element of V.*

6. *The action map $G \times C^\circ \to V, (g, x) \mapsto g \cdot x$ is smooth.*

Proof. This is proved in Thorne's thesis. The first three parts are [83, Theorem 3.8]; for the definition of a simple curve singularity, see [82, End of §2]. The fourth part follows from the fact that the semi-universal deformation of an isolated hypersurface singularity can be explicitly computed [77, §2.4] and agrees with the equations given in Table 1.1. The last two parts are contained in [83, Proposition 3.4 and Proposition 3.10]. □

The next lemma describes the singularities of the fibres of $C^\circ \to B$ very precisely; see [83, Corollary 3.16] for its proof.

Lemma 3.7.2. *Let $k/\mathbb{Q}$ be a field, $b \in B(k)$ and $v \in V_b(k)$ a semisimple element. Then there is a bijection between the connected components of the Dynkin diagram of $Z_H(v)$ and the singularities of C_b°, which takes each (connected, simply laced) Dynkin diagram to a singularity of the corresponding type.*

We compactify the flat affine family of curves $C^\circ \to B$ to a flat projective family of curves $C \to B$ as described in [83, Lemma 4.9]. That lemma implies that the complement $C \setminus C^\circ$ is a disjoint union of sections $\infty_1, \dots, \infty_m \colon B \to C$ and $C \to B$ is smooth in a Zariski open neighbourhood of these sections. For every field $k/\mathbb{Q}$ and $b \in B(k)$, the curve C_b has k-rational points $\infty_{1,b}, \dots, \infty_{m,b} \in C_b(k)$; we call these the *marked points of C_b*.

Lemma 3.7.3. *There are natural bijections between:*

1. *The sections $\infty_1, \dots, \infty_m$ of $C \to B$;*

2. *Irreducible components of C_0;*

3. *G-orbits of regular nilpotent elements of V whose closure contains e.*

The bijections are given as follows: given a section ∞_i, map it to the irreducible component containing $\infty_{i,0} \in C_0$; given an irreducible component of C_0, map it to the G-orbit of any point on its smooth locus.

Proof. See [83, Lemma 4.14] and its proof. □

For the remainder of this thesis, we fix a section $\infty_1 = \infty$ of $C \to B$ and a regular nilpotent element $E \in V(\mathbb{Q})$ whose G-orbit corresponds to ∞ under Lemma 3.7.3. Moreover, we fix a choice of polynomials $p_{d_1}, \dots, p_{d_r} \in \mathbb{Q}[V]^G$ and coordinates x, y of C° satisfying the conclusions of Proposition 3.7.1. Recall that we have defined a $\mathbb{G}_m$-action on B which satisfies $\lambda \cdot p_{d_i} = \lambda^{d_i} p_{d_i}$. There exist unique positive integers a, b such that $\lambda \cdot (x, y, p_{d_1}, \dots, p_{d_{r-1}}) := (\lambda^a x, \lambda^b y, \lambda^{2d_1} p_{d_1}, \dots, \lambda^{2d_{r-1}} p_{d_{r-1}})$ defines a $\mathbb{G}_m$-action on C and such that the morphism $C \to B$ is $\mathbb{G}_m$-equivariant with respect to the square of the usual $\mathbb{G}_m$-action on B. (The integers (a, b) are given by (w_r, w_{r+1}) in the table of [83, Proposition 3.6]. These weights can also be defined Lie theoretically, but we will not need this fact in what follows.)

3.8 Universal centralisers

Recall from the last paragraph of §3.7 that we have fixed a regular nilpotent $E \in V(\mathbb{Q})$; let $\kappa \colon B \to V$ be the Kostant section corresponding to E constructed in §3.6. Recall from our conventions in §1.7 that if $v \colon S \to V$ is an S-point of V then $Z_G(v) \to S$ denotes the centraliser of v in G.

Definition 3.8.1. *Let $Z \to B$ be the centraliser $Z_G(\kappa)$ of the Kostant section $\kappa \colon B \to V$ with respect to the G-action on V. Similarly, let $A \to B$ be the centraliser $Z_H(\kappa)$ of $\kappa \colon B \to \mathfrak{h}$ with respect to the H-action on $\mathfrak{h}$.*

For every field $k/\mathbb{Q}$ and $b \in B(k)$, the group scheme Z_b (respectively A_b) is the centraliser $Z_G(\kappa_b) \subset G$ of κ_b in G (respectively $Z_H(\kappa_b) \subset H$). We have $Z = A \cap (G \times B)$. Since κ lands in the regular locus of V, A and Z are commutative group schemes. To state the next lemma, recall that $V^{reg} \subset V$ denotes the open subscheme of regular elements and that $\pi \colon V \to B$ and $p \colon \mathfrak{h} \to B$ denote the morphisms of taking invariants.

Lemma 3.8.2. *Let $v \colon S \to V^{reg}$ be a morphism with $b = \pi(v) \in B(S)$. Then there is a canonical isomorphism $Z_G(v) \simeq Z_b$. Similarly if $v \colon S \to \mathfrak{h}^{reg}$ is a morphism with invariants $b = p(v) \in B(S)$ then there is a canonical isomorphism $Z_H(v) \simeq A_b$.*

Proof. The isomorphism $Z_G(v) \simeq Z_b$ follows from [83, Proposition 4.1] and a very similar proof works for A; we briefly sketch it. The morphism $H \times B \to \mathfrak{h}^{reg}, (h, b) \mapsto h \cdot \kappa_b$ is smooth and surjective [70, Lemma 3.3.1], so has sections étale locally. It follows that v is H-conjugate to κ_b étale locally on S. Conjugating defines isomorphisms $Z_H(v) \simeq A_b$, again étale locally on S. Since A_b is commutative, these isomorphisms do not depend on the choice of element by which we conjugate v to κ_b. Using étale descent, these isomorphisms glue to give an isomorphism of group schemes $Z_H(v) \simeq A_b$. □

The next lemma gives a useful description of the fibres of $Z \to B$.

Lemma 3.8.3. *Let $k/\mathbb{Q}$ be a field and $x \in V(k)$ a regular element, with Jordan decomposition $x = x_s + x_n$. Let $\mathfrak{c} \subset V$ be a Cartan subspace containing x_s and let $C \subset H$ denote the maximal torus with Lie algebra $\mathfrak{c}$. Let $H_{sc} \to H$ be the simply connected cover of H and $C_{sc} \to C$ its restriction to C. Then there is a canonical isomorphism*

$$\mathrm{Hom}(Z_G(x), \mathbb{F}_2) \simeq \mathrm{image}\left(\frac{X^*(C)}{2X^*(C) + \mathbb{Z}\Phi_{\mathfrak{c}}(x)} \to \frac{X^*(C_{sc})}{2X^*(C_{sc}) + \mathbb{Z}\Phi_{\mathfrak{c}}(x)}\right). \tag{3.8.1}$$

Proof. A theorem of Steinberg [80, Theorem 8.1] shows that $(H_{sc})^\theta$ is connected. Therefore $Z_G(x) = \mathrm{image}(Z_{(H_{sc})^\theta}(x) \to Z_{H^\theta}(x))$. Now use [83, Corollary 2.9]. □

Let B^{rs} denote the image of the subscheme of regular semisimple elements in V under $\pi \colon V \to B$. Then B^{rs} is also the complement of the discriminant locus $(\Delta = 0)$ in B, by Part 3 of Proposition 2.3.3. For a B-scheme X, we denote its restriction to B^{rs} by X^{rs}. The group scheme $Z^{\mathrm{rs}} \to B^{\mathrm{rs}}$ is finite étale and $A^{\mathrm{rs}} \to B^{\mathrm{rs}}$ is a family of maximal tori.

Definition 3.8.4. *Let $\Lambda \to B^{\mathrm{rs}}$ be the character group of A^{rs}.*

In other words, Λ is the Cartier dual $\mathrm{Hom}(A^{\mathrm{rs}}, \mathbb{G}_m)$ of A^{rs}. The B^{rs}-scheme Λ is an étale sheaf of root lattices in the sense of §1.7. In particular, it comes equipped with a pairing $\langle \cdot, \cdot \rangle \colon \Lambda \times \Lambda \to \mathbb{Z}$. This pairing induces an alternating pairing $(\cdot, \cdot) \colon \Lambda/2\Lambda \times \Lambda/2\Lambda \to \mathbb{F}_2$ which might be degenerate. Setting $N_\Lambda := \mathrm{image}(\Lambda/2\Lambda \to \Lambda^\vee/2\Lambda^\vee)$, we see [83, Lemma 2.11] that $(\cdot, \cdot)$ descends to a nondegenerate pairing on N_Λ. Lemma 3.8.3 implies:

Lemma 3.8.5. *There exists a canonical isomorphism $Z^{\mathrm{rs}} \simeq N_\Lambda$.*

We use the isomorphism of Lemma 3.8.5 to transport the pairing from N_Λ to Z^{rs}: we thus obtain a nondegenerate pairing $Z^{\mathrm{rs}} \times Z^{\mathrm{rs}} \to \mathbb{F}_2$.

It follows from Lemma 3.7.2 that the restriction $C^{\mathrm{rs}} \to B^{\mathrm{rs}}$ is a family of smooth projective curves; write $J^{\mathrm{rs}} \to B^{\mathrm{rs}}$ for the relative Jacobian of the family of smooth projective curves $C^{\mathrm{rs}} \to B^{\mathrm{rs}}$ [23, §9.3; Theorem 1]. The next result is one of the main results of Thorne's thesis and a first step towards relating the curves $C^{\mathrm{rs}} \to B^{\mathrm{rs}}$ to the representation (G, V).

Proposition 3.8.6. *There exists an isomorphism $J^{\mathrm{rs}}[2] \simeq Z^{\mathrm{rs}}$ of finite étale group schemes that sends the Weil pairing on $J^{\mathrm{rs}}[2]$ to the pairing on Z^{rs} defined above.*

Proof. Since both group schemes are finite étale and B^{rs} is normal, it suffices to prove the statement above the generic point of B^{rs} by [79, Tag 0BQM]. In that case the statement follows from [83, Corollary 4.12]. $\square$

3.9 Monodromy of $J^{\mathrm{rs}}[2]$

We give some additional properties of the group scheme $J^{\mathrm{rs}}[2] \to B^{\mathrm{rs}}$, which by Lemma 3.8.5 and Proposition 3.8.6 we may identify with $N_\Lambda \to B^{\mathrm{rs}}$. Before we state them, we recall some definitions and set up notation.

Recall from §3.1 that T is a split maximal torus of H with Lie algebra $\mathfrak{t}$ and Weyl group W. Let $L := X^*(T)$ be its character group and $N_L := \mathrm{image}(L/2L \to L^\vee/2L^\vee)$. Consider the composition $\mathfrak{t} \to \mathfrak{t} /\!\!/ W \xrightarrow{\sim} \mathfrak{h} /\!\!/ H \xrightarrow{\sim} V /\!\!/ G = B$, where $\mathfrak{t} \to \mathfrak{t} /\!\!/ W$ is the natural projection, $\mathfrak{t} /\!\!/ W \xrightarrow{\sim} \mathfrak{h} /\!\!/ H$ the Chevalley restriction isomorphism (Proposition 2.1.1), and $\mathfrak{h} /\!\!/ H \xrightarrow{\sim} V /\!\!/ G$ is the isomorphism induced from the inclusion $V \subset \mathfrak{h}$ (Proposition 2.3.3). Restricting to regular semisimple elements defines a finite étale cover $f\colon \mathfrak{t}^{\mathrm{rs}} \to B^{\mathrm{rs}}$ with Galois group W.

Proposition 3.9.1. *The finite étale group scheme $J^{\mathrm{rs}}[2] \to B^{\mathrm{rs}}$ becomes trivial after the base change $f\colon \mathfrak{t}^{\mathrm{rs}} \to B^{\mathrm{rs}}$, where it becomes isomorphic to the constant group scheme N_L. The monodromy action is induced by the natural action of W on L.*

Proof. Since $J^{\mathrm{rs}}[2]$ is isomorphic to N_Λ, it suffices to prove that the torus $A \to B^{\mathrm{rs}}$ is isomorphic to the constant torus $T \times \mathfrak{t}^{\mathrm{rs}} \to \mathfrak{t}^{\mathrm{rs}}$ after pulling back along f, with monodromy given by the action of W on T.

To prove this, note that by Lemma 3.8.2, if $x\colon S \to \mathfrak{h}^{\mathrm{rs}}$ is an S-point with invariants $b = p(x) \in B^{\mathrm{rs}}(S)$, then $Z_H(x) \simeq A_b$ as group schemes over S. (Here $\mathfrak{h}^{\mathrm{rs}} \subset \mathfrak{h}$ denotes the subset of regular semisimple elements.) In particular, we can apply this to the $\mathfrak{t}^{\mathrm{rs}}$-point $i\colon \mathfrak{t}^{\mathrm{rs}} \to \mathfrak{h}^{\mathrm{rs}}$ (where i is the inclusion map), giving an isomorphism $T \times \mathfrak{t}^{\mathrm{rs}} \simeq A_{\mathfrak{t}^{\mathrm{rs}}}$. Since this isomorphism is induced by étale locally conjugating i to κ by elements of H, the monodromy action is indeed given by the natural action of W on T. $\square$

Proposition 3.9.1 shows that it suffices to understand the W-action on N_L if we wish to understand the group scheme $J^{\mathrm{rs}}[2]$. To this end, we perform some root system calculations in the following proposition.

Proposition 3.9.2. *Suppose that H is not of type A_1.*

1. *$L^\vee/2L^\vee$ has no nonzero W-invariant elements.*
2. *N_L has no nontrivial proper W-invariant subgroups.*
3. *There exists an element $w \in W$ that has no nonzero fixed points on N_L.*

Proof. 1. Note that $L^\vee/2L^\vee = \mathrm{Hom}(L/2L, \mathbb{F}_2)$, so let $f\colon L/2L \to \mathbb{F}_2$ be a nonzero W-invariant functional. If f vanishes on a root of L, then f vanishes on all of them since they form a single W-orbit. Since the roots of L generate $L/2L$, it follows that $f(\alpha) = 1$ for every root. Since we have assumed that L is not of type A_1, there exists roots α, β such that $\alpha+\beta$ is also a root. But then we would have $1 = f(\alpha+\beta) = f(\alpha)+f(\beta) = 1+1 = 0$. This is a contradiction hence no such nonzero f exists.

2. Let $S \subset N_L$ be a W-stable subgroup, and assume that $v \in S$ is a nonzero element. Since the pairing $(\cdot,\cdot)$ on N_L is nondegenerate, there exists a root $\alpha \in L$ such that $(v,\alpha) \neq 0$ in $\mathbb{F}_2$. If $w_\alpha \in W$ denotes the reflection associated to α, then $w_a(v) = v-(v,\alpha)\alpha = v+\alpha$ also lies in S. It follows that $w_a(v)-v = \alpha$ lies in S. Since W acts transitively on the roots, every root is contained in S. Since the roots generate $L/2L$, it follows that $S = N_L$, as claimed. (We thank Beth Romano for helping us with the proof of this fact.)

3. We first consider the case that the pairing on $L/2L$ is nondegenerate, which is equivalent to the projection map $L/2L \to N_L$ being injective. Since $L/2L$ and $L^\vee/2L^\vee$ have the same order, the latter statement is also equivalent to the fact that $L/2L \to L^\vee/2L^\vee$ is an isomorphism. We show that in this case it suffices to take a Coxeter element w_{cox} of W. Indeed, let $H_{sc} \to H$ be the simply connected cover of H, let π_1 be the centre of H_{sc} and let T_{sc} be the preimage of T in H_{sc}. It is a classical fact that the inclusion $\pi_1 \subset T_{sc}$ restricts to an equality $\pi_1 = T_{sc}^{w_{cox}}$, see [35, Theorem 1.6].[1] Taking 2-torsion implies that $\pi_1[2] = T_{sc}[2]^{w_{cox}}$. Since the map $L/2L \to L^\vee/2L^\vee$ is an isomorphism, the same is true for the map $T_{sc}[2] \to T[2]$ which has kernel $\pi_1[2]$, hence $T_{sc}[2]^{w_{cox}} = \pi_1[2] = \{1\}$. Since $T_{sc}[2] \simeq L/2L$, we have shown that $(L/2L)^{w_{cox}} = N_L^{w_{cox}} = 0$, as claimed.

   We now consider the general case. Let S be a root basis of L, which is an $\mathbb{F}_2$-basis of the vector space $L/2L$. Since $L/2L \to N_L$ is surjective, there exists a subset $S_M \subset S$ projecting onto a basis of N_L. Let M be the $\mathbb{F}_2$-span of S_M. Then M is a (possibly reducible) root lattice associated to the sub-root system generated by S_M, and the composition $M/2M \hookrightarrow L/2L \twoheadrightarrow N_L$ is an isomorphism. The pairing $(\cdot,\cdot)$ on $L/2L$ restricts to a pairing on $M/2M$, and the previous sentence shows that this pairing on

[1] The reference assumes that T is a maximal torus in a compact Lie group, but this implies the corresponding result for a maximal torus in a semisimple group over a field of characteristic zero.

$M/2M$ is nondegenerate. It follows that M is a direct sum of irreducible root lattices of the form considered in the first case of this proof. Let w be a Coxeter element with respect to S_M, i.e. a product of the simple reflections in S_M. Then $(M/2M)^w = 0$ by the first case of the proof, so $N_L^w = 0$ too.

$\square$

Chapter 4

The mildly singular locus

We keep the notations from Chapter 3. Recall from §3.8 that $B^{\mathrm{rs}} \subset B$ denotes the locus where the discriminant polynomial Δ is nonzero, and that the family of curves $C \to B$ is smooth exactly above B^{rs} (Lemma 3.7.2). In this chapter we introduce an open subset $B^1 \subset B$ strictly containing B^{rs} where we allow the fibres of $C \to B$ to have one nodal singular point. We therefore call B^1 the 'mildly singular locus' of B. We then extend some results concerning the representation V and the family of curves from B^{rs} to B^1 in §4.2 and §4.3, and generalise Proposition 3.8.6 in §4.4. This will be useful for the construction of orbits in §6 and for the analysis of integral orbits of square-free discriminant in §7.4. To avoid stating the same assumption repeatedly, we will make the following assumption throughout the rest of this thesis:

Convention 4.0.1. *The group H is not of type A_1.*

4.1 The discriminant locus

Recall that we have fixed a maximal torus $T \subset H$ in §3.1. Recall from §2.1 that the discriminant polynomial $\Delta \in \mathbb{Q}[\mathfrak{h}]^H$ is the image of $\prod_{\alpha \in \Phi_{\mathfrak{t}}} \alpha \in \mathbb{Q}[\mathfrak{t}]^W$ under the isomorphism $\mathbb{Q}[\mathfrak{t}]^W \xrightarrow{\sim} \mathbb{Q}[\mathfrak{h}]^H$ of the Chevalley restriction theorem. Using the isomorphism $\mathbb{Q}[\mathfrak{h}]^H \xrightarrow{\sim} \mathbb{Q}[V]^G = \mathbb{Q}[B]$ from Proposition 2.3.3, we view Δ as an element of $\mathbb{Q}[B]$.

Lemma 4.1.1. *For every field $k/\mathbb{Q}$, Δ is irreducible in $k[B]$.*

Proof. It suffices to prove that we cannot partition $\Phi_{\mathfrak{t}}$ into two nonempty W-invariant subsets. Equivalently, we need to prove that W acts transitively on $\Phi_{\mathfrak{t}}$. This is true since $\Phi_{\mathfrak{t}}$ is irreducible and simply laced. $\square$

We write D for the subscheme of B cut out by Δ. Lemma 4.1.1 implies:

Corollary 4.1.2. *The scheme D is geometrically integral.*

Write D_{sing} for the singular locus of D, a closed subscheme of D.

Definition 4.1.3. *We define B^1 as the complement of D_{sing} in B; we call B^1 the* mildly singular locus. *We define D^1 as the complement of D_{sing} in D.*

The subscheme $B^1 \subset B$ is open and we have inclusions $B^{\mathrm{rs}} \subsetneq B^1 \subsetneq B$. Since D is geometrically integral, the complement of B^1 in B has codimension ≥ 2. (In fact, Lemma 4.2.1 shows that it has codimension exactly 2.) As a general piece of notation, if X is a B-scheme we write X^1 for its restriction to B^1.

4.2 Representation theory over B^1

If b is a point of B we write $\mathfrak{h}_b$ for the fibre of the adjoint quotient $\mathfrak{h} \xrightarrow{p} \mathfrak{h} /\!\!/ H = B$ along this point.

Lemma 4.2.1. *Suppose that $k/\mathbb{Q}$ is an algebraically closed field and $b \in B(k)$. Then $b \in D^1(k)$ if and only if some (equivalently, every) semisimple $x \in \mathfrak{h}_b(k)$ has the property that the derived subgroup of $Z_H(x)$ is of type A_1.*

Proof. Since every two semisimple elements in $\mathfrak{h}_b(k)$ are $H(k)$-conjugate (Proposition 2.1.1), requiring the last claim for some semisimple element of $\mathfrak{h}_b(k)$ is equivalent to requiring it for all of them. Let $T \subset H$ be the fixed maximal torus of §3.1, with root system $\Phi_{\mathfrak{t}}$ and Weyl group W. Let x be an element of $\mathfrak{t}$ with invariants b. By Lemma 2.1.2, $Z_H(x)$ is a reductive group with root system $\Phi_{\mathfrak{t}}(x) = \{\alpha \in \Phi_{\mathfrak{t}} \mid \alpha(x) = 0\}$ and its Weyl group W_x is the subgroup of W generated by the reflections through $\Phi_{\mathfrak{t}}(x)$.

To prove the lemma, we need to prove that $b \in D^1(k)$ if and only if $\Phi_{\mathfrak{t}}(x)$ is of type A_1. Let b_x be the image of x in $\mathfrak{t} /\!\!/ W_x$ and let $D_x \subset \mathfrak{t} /\!\!/ W_x$ be the discriminant locus of $Z_H(x)$, with smooth locus D_x^1. By Lemma 2.1.3, $b \in D^1(k)$ if and only if $b_x \in D_x^1(k)$. So it suffices to prove that $b_x \in D_x^1(k)$ if and only if $\Phi_{\mathfrak{t}}(x)$ is of type A_1.

Firstly, suppose that $\Phi_{\mathfrak{t}}(x) = \{\alpha, -\alpha\}$ is of type A_1, so $W_x = \{1, w_\alpha\}$ is generated by the reflection through α. Then one can compute D_x explicitly: it is given, up to taking a product with an affine space, by the quotient of $\operatorname{Spec} k[X]$ by the $\mathbb{Z}/2\mathbb{Z}$-action $X \mapsto -X$. This quotient is $\operatorname{Spec} k[X^2]$ so smooth, hence D_x is smooth as well. Therefore $b_x \in D_x^1(k)$, which proves one direction.

Conversely, suppose that $\Phi_{\mathfrak{t}}(x)$ is not of type A_1. If $\Phi_{\mathfrak{t}}(x)$ were empty then $b \in B^{\mathrm{rs}}(k)$, so $\Phi_{\mathfrak{t}}(x)$ is nonempty and of rank ≥ 2. We need to prove that D is singular at b. Since the singular locus of D is closed and x is the specialisation of a point y for which the rank of

$\Phi_{\mathfrak{t}}(y)$ is exactly 2, we may assume that $\Phi_{\mathfrak{t}}(x)$ is either of type A_2 or $A_1 \times A_1$. In both cases, one can compute explicitly that D_x is not smooth at b_x, as required. □

Recall from Proposition 3.8.6 that if $k/\mathbb{Q}$ is a field and $b \in B^{\mathrm{rs}}(k)$, we have an isomorphism $Z_b \simeq J_b[2]$ of finite étale k-groups. So if g denotes the common arithmetic genus of the curves C_b, the group scheme Z_b has order 2^{2g}.

Lemma 4.2.2. *If $b \in D^1(k)$, the group scheme Z_b has order 2^{2g-1}.*

Proof. The group scheme Z_b is the centraliser of the element κ_b, which is regular by Proposition 3.6.1. By Lemma 3.8.3, it suffices to prove that if L is a root lattice of the same type as H, $N_L = \text{image}(L/2L \to L^\vee/2L^\vee)$ and $\alpha \in L$ is a root, then α is nonzero in N_L. Since L is not of type A_1 (Convention 4.0.1), there exists a root β with $(\alpha, \beta) = -1$. Therefore $\alpha \notin 2L^\vee$, so α is nonzero in N_L, as claimed. □

Before we state the last result of this section, we record a useful lemma.

Lemma 4.2.3. *Let $k/\mathbb{Q}$ be a field and $x \in \mathfrak{h}(k)$ a semisimple element with centraliser $L := Z_H(x)$. Then the centre of L is connected.*

Proof. We may assume that k is algebraically closed and that x lies in $\mathfrak{t}(k)$, the Lie algebra of the maximal torus $T \subset H$ fixed in §3.1. It suffices to prove that the character group of the centre of L is torsion-free. By Lemma 2.1.2 this group can be identified with $X^*(T)/\mathbb{Z}\Phi_{\mathfrak{t}}(x)$. Since H is adjoint, $X^*(T) = \mathbb{Z}\Phi_{\mathfrak{t}}$. The definition of the root system $\Phi_{\mathfrak{t}}(x)$ shows that it is $\mathbb{Q}$-closed in the sense of [77, §3.5]. By [77, Proposition 3.5], every root basis of $\Phi_{\mathfrak{t}}(x)$ can be extended to a root basis of $\Phi_{\mathfrak{t}}$. This implies that $\mathbb{Z}\Phi_{\mathfrak{t}}(x)$ is a direct summand of $\mathbb{Z}\Phi_{\mathfrak{t}}$ so the quotient $\mathbb{Z}\Phi_{\mathfrak{t}}/\mathbb{Z}\Phi_{\mathfrak{t}}(x)$ is indeed torsion-free. □

To state the next proposition, recall that $V^{reg} \subset V$ denotes the open subscheme of regular elements and that we have fixed a Kostant section κ in §3.8.

Proposition 4.2.4. *The action map $G \times B^1 \to V^{reg}|_{B^1}$, $(g, b) \mapsto g \cdot \kappa_b$ is surjective.*

Proof. Part 2 of Proposition 2.3.3 implies that this map is surjective when restricted to B^{rs}. Therefore it suffices to prove that if $k/\mathbb{Q}$ is algebraically closed and $b \in D^1(k)$, then every two elements $x, y \in V_b^{reg}(k)$ are $G(k)$-conjugate. Let $x = x_s + x_n$ and $y = y_s + y_n$ be the Jordan decompositions of x and y. Since the semisimple parts x_s and y_s are $G(k)$-conjugate by Proposition 2.2.4, we may assume that $x_s = y_s$. The centraliser $L := Z_H(x_s)$ is a reductive group with derived subgroup of type A_1 (Lemma 4.2.1); write $\mathfrak{l}$ for its Lie algebra. The involution θ restricts to a stable involution $\theta|_L$ on L [83, Lemma 2.5]. Since x and y are regular, x_n, y_n are regular nilpotent elements of $\mathfrak{l}^{\theta=-1}$. Therefore to prove the lemma, it suffices to prove that $L^\theta \cap G$ acts transitively on the regular nilpotents in $\mathfrak{l}^{\theta=-1}$. (Note that $L^\theta \subset H^\theta$ but we don't have $L^\theta \subset G$ in general.)

We first claim that L^θ acts transitively on the regular nilpotents in $\mathfrak{l}^{\theta=-1}$. To this end, let $Z(L)$ denote the centre of L and consider the exact sequence

$$0 \to Z(L) \to L \to \mathrm{PGL}_2 \to 0. \tag{4.2.1}$$

The involution θ preserves $Z(L)$ (acting via inversion by [83, Lemma 2.7(3)]) and by Lemma 2.3.2 we may choose the isomorphism $L/Z(L) \simeq \mathrm{PGL}_2$ so that θ corresponds to the standard stable involution $\xi = \mathrm{Ad}(\mathrm{diag}(1,-1))$ of PGL_2 from §3.1. An elementary computation in $\mathfrak{sl}_2$ (or Proposition 3.5.1) shows that PGL_2^ξ acts transitively on the regular nilpotents in $\mathfrak{l}^{\xi=-1}$. To prove the claim, we only need to show that $L^\theta \to \mathrm{PGL}_2^\xi$ is surjective. Since $Z(L)$ is connected (Lemma 4.2.3), $Z(L)/(1-\theta)Z(L)$ is trivial and therefore taking θ-invariants of (4.2.1) shows that indeed $L^\theta \to \mathrm{PGL}_2^\xi$ is surjective, proving the claim.

To prove that $L^\theta \cap G$ acts transitively on the regular nilpotents in $\mathfrak{l}^{\theta=-1}$, it suffices to prove that $L^\theta \cap G$ surjects onto PGL_2^ξ. We first claim that there exists a semisimple element $t \in V$ with centraliser $M = Z_H(t)$ such that $L \subset M$ and such that the derived subgroup of M is of type A_2. Indeed, take a Cartan subspace $\mathfrak{c} \subset V$ containing x_s; then $\Phi_\mathfrak{c}(x_s) = \{\pm\alpha\}$ for some root α. Since $\Phi_\mathfrak{c}$ is not of type A_1, there exists a root β such that $\{\pm\alpha, \pm\beta, \pm(\alpha+\beta)\} \subset \Phi_\mathfrak{c}$. Taking t to be an element of $\mathfrak{c}$ that vanishes exactly on those roots satisfies the requirements.

Again θ restricts to a stable involution on M and the isomorphism $M/Z(M) \simeq \mathrm{PGL}_3$ can be chosen so that θ agrees with the standard stable involution ψ of PGL_3 from §3.1. Again $Z(M)$ is connected by Lemma 4.2.3 and taking θ-invariants of the analogue of the sequence (4.2.1) for M gives an exact sequence

$$1 \to Z(M)^\theta \to M^\theta \to \mathrm{PGL}_3^\psi \to 1. \tag{4.2.2}$$

A component group calculation (Corollary 3.3.5) shows that PGL_3^ψ is connected. Therefore the identity component $(M^\theta)^\circ$ maps surjectively onto PGL_3^ψ. Since $(M^\theta)^\circ \subset M^\theta \cap G$, this implies that $M^\theta = (M^\theta \cap G)\cdot Z(M)^\theta$. It follows that $L^\theta = (L^\theta \cap G)\cdot Z(L)^\theta$. Indeed, if $l \in L^\theta$ there exists an element $z \in Z(M)^\theta$ such that $lz \in M^\theta \cap G$. Since $Z(M)^\theta \subset Z(L)^\theta$, we have $lz \in L^\theta \cap G$. We have established the equality $L^\theta = (L^\theta \cap G)\cdot Z(L)$, and it implies that $L^\theta \cap G$ surjects onto PGL_2^ξ. □

Remark 4.2.5. *Proposition 4.2.4 is false when H is of type A_1.*

4.3 Geometry over B^1

Recall from §3.7 that we have introduced a family of projective curves $C \to B$ which is smooth exactly above B^{rs}.

Lemma 4.3.1. *Let $k/\mathbb{Q}$ be a field and $b \in B(k)$. Then $b \in D^1(k)$ if and only if the curve C_b has a unique nodal singularity.*

Proof. A node is a simple singularity of type A_1. Therefore the lemma follows from Lemmas 3.7.2 and 4.2.1. □

The fibres of the morphism $C \to B$ may be reducible. However, this does not happen over B^1:

Lemma 4.3.2. *The fibres of $C^1 \to B^1$ are geometrically integral.*

Proof. The geometric fibres of $C \to B$ are reduced, connected, and over B^{rs} these fibres are smooth. Therefore it suffices to prove that C_b is irreducible if $k/\mathbb{Q}$ is algebraically closed and $b \in D^1(k)$. We prove this statement in two different ways.

For the first proof, let $Z \subset D^1$ be the locus above which the fibres fail to be geometrically integral. Then Z is closed by [39, Théorème 12.2.1(x)]. We claim that Z is also open. To prove this, it suffices to prove that Z is closed under generalisation [79, Tag 0903]. By [79, Tag 054F] this amounts to showing that for every complete discrete valuation ring R and morphism $\operatorname{Spec} R \to D^1$, the generic point of $\operatorname{Spec} R$ lands in Z if the closed point of $\operatorname{Spec} R$ does. If $b \in D^1(k)$ then C_b has a unique nodal singularity by Lemma 4.3.1, so either C_b is irreducible with one node or a union of two irreducible components intersecting transversally. Therefore if $b \in D^1(k)$, then C_b is reducible (in other words, $b \in Z$) if and only if the generalised Jacobian $\mathrm{Pic}^0_{C_b/k}$ is an abelian variety [23, §9.2, Example 8]. On the other hand, since the locus of $\operatorname{Spec} R$ where the relative Jacobian $\mathrm{Pic}^0_{C_R/R} \to \operatorname{Spec} R$ (which exists and is a semi-abelian scheme by [23, §9.3, Theorem 7]) is an abelian variety is open (this follows from looking at torsion points), we conclude that the generic fibre of $\mathrm{Pic}^0_{C_R/R}$ is an abelian variety if its special fibre is. It follows that Z is closed under generalisation, proving the claim. Since D^1 is irreducible and Z is open and closed, it follows that Z is empty or equal to D^1; we will exclude the latter case.

To this end, it suffices to prove that C_η is geometrically integral, where η is the generic point of D. Assume by contradiction that this is not the case. As observed in the previous paragraph, this implies that $\mathrm{Pic}^0_{C_\eta/\eta}$ is an abelian variety. Therefore the finite étale group scheme $J^{\mathrm{rs}}[2] \to B^{\mathrm{rs}}$ is unramified along D. By Zariski–Nagata purity for finite étale covers, this implies that $J^{\mathrm{rs}}[2]$ extends to a finite étale cover over B. Since B is isomorphic to affine space over k, this cover must be trivial. However, a monodromy calculation (Propositions 3.9.1 and 3.9.2) shows that $J^{\mathrm{rs}}[2]$ is nontrivial. (Recall that we have excluded that H is of type A_1.) This is a contradiction, completing the first proof of the lemma.

For the second proof, which we only sketch, we argue on a case-by-case basis. The only cases where reducible fibres occur are those of type A_{2n+1}, D_n and E_7. Let us treat the A_{2n+1} case and E_7 case, omitting details for the D_n case.

In the A_{2n+1} case, note that a hyperelliptic curve defined by $y^2 = f(x) = x^{2n+2} + \dots$ is reducible if and only if $f(x)$ is the square of a polynomial $h(x)$. In that case the curves $y = h(x)$ and $y = -h(x)$ intersect in $n+1$ points, counted with multiplicity. If $b \in D^1(k)$, then C_b has exactly one node, implying that $n+1 = 1$ so $n = 0$. Since we have excluded the A_1 case, this is a contradiction.

In the E_7 case, note that if $b \in B(k)$ then C_b is embedded in $\mathbb{P}^2$ as a plane quartic curve. If C_b were reducible, it would be the union of a curve of degree d_1 and d_2 with $d_1 + d_2 = 4$. By Bézout's theorem, such curves intersect in $d_1 d_2$ points (counted with multiplicity). If $b \in D^1(k)$, then C_b has exactly one node, implying that $d_1 d_2 = 1$, which is a contradiction. □

Since $C^1 \to B^1$ has geometrically integral fibres by Lemma 4.3.2, the group scheme $\mathrm{Pic}^0_{C^1/B^1}$ is well-defined and we denote it by $J^1 \to B^1$ [23, §9.3, Theorem 1]. It is a semi-abelian scheme. The 2-torsion subgroup $J^1[2] \to B^1$ is a quasi-finite étale group scheme; we may therefore view it as a sheaf on the étale site of B^1.

Lemma 4.3.3. *Let $j \colon B^{\mathrm{rs}} \hookrightarrow B^1$ be the open inclusion. Then $j_* J^{\mathrm{rs}}[2] = J^1[2]$ as étale sheaves on B^1.*

Proof. Consider the natural morphism $\phi \colon J^1[2] \to j_* j^* J^1[2] = j_* J^{\mathrm{rs}}[2]$ obtained by adjunction. Since $J^1 \to B^1$ is separated, $J^1[2] \to B^1$ is separated as well so ϕ is injective. To prove that ϕ is an isomorphism, it suffices to check this at geometric points of B^1. Combining the last two sentences, it suffices to prove that $(J^1[2])_{\bar{b}}$ and $(j_* J^{\mathrm{rs}}[2])_{\bar{b}}$ have the same cardinality for all geometric points $\bar{b}$ of B^1, or even that the cardinality of the latter is bounded above by the cardinality of the first. This is obvious if $\bar{b}$ lands in B^{rs}, so assume that $\bar{b}$ lands in D^1.

By Lemma 4.3.2, $C_{\bar{b}}$ is integral and has a unique singularity, which is a node. It follows that $J^1_{\bar{b}}$ has order 2^{2g-1}, where g is the arithmetic genus of C_b. On the other hand, the order of $(j_* J^{\mathrm{rs}}[2])_x$ for $x \in D^1$ can only go down under specialisation. It therefore suffices to prove that if η denotes the generic point of D, then $(j_* J^{\mathrm{rs}}[2])_\eta$ has order 2^{2g-1}. In fact, we claim that ϕ_η is an isomorphism.

To this end, let K be the fraction field of the discrete valuation ring $\mathscr{O}_{B,\eta}$ and let j_η be the inclusion $\operatorname{Spec} K \hookrightarrow \operatorname{Spec} \mathscr{O}_{B,\eta}$. Then the pullback of $j_* J^{\mathrm{rs}}[2]$ along $\operatorname{Spec} \mathscr{O}_{B,\eta} \to B$ equals $(j_\eta)_* J^{\mathrm{rs}}_K[2]$, where J^{rs}_K denotes the pullback J^{rs} along the generic point of B. The curve $C_{\mathscr{O}_{B,\eta}}$

is regular, since $\operatorname{Spec}\mathscr{O}_{B,\eta} \to B$ hence $C_{\mathscr{O}_{B,\eta}} \to C$ is formally smooth and the total space C is smooth. Therefore a result of Raynaud [23, §9.5, Theorem 1] shows that the identity component of the Picard functor of $C_{\mathscr{O}_{B,\eta}}$, which equals $J^1_{\mathscr{O}_{B,\eta}}$ by definition, is isomorphic to the Néron model of J_K. By the Néron mapping property, this shows that $J^1_\eta[2] = (j_*J^{\mathrm{rs}}[2])_\eta$. This completes the proof of the claim hence that of the lemma. $\square$

4.4 Summary of properties of B^1

We summarise the properties of D^1 in the next theorem.

Theorem 4.4.1. *Let $k/\mathbb{Q}$ be an algebraically closed field and $b \in B(k)$. Then the following are equivalent:*

1. *$b \in D^1(k)$;*
2. *for every semisimple $v \in V_b(k)$, the derived subgroup of $Z_H(v)$ is of type A_1;*
3. *C_b is irreducible and has a unique singular point, which is a node.*

Proof. Combine Lemmas 4.2.1 and 4.3.1. $\square$

Theorem 4.4.2. *The isomorphism $J^{\mathrm{rs}}[2] \simeq Z^{\mathrm{rs}}$ from Proposition 3.8.6 uniquely extends to an isomorphism $J^1[2] \simeq Z^1$ of separated étale group schemes over B^1.*

Proof. Since $J^{\mathrm{rs}}[2]$ and Z^{rs} are dense in $J^1[2]$ and Z^1 respectively, uniqueness is clear. For the existence, denote the open immersion $B^{\mathrm{rs}} \hookrightarrow B^1$ by j. Consider the composition $\psi\colon Z^1 \to j_*Z^{\mathrm{rs}} \xrightarrow{\sim} j_*J^{\mathrm{rs}}[2] \xrightarrow{\sim} J^1[2]$ of the adjunction morphism $Z^1 \to j_*Z^{\mathrm{rs}}$, the pushforward of the isomorphism $Z^{\mathrm{rs}} \xrightarrow{\sim} J^{\mathrm{rs}}[2]$ along j and the isomorphism $j_*J^{\mathrm{rs}}[2] \xrightarrow{\sim} J^1[2]$ of Lemma 4.3.3. Since $Z^1 \to B^1$ is separated, ψ is injective. It therefore suffices to prove that $Z^1_{\bar{b}}$ and $J^1_{\bar{b}}$ have the same cardinality for every geometric point $\bar{b}$ of D^1. If g denotes the common arithmetic genus of the fibres of $C \to B$, then $Z^1_{\bar{b}}$ has cardinality 2^{2g-1} by Lemma 4.2.2. On the other hand, $J^1_{\bar{b}}$ also has cardinality 2^{2g-1} by Lemmas 4.3.1 and 4.3.2. $\square$

Chapter 5

The compactified Jacobian

Recall from §3.8 that the family of smooth projective curves $C^{\mathrm{rs}} \to B^{\mathrm{rs}}$ has Jacobian variety $J^{\mathrm{rs}} \to B^{\mathrm{rs}}$ which is itself a smooth and projective morphism. The goal of this chapter is to extend the B^{rs}-scheme J^{rs} to a proper B-scheme $\bar{J}$ with good geometric properties. We achieve this using the theory of the compactified Jacobian of Altman–Kleiman [1], extended by Esteves [36] to incorporate reducible curves. Its construction is given in §5.2 and its basic properties are summarised in Theorem 5.3.5. Note that the occurrence of reducible fibres is the reason why the definition of $\bar{J}$ is more involved here than in our previous work [48, §4.3], which treats the E_6 case and where only irreducible fibres are present.

The results of this chapter will be useful for the construction of orbits in §6 (specifically §6.2) and the construction of integral representatives in §7.5.

5.1 Generalities on sheaves

The following material is largely taken from [36, 53]. Let k be an algebraically closed field. By a *curve* we mean a reduced projective scheme of pure dimension 1 over k.

Definition 5.1.1. *A coherent sheaf I on a connected curve X is said to be*

1. rank-1 *if $I_\eta \simeq \mathscr{O}_{X,\eta}$ as $\mathscr{O}_{X,\eta}$-modules for every generic point $\eta \in X$;*

2. torsion-free *if the associated points of I are precisely the generic points of X;*

3. simple *if* $\mathrm{End}_k(I) = k$.

We remark that the first two conditions imply the third if X is irreducible and that every torsion-free rank-1 sheaf on a smooth curve is invertible.

A *subcurve* Z of a curve X is a closed k-subscheme that is reduced and of pure dimension 1. If I is a torsion-free sheaf on X, its restriction to a subcurve $I|_Z$ is not necessarily torsion-free; it contains a biggest torsion subsheaf and the quotient of $I|_Z$ by this subsheaf is denoted by I_Z. The sheaf I_Z is the unique torsion-free quotient of I whose support is equal to Z.

Definition 5.1.2. *Let E be a vector bundle on a connected curve X of rank $r \geq 1$ and degree $-rd$ for some integer $d \in \mathbb{Z}$. Let I be a torsion-free rank-1 sheaf on X with Euler characteristic $\chi(I) = d$. We say that I is E-*semistable *if for every nonempty proper subcurve $Y \subsetneq X$ we have that*

$$\chi(I_Y) \geq -\frac{\deg(E|_Y)}{r}. \tag{5.1.1}$$

*We say that I is E-*stable *if for every nonempty proper subcurve the inequality* (5.1.1) *is strict.*

Given a vector bundle E on X, we may define its *multislope* $\underline{q}^E = \{q^E_{C_i}\}$ as follows. It is a tuple of rational numbers, one for each irreducible component C_i of X, defined by setting

$$q^E_{C_i} := -\frac{\deg(E|_{C_i})}{\operatorname{rank} E}.$$

If $Y \subset X$ is a subcurve, write $q^E_Y := \sum_{C_i \subset Y} q^E_{C_i}$, where the sum is taken over those irreducible components C_i that are contained in Y. If E is of rank r and degree $-rd$ then $q^E_X = d$. When the vector bundle E is clear from the context we omit the superscript from the notation $\underline{q}^E$.

Definition 5.1.3. *Let X be a curve and E a vector bundle on X of rank r and degree $-rd$ with multislope $\underline{q}$. We say that E is* general *if $q_Y \notin \mathbb{Z}$ for any nonempty proper subcurve $Y \subsetneq X$.*

If I is torsion-free rank-1 on X, then I is E-semistable if and only if $\chi(I_Y) \geq q_Y$ for every nonempty proper subcurve $Y \subset X$, and E-stable if every such inequality is strict. Therefore if E is general, a torsion-free rank-1 sheaf on X is E-semistable if and only if it is E-stable.

The next lemma shows that a family of simple torsion-free rank-1 sheaves has no unexpected endomorphisms. For a quasi-coherent sheaf $\mathscr{F}$ on a scheme X, we write $\mathscr{E}nd(\mathscr{F})$ for the sheaf of $\mathscr{O}_X$-module endomorphisms of $\mathscr{F}$, which is again a quasi-coherent sheaf on X.

Lemma 5.1.4. *Let $p\colon \mathscr{X} \to T$ be a flat family of projective curves whose geometric fibres are reduced and connected. Let I be a locally finitely presented $\mathscr{O}_{\mathscr{X}}$-module, flat over T, whose geometric fibres above T are simple torsion-free rank-1. Then $p_*\mathscr{E}nd(I) = \mathscr{O}_T$.*

Proof. Use [1, Corollary (5.3)] and the assumption that each geometric fibre is simple. $\square$

5.2 The definition

Recall from §3.7 that $C \to B$ is a flat projective morphism whose geometric fibres are reduced connected curves, and that this morphism has sections $\infty_1, \dots, \infty_m \colon B \to C$ landing in the smooth locus.

Lemma 5.2.1. *For every field $k/\mathbb{Q}$ and $b \in B(k)$, the irreducible components of C_b are geometrically irreducible. Moreover, every such irreducible component contains $\infty_{i,b}$ in its smooth locus for some i.*

Proof. The first claim follows from the second one. For the second one, we may assume that k is algebraically closed. Consider the line bundle $\mathscr{L} = \mathscr{O}_C(\infty_1 + \cdots + \infty_m)$ on C associated to the divisors ∞_i of C. For every $b \in B(k)$, $\mathscr{L}_b$ is ample if and only if every irreducible component of C_b contains $\infty_{i,b}$ for some i. Moreover, the locus of elements $b \in B$ for which $\mathscr{L}_b$ is ample is open [39, Corollaire (9.6.4)], $\mathbb{G}_m$-invariant (with respect to the $\mathbb{G}_m$-action on $C \to B$ introduced in §3.7) and contains the central point by Lemma 3.7.3. These three facts imply that it must be the whole of B. $\square$

In order to define a compactified Jacobian of $C \to B$, we first construct a vector bundle E on C using properties of the central fibre C_0. Recall from Lemma 3.7.3 that each of the m irreducible components of C_0 contains a unique marked point $\infty_{i,0}$. Let $\underline{q} = \{q_1, \dots, q_m\}$ be a tuple of rational numbers such that $\sum_{i=1}^m q_i = \chi(\mathscr{O}_{C_0}) = 1 - p_a(C_0)$ and $\sum_{i \in I} q_i \notin \mathbb{Z}$ for every nonempty proper subset $I \subset \{1, \dots, m\}$; it is easy to see that such a tuple exists. Write $q_i = e_i/r$ for some $e_i \in \mathbb{Z}$ and $r \in \mathbb{Z}_{\geq 1}$. By further multiplying e_i and r, we may assume that $r \geq m$. Let E be the following vector bundle on C:

$$E = \mathscr{O}_C(-e_1 \cdot \infty_1) \oplus \cdots \oplus \mathscr{O}_C(-e_m \cdot \infty_m) \oplus \mathscr{O}_C^{\oplus r-m}.$$

Since the image of $\infty_i \colon B \to C$ is a divisor of C, the line bundles $\mathscr{O}_C(-e_i \cdot \infty_i)$ are well-defined. Note that the vector bundle $E|_{C_0}$ has multislope $\underline{q}$ by construction. For every geometric point b of B, $E|_{C_b}$ is a vector bundle of rank r and degree $-r(1 - p_a(C_0))$ on the curve C_b.

Lemma 5.2.2. *For every geometric point b of B, the vector bundle $E|_{C_b}$ is general in the sense of Definition 5.1.3.*

Proof. Follows from Lemma 5.2.1 and the construction of E. $\square$

We are now ready to define the compactified Jacobian associated to E. We assume we have made a choice of $\underline{q}$ and E as above. Consider the functor

$$\bar{\mathbb{J}}_E \colon \{B\text{-}Schemes\} \to \{\text{Sets}\} \tag{5.2.1}$$

sending a B-scheme T to the set of equivalence classes of pairs (I,ϕ), where

- I is a locally finitely presented $\mathscr{O}_{C_T}$-module, flat over T, with the property that for every geometric point t of T, I_t is simple torsion-free rank-1, $\chi(I_t)=\chi(\mathscr{O}_{C_0})$ and I_t is E_t-stable;
- ϕ is an isomorphism $\infty_{1,T}^{*}I\simeq\mathscr{O}_T$ of $\mathscr{O}_T$-modules.

We say two pairs (I,ϕ) and (I',ϕ') are equivalent if there is an isomorphism $I\simeq I'$ mapping ϕ to ϕ'. We have the following basic representability result [36, Theorem B]:

Proposition 5.2.3 (Esteves)**.** *The functor $\bar{\mathbb{J}}_E$ is representable by a B-scheme $\bar{J}_E$.*

Proof. Let F be the functor from B-schemes to sets, sending a B-scheme T to the set of equivalence classes of locally finitely presented $\mathscr{O}_{C_T}$-modules I, flat over T, with the property that for every geometric point t of T, I_t is simple torsion-free rank-1, $\chi(I_t)=\chi(\mathscr{O}_{C_0})$ and I_t is E_t-stable. (In contrast to $\bar{\mathbb{J}}_E$, we omit the rigidification ϕ.) Here we say I and I' are equivalent if there exists an invertible sheaf $\mathscr{L}$ on T such that $I'\simeq\mathscr{L}_{C_T}\otimes I$. Let F^{et} denote the étale sheafification of F. By [36, Proposition 34], the functor F^{et} is representable by an open subspace of the algebraic space parametrising simple torsion-free rank-1 sheaves with no Euler characteristic or stability condition. By Lemma 5.2.1 and [36, Theorem B], the latter algebraic space is in fact a scheme, so F^{et} is representable by a scheme as well.

On the other hand, the forgetful morphism $\bar{\mathbb{J}}_E\to F,(T,\phi)\mapsto T$ is an isomorphism of functors, since every $I\in F(T)$ is equivalent to another element $I'\in F(T)$ admitting a rigidification. Since elements of $\bar{\mathbb{J}}_E$ have no nontrivial automorphisms by Lemma 5.1.4, étale descent of quasi-coherent sheaves implies that $\bar{\mathbb{J}}_E$ is an étale sheaf, so we have natural identifications $\bar{\mathbb{J}}_E=F=F^{et}$. Since F^{et} is representable by a scheme by the previous paragraph, the same is true for $\bar{\mathbb{J}}_E$. □

Definition 5.2.4. *We call $\bar{J}_E$ a compactified Jacobian of $C\to B$ associated to E.*

If $C\to B$ has reducible fibres, different choices of $\underline{q}$ may give rise to different compactified Jacobians. For our purposes, these differences will be harmless and for the remainder of this thesis we fix a choice of $\underline{q}$ and E as above and we simply write $\bar{J}=\bar{J}_E$.

Lemma 5.2.5. *Let k be a field and $b\in B(k)$ such that the curve C_b is integral. Then $\bar{J}_b$ parametrises torsion-free rank-1 sheaves on C_b with degree zero, i.e. Euler characteristic $1-p_a(C_0)$.*

Proof. If C_b is integral, the E_b-stability condition and the simplicity of the sheaves are automatic. □

5.3 Basic properties of $\bar{J}$

Lemma 5.3.1. *The morphism $\bar{J} \to B$ is projective*[1].

Proof. Since the vector bundle E is chosen to be general (Lemma 5.2.2), the notions of E-stable and E-semistable agree. Therefore, a theorem of Esteves [36, Theorem C.1 and C.4] shows that $\bar{J}$ is quasi-projective. Moreover, [36, Theorem A.1] shows that $\bar{J} \to B$ is universally closed. We conclude that $\bar{J}$ is projective over B. $\square$

Recall from §3.7 that we have defined a $\mathbb{G}_m$-action on C such that $C \to B$ is $\mathbb{G}_m$-equivariant with respect to the square of the usual $\mathbb{G}_m$-action on B. By functoriality, this induces a $\mathbb{G}_m$-action on $\bar{J}$ too such that $\bar{J} \to B$ is $\mathbb{G}_m$-equivariant (again with respect to the square of the usual $\mathbb{G}_m$-action on B). The following argument will be used in the next two lemmas: if $U \subset \bar{J}$ is an open $\mathbb{G}_m$-invariant subset containing the central fibre $\bar{J}_0$, then $U = \bar{J}$. Indeed, by the properness of $\bar{J} \to B$ the complement of U in $\bar{J}$ projects to a closed $\mathbb{G}_m$-invariant subset of B that does not contain the central point $0 \in B$, so must be empty.

Lemma 5.3.2. *The variety $\bar{J}$ is smooth.*

Proof. The family $C \to B$ is a semi-universal deformation of the plane curve singularity C_0 (Proposition 3.7.1). Therefore [53, Fact 4.2(ii)] implies that $\bar{J}$ is smooth in a neighbourhood of $\bar{J}_0$. Since the smooth locus of $\bar{J}$ is open, $\mathbb{G}_m$-invariant and contains $\bar{J}_0$, it must be the whole of $\bar{J}$. $\square$

We emphasise that the fibres of $\bar{J} \to B$ might be singular above points that do no lie in B^{rs}. In fact, we have a precise description of the smooth locus:

Lemma 5.3.3. *The morphism $\bar{J} \to B$ is flat of relative dimension $p_a(C_0)$. The smooth locus of $\bar{J} \to B$ coincides with the locus of invertible sheaves.*

Proof. By [53, Theorem 5.5(ii)], the morphism $\bar{J} \to B$ is flat in a neighbourhood of $\bar{J}_0$. Since the flat locus is open and $\mathbb{G}_m$-invariant, it follows that it must equal the whole of $\bar{J}$. The claim about the smooth locus is [53, Theorem 5.5(iii)]. $\square$

Lemma 5.3.4. *The geometric fibres of $\bar{J} \to B$ are reduced and connected. Consequently, $\bar{J}$ is geometrically integral. Moreover, if $k/\mathbb{Q}$ is an algebraically closed field and $b \in B(k)$ is such that C_b is integral, then $\bar{J}_b$ is integral.*

[1] There are several nonequivalent definitions of a projective morphism but in this case they all agree, see [79, Tag 0B45].

Proof. Since all the fibres of $C \to B$ have planar singularities, [53, Theorem A(i)-(iii)] shows that $\bar{J} \to B$ has geometrically reduced and connected fibres. Since $\bar{J}$ is B-flat, this implies that $\bar{J}$ is geometrically connected. Since $\bar{J}$ is smooth, it follows that it is geometrically irreducible. To establish the last claim, [53, Corollary 5.14] shows that the number of irreducible components of $\bar{J}_b$ can be calculated in terms of the intersections between the irreducible components of C_b. This number is always 1 when C_b is irreducible, as can be seen from [53, Definition 5.12]. □

For future reference, we summarise the above properties in the following theorem. Write $\bar{J}^1$ for the restriction of $\bar{J}$ to B^1. Recall from §4.3 that $J^1 \to B^1$ is the relative generalised Jacobian of the family of integral curves $C^1 \to B^1$. Note that by Lemma 5.2.5 and the definition of J^1 we have an open embedding $J^1 \to \bar{J}^1$.

Theorem 5.3.5. *Let $\bar{J} \to B$ be a compactified Jacobian associated to some choice of E as in Definition 5.2.4. Then the morphism $\bar{J} \to B$ is flat, projective and restricts to J^{rs} over B^{rs}. Its geometric fibres are reduced and connected. The scheme $\bar{J}$ is geometrically integral and smooth over $\mathbb{Q}$. The smooth locus of $\bar{J}^1 \to B^1$ is isomorphic to $J^1 \to B^1$. The complement of J^1 in $\bar{J}$ has codimension ≥ 2.*

Proof. Only the last two sentences remain to be established. The claim about the smooth locus of $\bar{J}^1$ follows from Lemmas 5.2.5 and 5.3.3 and the definition of J^1. For the claim about the codimension, let Z be the complement of J^1 in $\bar{J}$. Then Z is supported above the discriminant locus D of B. Moreover the fibres of the map $\bar{J}|_{D^1} \to D^1$ are geometrically integral by Lemmas 4.3.2 and 5.3.4, so the fibres of the map $Z|_{D^1} \to D^1$ have dimension strictly less than those of $\bar{J}|_{D^1} \to D^1$. Combining the last two sentences proves the claim. □

5.4 The Białynicki-Birula decomposition of $\bar{J}$

We recall the Białynicki-Birula decomposition [18] from geometric representation theory. If k is a field and X is a scheme of finite type of k, we define a *decomposition* of X to be a collection of locally closed subschemes $X_1, \ldots, X_n$ of X such that the underlying topological space of X is a disjoint union of the underlying topological spaces of the X_i.

Proposition 5.4.1. *Suppose that X is a smooth and separated scheme of finite type over a field k, endowed with a $\mathbb{G}_m$-action. Then the closed subscheme of fixed points $X^{\mathbb{G}_m}$ is smooth; let $F_1, \ldots, F_n$ denote its connected components. Suppose in addition that* $\lim_{\lambda \to 0} \lambda \cdot x$ *exists for every $x \in X$. Then there exists a decomposition of X into locally closed subschemes X_i and morphisms $X_i \to F_i$ which are affine space fibrations in the Zariski topology.*

Proof. See [43, Theorem 1.5] for a modern proof, which treats the generality in which we have stated it. We may informally describe X_i as those points $x \in X$ whose limit $\lim_{\lambda \to 0} \lambda \cdot x$ lies in F_i, and the map $X_i \to F_i$ as taking the limit $x \mapsto \lim_{\lambda \to 0} \lambda \cdot x$. $\square$

Corollary 5.4.2. *In the setting of Proposition 5.4.1, assume furthermore that X is geometrically integral and $X^{\mathbb{G}_m}$ is finite. Then there exists an open subset of X isomorphic to affine space $\mathbb{A}_k^{\dim X}$.*

Proof. Let $F_1, \dots, F_n$ denote the connected components of $X^{\mathbb{G}_m}$; since $X^{\mathbb{G}_m}$ is smooth and finite each F_i is the spectrum of a separable field extension k_i of finite degree over k. Let $X_1, \dots, X_n$ be the decomposition of X of Proposition 5.4.1. Then each X_i is isomorphic to $\mathbb{A}_{k_i}^{n_i}$ for some integer $n_i \geq 0$. There exists an X_i, say X_1, which is of maximal dimension $\dim X$. Since X_1 is locally closed, it is an open subset of its closure $\bar{X}_1 = X$, so X_1 is an open subset of X. Since X is geometrically irreducible, the same is true for X_1. This implies that $X_1 \times_k k_1$ is irreducible, so $k_1 = k$. Therefore X_1 is isomorphic to $\mathbb{A}_k^{\dim X}$. $\square$

Remark 5.4.3. *The proof shows that under the assumptions of Corollary 5.4.2, X is even decomposed into affine cells.*

We will apply Corollary 5.4.2 to the compactified Jacobian $\bar{J} \to B$ constructed in §5.2. Recall from §5.3 that $\bar{J}$ inherits a $\mathbb{G}_m$-action from C. We denote the central fibre of $\bar{J}$ by $\bar{J}_0$.

Lemma 5.4.4. *The set of $\mathbb{G}_m$-fixed points $\bar{J}_0^{\mathbb{G}_m}$ is finite.*

Proof. This follows from calculations of Beauville [4, §4.1] if C_0 is integral. It seems likely that one can extend his analysis to reducible curves, but we will proceed differently. We will assume that all schemes are base changed to a fixed algebraic closure k of $\mathbb{Q}$. Let $J(C_0)$ be the generalised Jacobian of C_0 parametrising line bundles having multidegree zero, i.e. degree zero on each irreducible component of C_0. Then $J(C_0)$ is an algebraic group acting on $\bar{J}_0$, compatibly with the $\mathbb{G}_m$-actions on $J(C_0)$ and $\bar{J}_0$.

First we claim that the closure of every $\mathbb{G}_m$-orbit of a point in $J(C_0)$ contains the identity. Indeed, every point of $[L] \in J(C_0)(k)$ is represented by a Cartier divisor $D_1 - \deg(D_1)\infty_{1,0} + \cdots + D_m - \deg(D_m)\infty_{m,0}$, where D_i is a Cartier divisor supported on the smooth affine part of the irreducible component $C_{0,i}$ of C_0 containing $\infty_{i,0}$. Since every smooth point P of $C_{0,i}$ satisfies $\lim_{\lambda \to \infty} \lambda \cdot P = \infty_{i,0}$ (as can be seen from the definition of the $\mathbb{G}_m$-action on C_0 in §3.7 and Table 1.1), we see that $\lambda \cdot [L] \to 0$ as $\lambda \to \infty$, proving the claim.

Secondly, we claim that the action of $J(C_0)$ on $\bar{J}_0$ has finitely many orbits. Indeed, let $p \in C_0$ be the unique singular point. Since p is an ADE-singularity, there are only finitely many isomorphism classes of torsion-free rank-1 modules over the completed local ring

$\widehat{\mathscr{O}}_{C_0,p}$ (see [44], in fact this property can be used to characterise ADE-singularities amongst Gorenstein singularities). It therefore suffices to prove that if $[\mathscr{F}],[\mathscr{G}] \in \bar{J}_0(k)$ are two sheaves whose completed stalks at p are isomorphic, then $\mathscr{F} \simeq \mathscr{G} \otimes \mathscr{L}$, where $\mathscr{L}$ is a line bundle on C_0 whose multidegree can only take finitely many values (independently of $\mathscr{F}$ and $\mathscr{G}$). To prove this, consider the Hom-sheaf $\mathscr{H} = \mathscr{H}om(\mathscr{F},\mathscr{G})$ and the endomorphism sheaf $\mathscr{E} = \mathscr{E}nd(\mathscr{F})$. Since $\mathscr{F}|_{C_0\setminus\{p\}}$ is a line bundle, $\mathscr{E}$ is a coherent commutative $\mathscr{O}_{C_0}$-algebra which is generically isomorphic to $\mathscr{O}_{C_0}$, and $\mathscr{H}$ is a coherent $\mathscr{E}$-module. Since the formation of $\mathscr{H}$ and $\mathscr{E}$ commutes with flat base change [79, Tag 0C6I], the completed stalk $\mathscr{H}_p \otimes \widehat{\mathscr{O}}_{C_0,p}$ is free of rank 1 over $\mathscr{E}_p \otimes \widehat{\mathscr{O}}_{C_0,p}$. It follows that $\mathscr{H}_p$ is free of rank 1 over $\mathscr{E}_p$, so the stalks $\mathscr{F}_p,\mathscr{G}_p$ are isomorphic $\mathscr{O}_{C_0,p}$-modules. (An isomorphism is given by choosing an $\mathscr{E}_p$-generator of $\mathscr{H}_p$.) By spreading out such an isomorphism, we may find an open subset $U \subset C_0$ containing p and an isomorphism $\phi_U : \mathscr{F}|_U \xrightarrow{\sim} \mathscr{G}|_U$. The restrictions of $\mathscr{F},\mathscr{G}$ to $C_0 \setminus \{p\}$ are line bundles. Since C_0 is connected and p is its unique singular point, the complement $C_0 \setminus U$ is a union of finitely many points. We may therefore find an open subset $V \subset C_0 \setminus \{p\}$ containing those points and an isomorphism $\phi_V : \mathscr{F}|_V \xrightarrow{\sim} \mathscr{G}|_V$. The transition map $(\phi_V)|_{U\cap V}^{-1} \circ (\phi_U)|_{U\cap V} : \mathscr{F}|_{U\cap V} \xrightarrow{\sim} \mathscr{F}|_{U\cap V}$ defines an element $f \in \mathrm{H}^0(U \cap V, \mathscr{O}_{C_0}^{\times})$. Let $\mathscr{L}$ be the line bundle on C_0 obtained by glueing $\mathscr{O}_U$ and $\mathscr{O}_V$ along the automorphism f. One can then explicitly check that the maps

$$\mathscr{F}_U \otimes \mathscr{O}_U \to \mathscr{G}_U : s \otimes 1 \mapsto \phi_U(s),$$
$$\mathscr{F}_V \otimes \mathscr{O}_V \to \mathscr{G}_V : s \otimes 1 \mapsto \phi_V(s),$$

glue to an isomorphism $\mathscr{F} \otimes \mathscr{L} \simeq \mathscr{G}$. The multidegree of $\mathscr{L}$ can only take on finitely many values (when we vary $\mathscr{F}$ and $\mathscr{G}$ in $\bar{J}_0$) because of the E-stability condition imposed on sheaves in $\bar{J}_0$. This completes the proof of the claim. (We thank Jesse Leo Kass for his help with the proof of this claim.)

We now use the last two paragraphs to show that $\bar{J}_0^{\mathbb{G}_m}$ is finite. Indeed, by the second claim, it suffices to prove that every $J(C_0)$-orbit contains at most one $\mathbb{G}_m$-fixed point. If $x \in \bar{J}_0^{\mathbb{G}_m}$ and $g \in J(C_0)$ are such that $g \cdot x \in \bar{J}_0^{\mathbb{G}_m}$, then $g^{-1}(\lambda \cdot g)$ lies in the stabiliser of x in $J(C_0)$ for all $\lambda \in \mathbb{G}_m$. Since this stabiliser is closed, the first claim implies that it contains $\lim_{\lambda\to\infty} g^{-1}\lambda \cdot g = g^{-1}$. Therefore g lies in the stabiliser of x, that is $g \cdot x = x$. We conclude that x is the only $\mathbb{G}_m$-fixed point in the $J(C_0)$-orbit of x. □

Theorem 5.4.5. *The variety $\bar{J}$ has a dense open subset isomorphic to affine space $\mathbb{A}^d_{\mathbb{Q}}$ for some $d \geq 1$.*

Proof. The compactified Jacobian is a smooth, geometrically integral and quasi-projective scheme over $\mathbb{Q}$ (Theorem 5.3.5). Since $\bar{J} \to B$ is proper and $\lim_{\lambda\to 0} \lambda \cdot b$ exists for every

$b \in B$, $\lim_{\lambda \to 0} \lambda \cdot x$ exists for every $x \in \bar{J}$. We wish to apply Corollary 5.4.2, so it suffices to prove that the fixed point locus $\bar{J}^{\mathbb{G}_m}$ is finite. Since $B^{\mathbb{G}_m}$ consists of the central point 0, it suffices to prove that $\bar{J}_0^{\mathbb{G}_m}$ is finite, which is exactly Lemma 5.4.4. $\square$

Remark 5.4.6. *The Białynicki-Birula decomposition gives a canonical decomposition of $\bar{J}$ into locally closed subschemes isomorphic to affine space. If H is of type A_{2g}, $C \to B$ is the family of odd hyperelliptic curves of genus g (see Table 1.1) and this decomposition is closely related to the Mumford representation of a point in the Jacobian of such a curve [55, IIIa]. It would be interesting to obtain a similarly concrete interpretation of this decomposition for other families of curves studied here.*

Chapter 6

Constructing orbits

The goal of this chapter is to construct for every $b \in B^{\mathrm{rs}}(\mathbb{Q})$ and every element of $\mathrm{Sel}_2 J_b$ a $G(\mathbb{Q})$-orbit of $V_b(\mathbb{Q})$, see Corollary 6.4.2. The technical input is the Zariski triviality of a certain universal torsor on J^{rs} in §6.2, see Theorem 6.2.1. This will be achieved using generalities concerning torsors on open subsets of affine spaces developed in §6.1.

6.1 Torsors on open subsets of affine space

The purpose of this subsection is to prove the following theorem, which will be useful in the proof of Theorem 6.2.1.

Theorem 6.1.1. *Let k be a field of characteristic zero and X an open subset of $\mathbb{A}^n_k$ whose complement has codimension ≥ 2. Let G be a reductive group over k and let $T \to X$ be a G-torsor. Suppose that X contains a k-rational point over which T is trivial. Then T is Zariski locally trivial.*

Example 6.1.2. *We illustrate Theorem 6.1.1 in the concrete case $G = \mathrm{PGL}_2$. If k and X are as in the theorem, then a PGL_2-torsor can alternatively be viewed as a Severi–Brauer curve $\mathscr{C} \to X$. In other words, $\mathscr{C} \to X$ is a smooth projective family of genus zero curves (i.e. conics). Suppose that X contains a point $x \in X(k)$ such that the conic $\mathscr{C}_x$ has a k-rational point. Then Theorem 6.1.1 says that $\mathscr{C}$ is a projective bundle over X. This implies that all the other fibres of $\mathscr{C} \to X$ also contain a k-rational point.*

Theorem 6.1.1 might be well known to experts, although we have not been able to locate it explicitly in the literature. It will follow from a slight variant of the formalism developed by Colliot-Thélène in [28, §1].

Let k be a field and let F be a covariant functor from the category of local k-algebras (with morphisms given by homomorphisms of k-algebras) to the category of pointed sets. For any integral k-scheme X, we write

$$D^F(X) := \bigcap_{P\in X} \operatorname{image}\left(F(\mathscr{O}_{X,P}) \to F(k(X))\right).$$

We interpret $D^F(X)$ as the subset of elements of $F(k(X))$ which have 'good reduction' at every point $P \in X$. Consider the following properties of the functor F:

- We say F satisfies (**S**) (the specialisation property) if for every k-algebra A that is a discrete valuation ring with fraction field K and residue field κ, two elements in $F(A)$ that have the same image in $F(K)$ have the same image in $F(\kappa)$.
- We say F satisfies (**H**) (the homotopy invariance property) if for every field extension K/k, the natural map $F(K) \to D^F(\mathbb{A}^1_K)$ is a bijection.

The main input for the proof of Theorem 6.1.1 is the next proposition, which will occupy the remainder of this subsection.

Proposition 6.1.3. *Let X be an open subset of $\mathbb{A}^n_k$ whose complement has codimension ≥ 2. Let F be a functor satisfying property (**S**) and (**H**). Suppose that k is infinite. Then the natural map $F(k) \to D^F(X)$ is a bijection.*

An analogue of Proposition 6.1.3 is proved in [28, Théorème 1.5], but where the functor F takes values in abelian groups rather than pointed sets. Therefore the arguments are slightly different at various points, and for the sake of completeness we give full details even though all the ideas are already present in [28, §1]. The proofs of Proposition 6.1.3 and Theorem 6.1.1 are given after some preparatory lemmas.

Lemma 6.1.4. *Suppose that F satisfies (**S**), and let $(A,\mathfrak{m})$ be a regular local k-algebra with fraction field K and residue field κ. Then every two elements in $F(A)$ that have the same image in $F(K)$ have the same image in $F(\kappa)$.*

Proof. We will prove the lemma by induction on the dimension of A. If $\dim A = 1$, the lemma holds by assumption (**S**), so suppose that $\dim A \geq 2$. Let $t \in \mathfrak{m}$ be a regular parameter, and write $B = A/t$. Then B is a regular local k-algebra with $\dim B = \dim A - 1$ and with residue field κ. Moreover $A_{(t)}$ (the localisation of A at the prime ideal (t)) is a discrete valuation ring with fraction field K and residue field isomorphic to $\operatorname{Frac} B$, the fraction field of B. Let $x, y \in F(A)$ be two elements that have the same image in $F(K)$. Since the conclusion of the lemma holds for the discrete valuation ring $A_{(t)}$ which also has fraction field K, x and y map to the same element in $F(A_{(t)}/(t)) = F(\operatorname{Frac} B)$. By the induction hypothesis applied to B, x and y have the same image in κ (the residue field of B), as required. □

If $f\colon X \to Y$ is a dominant morphism between regular integral k-schemes, the pullback map $F(k(Y)) \to F(k(X))$ restricts to a map $D^F(f)\colon D^F(Y) \to D^F(X)$. If F satisfies (**S**), we may extend this functorial assignment $f \mapsto D^F(f)$ to morphisms which are not necessarily dominant.

Construction 6.1.5. *Suppose that F satisfies (**S**). Let $f\colon X \to Y$ be a (not necessarily dominant) morphism between regular integral k-schemes. Let η be the generic point of X and let $f(\eta) = P$, which defines a homomorphism $\mathcal{O}_{Y,P} \to k(X)$. Define the map $D^F(f)\colon D^F(Y) \to D^F(X)$ as follows: let $\alpha \in D^F(Y)$ be an arbitrary element and let $\beta \in F(\mathcal{O}_{Y,P})$ be an element mapping to α under $F(\mathcal{O}_{Y,P}) \to F(k(Y))$. Define $D^F(f)(\alpha)$ as the image of β under $F(\mathcal{O}_{Y,P}) \to F(k(X))$.*

Lemma 6.1.6. *Suppose that F satisfies (**S**). Then Construction 6.1.5 turns D^F into a contravariant functor from the category of regular integral k-schemes to the category of pointed sets.*

Proof. We first show that $D^F(f)(\alpha)$ does not depend on the choice of β, so is well defined. Indeed, if $\beta' \in F(\mathcal{O}_{Y,P})$ is another lift of α, then by Lemma 6.1.4 (which uses assumption (**S**)) β and β' have the same image in $F(k(P))$, where $k(P)$ denotes the residue field of Y at P. Since the homomorphism $\mathcal{O}_{Y,P} \to k(X)$ factors through $\mathcal{O}_{Y,P} \to k(P)$, β and β' have the same image in $F(k(X))$, as required.

Next we show that $D^F(f)(\alpha) \in F(k(X))$ actually lands in $D^F(X)$. Indeed, if $x \in X$ with $f(x) = y$, then by assumption α is the image of an element $\gamma \in F(\mathcal{O}_{Y,y})$ under the map $F(\mathcal{O}_{Y,y}) \to F(k(Y))$. Since the generic point of X specialises to x, P specialises to y and the morphism $\mathcal{O}_{Y,y} \to k(Y)$ factors through $\mathcal{O}_{Y,y} \to \mathcal{O}_{Y,P}$. Therefore the image of γ under $F(\mathcal{O}_{Y,y}) \to F(\mathcal{O}_{Y,P})$ is a lift of α to $F(\mathcal{O}_{Y,P})$ and can be used to define $D^F(f)(\alpha)$. The commutative diagram

$$\begin{tikzcd} \mathcal{O}_{Y,y} \arrow[r] \arrow[d] & \mathcal{O}_{Y,P} \arrow[d] \\ \mathcal{O}_{X,x} \arrow[r] & k(X) \end{tikzcd}$$

shows that $D^F(f)(\alpha)$ lies in the image of $F(\mathcal{O}_{X,x}) \to F(k(X))$, as required.

Finally, the functoriality of D^F follows from the construction and the functoriality of F. □

Lemma 6.1.7. *Let $\pi\colon X \to Y$ be a morphism between regular integral k-schemes. Let η denote the generic point of Y and $p\colon X_\eta \to \eta = \operatorname{Spec} k(Y)$ the generic fibre of π. Suppose that F satisfies* (**S**) *and that:*

1. *π has sections Zariski locally: for each $y \in Y$ there is an open subset $U \subset Y$ containing y such that $\pi|_U : X|_U \to U$ admits a section;*
2. *The induced map $D^F(p)\colon F(k(Y)) \to D^F(X_\eta)$ is a bijection.*

Then the induced map $D^F(\pi)\colon D^F(Y) \to D^F(X)$ is a bijection.

Proof. Follows from a diagram chase similarly to [28, Proposition 1.3]. Indeed, let $\sigma\colon U \to X$ be a section of π over an open subset $U \subset Y$, and let $s\colon \eta \to X_\eta$ be its generic fibre, a section of p. Using the functoriality of D^F, consider the following commutative diagram of pointed sets:

$$\begin{array}{ccccc}
D^F(Y) & \xrightarrow{\pi^*} & D^F(X) & & \\
\rotatebox{90}{$\supseteq$} & & \rotatebox{90}{$\supseteq$} & & \\
D^F(U) & \xrightarrow{\pi_U^*} & D^F(\pi^{-1}(U)) & \xrightarrow{\sigma^*} & D^F(U) \\
\rotatebox{90}{$\supseteq$} & & \rotatebox{90}{$\supseteq$} & & \rotatebox{90}{$\supseteq$} \\
F(k(Y)) & \xrightarrow[\sim]{p^*} & D^F(X_\eta) & \xrightarrow[\sim]{s^*} & F(k(Y))
\end{array}$$

Here we have written π^* instead of $D^F(\pi)$ etcetera to ease notation. The map p^* is a bijection by assumption. Moreover $s^* \circ p^* = \mathrm{Id}$ by functoriality, hence s^* is a bijection too and $p^* \circ s^* = \mathrm{Id}$. The latter identity and functoriality again imply that π_U^* and σ^* are mutually inverse bijections.

We prove that π^* is a bijection. Since π^* is the restriction of the injective map π_U^*, it is injective as well. To prove surjectivity, note that every $\alpha \in D^F(X)$ has a unique lift to $F(k(Y))$ under p^* which moreover lies in $D^F(U)$. Since π has sections Zariski locally by assumption and $D^F(X)$ equals the intersection of $D^F(U)$ where U ranges over an open cover of X, this unique lift lies in $D^F(X)$, proving surjectivity. □

Lemma 6.1.8. *Suppose that k is infinite. Let $X \subset \mathbb{A}_k^n$ be an open subset whose complement has codimension ≥ 2. Then there exists a sequence of morphisms $X_n \xrightarrow{\pi_n} \cdots \to X_2 \xrightarrow{\pi_2} X_1 \xrightarrow{\pi_1} X_0$, where each X_m is an open subset of $\mathbb{A}_k^m$, satifying the following properties:*

1. *$X_n = X$, $X_0 = \operatorname{Spec} k$ and for every $m \geq 1$ the complement of X_m in $\mathbb{A}_k^m$ has codimension ≥ 2;*

2. *Each $\pi_m \colon X_m \to X_{m-1}$ has sections Zariski locally and has generic fibre isomorphic to $\mathbb{A}^1_\eta \to \eta$, where η is the generic point of X_{m-1}.*

Proof. Apply [28, Proposition 1.4] repeatedly. $\square$

Proof of Proposition 6.1.3. Let X be an open subset of $\mathbb{A}^n_k$ whose complement has codimension ≥ 2. Choose a sequence of morphisms $X = X_n \xrightarrow{\pi_n} X_{n-1} \to \dots \xrightarrow{\pi_2} X_1 \xrightarrow{\pi_1} X_0 = \operatorname{Spec} k$ satisfying the conclusions of Lemma 6.1.8. Since we have assumed that F satisfies (**H**) and (**S**), we may apply Lemma 6.1.7 to obtain bijections $D^F(X_0) \xrightarrow{\sim} D^F(X_1) \xrightarrow{\sim} \dots \xrightarrow{\sim} D^F(X_n) = D^F(X)$. By functoriality of D^F, the composition of these maps equals the natural map $F(k) = D^F(\operatorname{Spec} k) \to D^F(X)$, which is therefore a bijection. $\square$

Proof of Theorem 6.1.1. We claim that the functor $F = \mathrm{H}^1(-, G)$ satisfies (**S**) and (**H**). Property (**S**) follows from (a very weak form of) known cases of the Grothendieck–Serre conjecture (Proposition 2.5.3). To prove Property (**H**), let K/k be a field extension and consider the natural map $h \colon F(K) \to D^F(\mathbb{A}^1_K)$. Since $\mathbb{A}^1_K$ has a K-point, functoriality of D^F (Lemma 6.1.6) shows that h is injective. On the other hand, every element of $D^F(\mathbb{A}^1_K)$ extends to a G-torsor on $\mathbb{A}^1_K$ by [29, Proposition 6.8]. (Note that their definition of D^G is not compatible with our notation.) Since every G-torsor on $\mathbb{A}^1_K$ is induced from $\operatorname{Spec} K$ by a result of Ranghunathan and Ramanathan ([66, Theorem 1.1] and the remark immediately thereafter), it follows that h is also surjective.

We may therefore apply Proposition 6.1.3, which says that the natural map $F(\operatorname{Spec} k) \to D^F(X)$ is a bijection. Let T be a G-torsor on X satisfying the assumptions of Theorem 6.1.1. Since the generic fibre of T (which defines a class in $D^F(X)$) is induced from $F(\operatorname{Spec} k)$, Corollary 2.5.4 shows that T is Zariski locally isomorphic to a G-torsor $T' \to X$ that is induced from $\operatorname{Spec} k$. So to prove that T is Zariski locally trivial, it suffices to prove that T' is a trivial torsor. Since T' is induced from $\operatorname{Spec} k$, it suffices to prove that T' is trivial when pulled back along a k-point of X. Since X has a k-point $x \in X(k)$ above which T is trivial and since T and T' are isomorphic in a neighbourhood of x, T' is also trivial above x, as desired. $\square$

6.2 A universal torsor

Recall from §3.8 that $J^{\mathrm{rs}} \to B^{\mathrm{rs}}$ denotes the relative Jacobian of the family of smooth curves $C^{\mathrm{rs}} \to B^{\mathrm{rs}}$, that $Z \to B$ denotes the universal stabiliser of the Kostant section κ, and that there is an isomorphism of finite étale group schemes $J^{\mathrm{rs}}[2] \simeq Z^{\mathrm{rs}}$ over B^{rs}.

Since $J^{\mathrm{rs}} \to B^{\mathrm{rs}}$ is an abelian scheme, the multiplication-by-2 map $J^{\mathrm{rs}} \xrightarrow{\times 2} J^{\mathrm{rs}}$ is a $J^{\mathrm{rs}}[2]$-torsor. Pushing out this torsor along the maps $J^{\mathrm{rs}}[2] \xrightarrow{\sim} Z^{\mathrm{rs}} \hookrightarrow G$ defines a G-torsor $T^{\mathrm{rs}} \to J^{\mathrm{rs}}$.

(This procedure is also called 'changing the structure group'.) The following theorem is one of the main technical results of this thesis, and is the essential input for constructing orbits associated to elements of $J_b(\mathbb{Q})$ (Theorem 6.3.2).

Theorem 6.2.1. *The torsor T^{rs} is Zariski locally trivial. That is, for every $x \in J^{\mathrm{rs}}$ there exists an open subset $U \subset J^{\mathrm{rs}}$ containing x such that $T^{\mathrm{rs}}|_U$ is trivial.*

To briefly explain why this is relevant for constructing orbits, note that if $b \in B^{\mathrm{rs}}(\mathbb{Q})$ and $P \in J_b(\mathbb{Q})$, the image of P under the composition $J_b(\mathbb{Q})/2J_b(\mathbb{Q}) \to \mathrm{H}^1(\mathbb{Q}, J_b[2]) \xrightarrow{\sim} \mathrm{H}^1(\mathbb{Q}, Z_b) \to \mathrm{H}^1(\mathbb{Q}, G)$ coincides with the isomorphism class of the pullback of T^{rs} along $P\colon \operatorname{Spec}\mathbb{Q} \to J^{\mathrm{rs}}$. Theorem 6.2.1 implies that this pullback defines the trivial class in $\mathrm{H}^1(\mathbb{Q}, G)$, which implies that it corresponds to a $G(\mathbb{Q})$-orbit of $V_b(\mathbb{Q})$; see Theorem 6.3.2 for full details.

Proof of Theorem 6.2.1. Recall from §4 that $B^1 \subset B$ is an open subset containing B^{rs} and that the family of curves $J^1 \to B^1$ is the relative (generalised) Jacobian of the family of curves $C^1 \to B^1$. By Theorem 4.4.2 the isomorphism $J^{\mathrm{rs}}[2] \simeq Z^{\mathrm{rs}}$ extends to an isomorphism $J^1[2] \simeq Z^1$ of quasi-finite étale group schemes over B^1. The multiplication-by-two map $J^1 \xrightarrow{\times 2} J^1$ is a $J^1[2]$-torsor, and pushing out this torsor along the composition $J^1[2] \xrightarrow{\sim} Z^1 \to G$ defines a G-torsor $T^1 \to J^1$. By construction, the restriction of T^1 to J^{rs} is isomorphic to T^{rs}.

To prove the theorem, it suffices to prove that T^1 is Zariski locally trivial. Using known cases of the Grothendieck–Serre conjecture (Corollary 2.5.4) it even suffices to prove that T^1 is Zariski locally trivial when restricted to a nonempty open subset of J^1.

Recall from §5 that we have constructed a scheme $\bar{J} \to B$ containing J^1 as an open subscheme. By Theorem 5.3.5, the complement of J^1 in $\bar{J}$ has codimension ≥ 2; by Theorem 5.4.5, $\bar{J}$ contains an open dense subscheme U isomorphic to affine $\mathbb{Q}$-space. This implies that the complement of $U^1 := U \cap J^1$ in U has codimension ≥ 2.

We claim that $T^1|_{U^1}$ is Zariski locally trivial. By Theorem 6.1.1, it suffices to prove that T^1_x is trivial for some $x \in U^1(\mathbb{Q})$. In fact, we will show the stronger statement that $\{x \in J^1(\mathbb{Q}) \mid T^1_x \text{ is trivial}\}$ is Zariski dense in J^1. Indeed, since J^1 is a rational variety (it contains U^1 as a dense open subscheme), the set $J^1(\mathbb{Q})$ is dense in J^1. Since the multiplication-by-two map $J^1 \xrightarrow{\times 2} J^1$ is dominant, the subset $2J^1(\mathbb{Q}) \subset J^1(\mathbb{Q})$ is still dense in J^1. By construction of T^1, the pullback of T^1 along a point $x \in 2J^1(\mathbb{Q})$ is trivial. This completes the proof of the claim, hence the proof of the theorem. $\square$

6.3 Constructing orbits for 2-descent elements

We start by applying a well known lemma from arithmetic invariant theory recalled in §2.4 to give a cohomological description of the G-orbits of V.

Corollary 6.3.1. *Let R be a $\mathbb{Q}$-algebra and $b \in B^{\mathrm{rs}}(R)$. Then the association $v \mapsto \{g \in G \mid g \cdot v = \kappa_b\}$ induces an injection*

$$\gamma_b \colon G(R)\backslash V_b(R) \hookrightarrow \mathrm{H}^1(R, J_b[2]).$$

Its image coincides with the pointed kernel of the map $\mathrm{H}^1(R, J_b[2]) \xrightarrow{\sim} \mathrm{H}^1(R, Z_b) \to \mathrm{H}^1(R, G)$.

Proof. We apply Lemma 2.4.2 to the action of $G_{B^{\mathrm{rs}}}$ on V^{rs}. Indeed, the action map $G \times B^{\mathrm{rs}} \to V^{\mathrm{rs}}, (g, b) \mapsto g \cdot \kappa_b$ is étale (Proposition 3.6.1) and it is surjective by Proposition 2.3.3. Pulling back along $b \colon \operatorname{Spec} R \to B^{\mathrm{rs}}$ and using the isomorphism $J_b[2] \simeq Z_b$ from Proposition 3.8.6 gives the desired bijection. □

We now piece all the ingredients obtained so far together to deduce our first main theorem.

Theorem 6.3.2. *Let R be a local $\mathbb{Q}$-algebra (for example, a field of characteristic zero) and $b \in B^{\mathrm{rs}}(R)$. Then the image of the 2-descent map $J_b(R)/2J_b(R) \to \mathrm{H}^1(R, J_b[2]) \simeq \mathrm{H}^1(R, Z_b)$ lies in the image of γ_b of Corollary 6.3.1. Consequently, there is a canonical injection*

$$\eta_b \colon J_b(R)/2J_b(R) \hookrightarrow G(R)\backslash V_b(R)$$

compatible with base change.

Proof. By Corollary 6.3.1, it suffices to prove that the composition $J_b(R)/2J_b(R) \to \mathrm{H}^1(R, J_b[2]) \simeq \mathrm{H}^1(R, Z_b) \to \mathrm{H}^1(R, G)$ is trivial. Recall that in §6.2 we have constructed a G-torsor $T^{\mathrm{rs}} \to J^{\mathrm{rs}}$ such that its pullback along a point $P \colon \operatorname{Spec} R \to J^{\mathrm{rs}}$ defines a G-torsor $T^{\mathrm{rs}}_P \to \operatorname{Spec} R$ whose isomorphism class equals the image of P under the above composite map. Since T^{rs} is Zariski locally trivial by Theorem 6.2.1, T^{rs}_P is Zariski locally trivial. Since R is a local ring, it follows that T^{rs}_P is trivial. This completes the proof. □

Remark 6.3.3. *In the proof of Theorem 6.2.1 we have shown the stronger statement that the torsor $T^1 \to J^1$ (a natural extension of T^{rs} to J^1) is Zariski locally trivial. A straightforward adaption of the proof of Theorem 6.3.2 then shows that if R is a local ring and $b \in B^1(R)$ (instead of $b \in B^{\mathrm{rs}}(R)$), then there exists an injection $J^1_b(R)/2J^1_b(R) \hookrightarrow G(R)\backslash V^{reg}_b(R)$. We do not know if this observation is useful.*

6.4 Constructing orbits for 2-Selmer elements

The next proposition might be well known to experts — see for example [61, Remark after Theorem 6.22] — but we believe it deserves to be stated explicitly. We slightly deviate from our standing notation and allow G to be an arbitrary split semisimple group in this proposition.

Proposition 6.4.1. *Let G be a split semisimple group over a number field k. Then the kernel of $\mathrm{H}^1(k,G) \to \prod_v \mathrm{H}^1(k_v,G)$ (where v runs over all places) is trivial.*

Proof. We have an exact sequence

$$1 \to \mu \to G_{sc} \to G \to 1$$

where G_{sc} is simply connected and μ is a finite subgroup of a split torus (i.e. a product of μ_n's). This sequence induces a long exact sequence in nonabelian cohomology. Let $\alpha \in \mathrm{H}^1(k,G)$ be a class with $\alpha_v = 1$ for all v. Since $\mathrm{H}^2(k,\mu) \to \prod_v \mathrm{H}^2(k_v,\mu)$ is injective by the Hasse principle for the Brauer group, we see that α lifts to a class $\beta \in \mathrm{H}^1(k,G_{sc})$. Since μ is a central subgroup of G_{sc}, any other lift of α is given by $\lambda\beta$, where $\lambda \in \mathrm{H}^1(k,\mu)$ is a cocycle. We will show that we can choose λ so that $\lambda\beta$ is trivial. By the Hasse principle for simply connected groups [61, Theorem 6.6], the map $\mathrm{H}^1(k,G_{sc}) \to \prod_v \mathrm{H}^1(k_v,G_{sc})$ is injective. (This map is even bijective.) If v is a finite or complex place, then $\mathrm{H}^1(k_v,G_{sc})$ is trivial [63, Theorem 5.12.24(b)]. If v is real then $\beta_v \in \mathrm{H}^1(k_v,G_{sc})$ has trivial image in $\mathrm{H}^1(k_v,G)$ so comes from an element of $\mathrm{H}^1(k_v,\mu)$. Since $\mathrm{H}^1(k,\mu) \to \prod_{v\text{ real}} \mathrm{H}^1(k_v,\mu)$ is surjective (this follows from the case $\mu = \mu_n$), we may choose $\lambda \in \mathrm{H}^1(k,\mu)$ such that $\lambda_v\beta_v = 1$ for every real place v. This implies that $\lambda\beta$ is trivial, as required. $\square$

Corollary 6.4.2. *Let k be a number field and $b \in B^{\mathrm{rs}}(k)$. Let $\mathrm{Sel}_2 J_b$ be the 2-Selmer group of the abelian variety J_b/k. Then $\mathrm{Sel}_2 J_b \subset \mathrm{H}^1(k,J_b[2])$ is contained in the image of γ_b. Consequently, the injection η_b from Theorem 6.3.2 extends to an injection*

$$\mathrm{Sel}_2 J_b \hookrightarrow G(k) \backslash V_b(k).$$

Proof. We have a commutative diagram for every place v:

$$\begin{tikzcd}
J_b(k)/2J_b(k) \arrow[r, "\delta"] \arrow[d] & \mathrm{H}^1(k,J_b[2]) \arrow[r] \arrow[d] & \mathrm{H}^1(k,G) \arrow[d] \\
J_b(k_v)/2J_b(k_v) \arrow[r, "\delta_v"] & \mathrm{H}^1(k_v,J_b[2]) \arrow[r] & \mathrm{H}^1(k_v,G)
\end{tikzcd}$$

By Corollary 6.3.1 it suffices to prove that 2-Selmer elements in $\mathrm{H}^1(k, J_b[2])$ are killed under the composition $\mathrm{H}^1(k, J_b[2]) \xrightarrow{\sim} \mathrm{H}^1(k, Z_G(\kappa_b)) \to \mathrm{H}^1(k, G)$. By definition, an element of $\mathrm{Sel}_2 J_b$ consists of a class in $\mathrm{H}^1(k, J_b[2])$ whose restriction to $\mathrm{H}^1(k_v, J_b[2])$ lies in the image of δ_v for every place v. So by Theorem 6.3.2 the image of such an element in $\mathrm{H}^1(k_v, G)$ is trivial for every v. Proposition 6.4.1 completes the proof. $\square$

6.5 Reducible orbits and marked points

Recall from Definition 3.6.2 that an element of $V^{\mathrm{rs}}(k)$ is k-reducible if it is $G(k)$-conjugate to a Kostant section. Recall from §3.7 that $\infty_1, \dots, \infty_m$ denote the set of marked points of $C \to B$.

Proposition 6.5.1. *Let $k/\mathbb{Q}$ be a field and $b \in B^{\mathrm{rs}}(k)$. Then the image under $\eta_b \colon J_b(k)/2J_b(k) \hookrightarrow G(k)\backslash V_b(k)$ of the subgroup of $J_b(k)/2J_b(k)$ generated by $\{\infty_2 - \infty_1, \dots, \infty_m - \infty_1\}$ coincides with the set of k-reducible $G(k)$-orbits of $V_b(k)$. Moreover, the set of k-reducible $G(k)$-orbits has the maximal size 2^{m-1} if and only if the inclusion $Z_G(\kappa_b) \subset Z_{H^\theta}(\kappa_b)$ is surjective on k-points.*

Proof. The proof is very similar to [71, Lemma 2.11]. Let K be an algebraic closure of k. For a scheme X/k we write $\mathrm{H}_1(X, \mathbb{F}_2) := \mathrm{Hom}(\mathrm{H}^1_{et}(X_K, \mathbb{F}_2), \mathbb{F}_2)$, where H^1_{et} denotes étale cohomology. We have an exact sequence of étale homology groups

$$1 \to \mu_2^m/\Delta(\mu_2) \to \mathrm{H}_1(C_b^\circ, \mathbb{F}_2) \to \mathrm{H}_1(C_b, \mathbb{F}_2) \to 1. \tag{6.5.1}$$

Let $H_{sc} \to H$ be the simply connected cover of H and let $C_{H_{sc}}$ be the centre of H_{sc}. By [83, Theorem 4.10], the sequence (6.5.1) is isomorphic to

$$1 \to C_{H_{sc}}[2] \to Z_{H_{sc}^\theta}(\kappa_b) \to Z_G(\kappa_b) \to 1. \tag{6.5.2}$$

It follows that the duals of these sequences are also isomorphic. We will calculate these duals and their connecting maps in Galois cohomology.

The dual of (6.5.1) is isomorphic to

$$1 \to J_b[2] \to \mathrm{H}^1_{et}(C_{b,K}^\circ, \mathbb{F}_2) \to (\mu_2^m)_{\Sigma=0} \to 1. \tag{6.5.3}$$

Here we use the identification $J_b[2] = \mathrm{H}^1_{et}(C_{b,K}, \mathbb{F}_2)$, and $(\mu_2^m)_{\Sigma=0}$ denotes the subset of μ_2^m of elements summing to zero. An explicit calculation shows that the image of the connecting map $(\mu_2^m)_{\Sigma=0}(k) \to \mathrm{H}^1(k, J_b[2])$ coincides with the image of the subgroup of $J_b(k)/2J_b(k)$ generated by $\{\infty_2 - \infty_1, \dots, \infty_m - \infty_1\}$ under the 2-descent map $J_b(k)/2J_b(k) \hookrightarrow \mathrm{H}^1(k, J_b[2])$.

On the other hand, we claim that the dual of (6.5.2) is isomorphic to

$$1 \to Z_G(\kappa_b) \to Z_{H^\theta}(\kappa_b) \to \pi_0(H^\theta) \to 1. \tag{6.5.4}$$

Indeed, the identification of the first two terms follows from [83, Corollary 2.9] and the existence of a nondegenerate pairing on $Z_G(\kappa_b)$ [83, Corollary 2.12]. It follows from Lemma 3.3.4 that we may identify the last term with $\pi_0(H^\theta)$. Next, we claim that the image of the connecting map $\pi_0(H^\theta) \to \mathrm{H}^1(k, Z_G(\kappa_b))$ coincides with the image of the k-reducible orbits in $V_b(k)$ under the map $G(k)\backslash V_b(k) \hookrightarrow \mathrm{H}^1(k, Z_G(\kappa_b))$ from Lemma 2.4.2. Indeed, consider the commutative diagram

$$\begin{tikzcd}
G(k)\backslash V_b(k) \arrow[r] \arrow[d, hook] & H^\theta(k)\backslash V_b(k) \arrow[d, hook] \\
\mathrm{H}^1(k, Z_G(\kappa_b)) \arrow[r] & \mathrm{H}^1(k, Z_{H^\theta}(\kappa_b))
\end{tikzcd}$$

where the horizontal maps are induced by the inclusions $G \subset H^\theta$ and $Z_G(\kappa_b) \subset Z_{H^\theta}(\kappa_b)$, and the vertical maps arise from Lemma 2.4.2. It follows from Corollary 3.3.2 that the map $\mathrm{H}^1(k, G) \to \mathrm{H}^1(k, H^\theta)$ has trivial pointed kernel. Moreover all k-reducible elements in $V_b(k)$ are $H^\theta(k)$-conjugate by Proposition 3.5.1. Therefore the set of k-reducible $G(k)$-orbits corresponds to the kernel of $\mathrm{H}^1(k, Z_G(\kappa_b)) \to \mathrm{H}^1(k, Z_{H^\theta}(\kappa_b))$ which, using (6.5.4), coincides with the image of the map $\pi_0(H^\theta) \to \mathrm{H}^1(k, Z_G(\kappa_b))$. This proves the claim and the first part of the proposition.

To prove the remaining part, note that there are 2^{m-1} k-reducible orbits if and only if the map $(\mu_2^m)_{\Sigma=0}(k) \to \mathrm{H}^1(k, J_b[2])$ is injective. By considering the long exact sequences associated to the isomorphic sequences (6.5.3) and (6.5.4), this is equivalent to the surjectivity of $\mathrm{H}^0(k, Z_G(\kappa_b)) \to \mathrm{H}^0(k, Z_{H^\theta}(\kappa_b))$. □

Chapter 7

Integral representatives

In this chapter we introduce integral structures for G and V and prove that for large primes p, the image of the map from Theorem 6.3.2 applied to $R = \mathbb{Q}_p$ lands in the orbits which admit a representative in $\mathbb{Z}_p$. See Theorem 7.2.4 for a precise statement. In §7.6, we deduce an integrality result for orbits over $\mathbb{Q}$ (as opposed to orbits over $\mathbb{Q}_p$).

7.1 Integral structures

So far we have considered properties of the pair (G,V) over $\mathbb{Q}$. In this subsection we define these objects over $\mathbb{Z}$.

Indeed, the pinning of H chosen in §3.1 extends to a Chevalley basis of $\mathfrak{h}$ (in the sense of [22, §1.2]), hence a $\mathbb{Z}$-form $\underline{\mathfrak{h}}$. This determines a $\mathbb{Z}$-form $\mathfrak{g} \cap \underline{\mathfrak{h}}$ of $\mathfrak{g}$, and the $\mathbb{Z}$-lattice $\underline{V} = V \cap \underline{\mathfrak{h}}$ is admissible [22, Definition 2.2] with respect to this form (the admissibility follows from [22, Proposition 2.6]). Define $\underline{G}$ as the Zariski closure of G in $\mathrm{GL}(\underline{V})$. The $\mathbb{Z}$-group scheme $\underline{G}$ has generic fibre G and acts faithfully on the free $\mathbb{Z}$-module $\underline{V}$.

Let $\underline{H}$ be the unique split reductive group over $\mathbb{Z}$ extending H. The automorphism $\theta\colon H \to H$ extends by the same formula to an automorphism $\underline{H} \to \underline{H}$, still denoted by θ.

Lemma 7.1.1. *1. $\underline{G}$ is a split reductive group over $\mathbb{Z}$.*

2. The equality $(H^\theta)^\circ = G$ extends to an isomorphism $(\underline{H}^\theta_{\mathbb{Z}[1/2]})^\circ \simeq \underline{G}_{\mathbb{Z}[1/2]}$, where $(\underline{H}^\theta_{\mathbb{Z}[1/2]})^\circ$ is the relative identity component of $\underline{H}^\theta_{\mathbb{Z}[1/2]}$.

Proof. For the first claim, since G is $\mathbb{Q}$-split it suffices to prove that $\underline{G} \to \operatorname{Spec}\mathbb{Z}$ is smooth and affine and that its geometric fibres are connected reductive groups. But $\underline{G}$ is $\mathbb{Z}$-flat and affine by construction, and its geometric fibres are reductive by [22, §4.3] hence smooth. The second claim follows from the fact that $(\underline{H}^\theta_{\mathbb{Z}[1/2]})^\circ$ is a reductive group scheme of the same type as $\underline{G}_{\mathbb{Z}[1/2]}$, which follows from [30, Remark 3.1.5]. $\square$

Recall from §3.7 that we have fixed polynomials $p_{d_1},\dots,p_{d_r} \in \mathbb{Q}[V]^G$ satisfying the conclusions of Proposition 3.7.1. Note that those conclusions are invariant under the $\mathbb{G}_m$-action on B. By rescaling the polynomials p_{d_i} using this $\mathbb{G}_m$-action, we can assume they lie in $\mathbb{Z}[\underline{V}]^{\underline{G}}$. We may additionally assume that the discriminant Δ from §4.1 lies in $\mathbb{Z}[\underline{V}]^{\underline{G}}$. Define $\underline{B} := \operatorname{Spec}\mathbb{Z}[p_{d_1},\dots,p_{d_r}]$ and $\underline{B}^{\mathrm{rs}} := \underline{B}[\Delta^{-1}]$. Taking invariants defines a map $\pi\colon \underline{V} \to \underline{B}$.

We extend the family of curves given by the equation in Table 1.1 to the family $\underline{C} \to \underline{B}$ given by that same equation.

Proposition 7.1.2. *$\underline{G}$ has class number* 1*:* $G(\mathbb{A}^\infty) = G(\mathbb{Q})\underline{G}(\widehat{\mathbb{Z}})$.

Proof. The group $\underline{G}$ is the Zariski closure of G in $\mathrm{GL}(\underline{V})$ and in a suitable basis of $\underline{V}$, G contains a maximal $\mathbb{Q}$-split torus consisting of diagonal matrices in $\mathrm{GL}(V)$. Therefore $\underline{G}$ has class number 1 by [61, Theorem 8.11; Corollary 2] and the fact that $\mathbb{Q}$ has class number one. $\square$

7.2 Spreading out

Our constructions and theorems for (G,V) of the previous chapters will continue to be valid over $\mathbb{Z}[1/N]$ for some appropriate choice of integer N, in a sense we will now explain.

Let us call a positive integer N *admissible* if the following properties are satisfied (set $S := \mathbb{Z}[1/N]$):

1. Each prime dividing the order of the Weyl group of H is a unit in S. (In particular, 2 is a unit in S.)

2. The zero locus $\underline{D}_S \to \operatorname{Spec} S$ of the discriminant Δ is flat and its smooth locus $\underline{D}^1_S$ coincides with the regular locus of $\underline{D}_S$. Moreover, the nonsmooth locus of $\underline{D}_S \to \operatorname{Spec} S$ is flat over $\operatorname{Spec} S$.

3. The morphism $\underline{C}_S \to \underline{B}_S$ is smooth exactly above $\underline{B}^{\mathrm{rs}}_S$.

4. The affine curve $\underline{C}^\circ_S$ is a closed subscheme of $\underline{V}_S$ and the action map $\underline{G}_S \times \underline{C}^\circ_S \to \underline{V}_S$, $(g,x) \mapsto g\cdot x$ is smooth.

5. For a field k of characteristic not dividing N, $b \in \underline{D}^1(k)$ if and only if every semisimple lift $v \in \underline{V}_b(k)$ has centraliser $Z_H(v)$ of semisimple rank 1, if and only if the curve $\underline{C}_b$ has a unique nodal singularity. In that case, the curve $\underline{C}_b$ is geometrically integral.

6. There exists open subschemes $\underline{V}^{\mathrm{rs}} \subset \underline{V}^{\mathrm{reg}} \subset \underline{V}_S$ such that if $S \to k$ is a map to a field and $v \in \underline{V}(k)$ then v is regular if and only if $v \in \underline{V}^{\mathrm{reg}}(k)$ and v is regular semisimple if and

only if $v \in \underline{V}^{\mathrm{rs}}(k)$. Moreover, $\underline{V}^{\mathrm{rs}}$ is the open subscheme defined by the nonvanishing of the discriminant polynomial Δ in $\underline{V}_S$.

7. The morphism $\pi\colon \underline{V}_S \to \underline{B}_S$ is smooth exactly at $\underline{V}^{reg}$.

8. $S[\underline{V}]^{\underline{G}} = S[p_{d_1}, \dots, p_{d_r}]$. The Kostant section κ fixed in §3.7 extends to a section $\kappa\colon \underline{B}_S \to \underline{V}^{\mathrm{reg}}$ of π satisfying the following property: for any $b \in \underline{B}(\mathbb{Z}) \subset \underline{B}_S(S)$, we have $\kappa_{N\cdot b} \in \underline{V}(\mathbb{Z})$. Moreover, each $G(\mathbb{Q})$-orbit of Kostant sections has a representative which satisfies the same property.

9. Let $\underline{B}^1$ be the complement of the singular locus of $\underline{D}$ in $\underline{B}$. Then the action map $\underline{G}_S \times \underline{B}_S \to \underline{V}^{\mathrm{reg}}, (g,b) \mapsto g \cdot \kappa_b$ is étale and its image contains $\underline{V}^{reg}|_{\underline{B}^1_S}$.

10. Let $\underline{J}^1_S \to \underline{B}_S$ denote the relative generalised Jacobian of the family of integral curves $\underline{C}_S|_{\underline{B}^1_S} \to \underline{B}^1_S$ [23, §9.3, Theorem 1] and let $\underline{J}^{\mathrm{rs}}_S \to \underline{B}^{\mathrm{rs}}_S$ denote its restriction to $\underline{B}^{\mathrm{rs}}_S$. Let $\underline{Z}_S \to \underline{B}_S$ be the centraliser of the Kostant section κ in $\underline{G}_S$. Then there is an isomorphism $\underline{J}^{\mathrm{rs}}_S[2] \simeq \underline{Z}^{\mathrm{rs}}_S$ of finite étale group schemes over $\underline{B}^{\mathrm{rs}}_S$ whose restriction to B^{rs} is the isomorphism of Proposition 3.8.6. It extends to an isomorphism $\underline{J}^1_S[2] \simeq \underline{Z}^1_S$.

11. The B-scheme $\bar{J}$ constructed in §5 extends to a $\underline{B}_S$-scheme $\bar{\underline{J}}_S \to \underline{B}_S$ which is flat, projective, with geometrically integral fibres and whose restriction to $\underline{B}^{\mathrm{rs}}_S$ is isomorphic to $\underline{J}^{\mathrm{rs}}_S$. Moreover, $\bar{\underline{J}}_S \to S$ is smooth with geometrically integral fibres, and the smooth locus of the morphism $\bar{\underline{J}}_S \to \underline{B}_S$ is an open subscheme of $\bar{\underline{J}}_S$ whose complement is S-fibrewise of codimension at least two.

12. The G-torsor $T \to J^{\mathrm{rs}}$ from §6.2 extends using the same definition to a $\underline{G}_S$-torsor $\underline{T}_S \to \underline{J}^{\mathrm{rs}}_S$, and $\underline{T}_S$ is Zariski locally trivial.

It might be possible to construct an explicit admissible integer for every pair (G,V). We will content ourselves with the following:

Proposition 7.2.1. *There exists an admissible integer N.*

Proof. The proof is very similar to the proof of [48, Proposition 4.1]. It follows from the results of the previous chapters and the principle of spreading out [63, §3.2]. It suffices to treat every property individually. We only treat a few properties in detail, but refer in each case to the corresponding property over $\mathbb{Q}$.

1. Take N to be the product of all the primes dividing the Weyl group of H.

2. We first choose N large enough such that $\underline{D}_S \to \operatorname{Spec} S$ is flat. In that case, let $U^{sm} \subset \underline{D}_S$ be the smooth locus of $\underline{D}_S \to \operatorname{Spec} S$ and let $U^{reg} \subset \underline{D}_S$ be the regular locus of $\underline{D}_S$. Then both U^{sm} and U^{reg} are open subsets of $\underline{D}_S$ (for U^{reg} this uses the excellence of $\underline{D}_S$) which coincide over $\mathbb{Q}$. It follows that they must coincide over an open subset $S' \subset S$ by spreading out. By shrinking S', we may additionally suppose that the nonsmooth locus of $\underline{D}_{S'} \to \operatorname{Spec} S'$ is flat over $\operatorname{Spec} S'$.

3. We first choose an N such that $\underline{C}_S \to \underline{B}_S$ is flat and proper. The locus of $\underline{B}_S$ above which the morphism $\underline{C}_S \to \underline{B}_S$ is smooth is an open subscheme which coincides with the open subscheme $\underline{B}_S^{\mathrm{rs}}$ after base change to $\mathbb{Q}$ by Lemma 3.7.2. Again by spreading out, we can enlarge N such that these two open subschemes coincide over S.

4. Follows from the definition of C° in §3.7 and the smoothness of the action map $G \times C^\circ \to V$ (Proposition 3.7.1).

5. Follows from Theorem 4.4.1.

6. We will construct open subschemes $\underline{\mathfrak{h}}_S^{\mathrm{rs}} \subset \underline{\mathfrak{h}}_S^{\mathrm{reg}} \subset \underline{\mathfrak{h}}_S$ with similar properties; the subschemes $\underline{V}^{\mathrm{rs}} \subset \underline{V}^{\mathrm{reg}} \subset \underline{V}_S$ will be obtained by restricting them to $\underline{V}_S$. Let $Z \to \underline{\mathfrak{h}}$ be the universal centralizer of the adjoint action of $\underline{H}$ on $\underline{\mathfrak{h}}$, so $Z = Z_{\underline{H}}(\mathrm{Id}_{\underline{\mathfrak{h}}})$. If k is any field and $x \in \underline{\mathfrak{h}}(k)$ then by definition x is regular if and only if the dimension of Z_x equals $\operatorname{rank} H$. By [39, Théorème 13.1.3] and the fact that the dimension of a group scheme can be computed at the identity, the function $x \mapsto \dim Z_x$ is upper-semicontinuous on $\underline{\mathfrak{h}}$. So the locus $\underline{\mathfrak{h}}^{\mathrm{reg}}$ where the fibre has dimension $\operatorname{rank} H$ is an open subscheme of $\underline{\mathfrak{h}}$. Let $Z^{\mathrm{reg}} \to \underline{\mathfrak{h}}^{\mathrm{reg}}$ be the restriction of Z to $\underline{\mathfrak{h}}^{\mathrm{reg}}$. By [70, Remark 4.4.2], the morphism $Z_S^{\mathrm{reg}} \to \underline{\mathfrak{h}}_S^{\mathrm{reg}}$ is smooth for some N. In that case the locus $\underline{\mathfrak{h}}_S^{\mathrm{rs}}$ where the fibres are tori is an open subscheme of $\underline{\mathfrak{h}}_S^{\mathrm{reg}}$ [2, Exposé X; Corollaire 4.9], as required. The statement about the discriminant locus follows from spreading out.

7. Follows from Lemma 3.1.2.

8. Note that $\mathbb{Z}[\underline{V}]^{\underline{G}}$ is a finitely generated $\mathbb{Z}$-algebra by [74, Theorem 2] and the fact that $\underline{G}$ is reductive over $\mathbb{Z}$. Moreover it contains the subring $\mathbb{Z}[p_{d_1}, \dots, p_{d_r}]$. Since this inclusion of finitely generated $\mathbb{Z}$-algebras is an equality after tensoring with $\mathbb{Q}$, the same holds after tensoring with $\mathbb{Z}[1/N]$ for some N. The claim about the Kostant section follows from considering the denominators of the morphism $\kappa\colon B \to V$ and spreading out.

Property 9 follows from Propositions 3.6.1 and 4.2.4; Property 10 follows from Proposition 3.8.6 and Theorem 4.4.2; Property 11 follows from Theorem 5.3.5; finally Property 12 follows from Theorem 6.2.1. □

For the remainder of the thesis, we fix an admissible integer N and continue to write $S = \operatorname{Spec}\mathbb{Z}[1/N]$. Moreover, to simplify notation, we will drop the subscript $\underline{()}_S$ and write $G, V, B, J, C\dots$ for $\underline{G}_S, \underline{V}_S, \underline{B}_S, \underline{J}_S, \underline{C}_S \dots$.

Using these properties, we can extend our previous results to S-algebras rather than $\mathbb{Q}$-algebras. We mention in particular:

Proposition 7.2.2 (Analogue of Corollary 6.3.1)**.** *Let R be an S-algebra and $b \in B^{\mathrm{rs}}(R)$. Then we have a natural bijection of pointed sets:*

$$G(R)\backslash V_b(R) \simeq \ker\left(\mathrm{H}^1(R, J_b[2]) \to \mathrm{H}^1(R, G)\right). \tag{7.2.1}$$

Proposition 7.2.3 (Analogue of Theorem 6.3.2)**.** *Let R be a local S-algebra and $b \in B^{\mathrm{rs}}(R)$. Then there is an injective map*

$$\eta_b \colon J_b(R)/2J_b(R) \hookrightarrow G(R)\backslash V_b(R)$$

compatible with base change on R.

We are now ready to state the main theorem of this chapter whose proof will be given at the end of §7.5. Write $\mathscr{E}_p$ for the set of all $b \in \underline{B}(\mathbb{Z}_p)$ that lie in $B^{\mathrm{rs}}(\mathbb{Q}_p)$. It consists of those elements of $\underline{B}(\mathbb{Z}_p)$ of nonzero discriminant.

Theorem 7.2.4. *Let p be a prime not dividing N. Then for any $b \in \mathscr{E}_p$, the image of the map*

$$\eta_b \colon J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p) \to G(\mathbb{Q}_p)\backslash V_b(\mathbb{Q}_p)$$

from Theorem 6.3.2 is contained in the image of the map $V(\mathbb{Z}_p) \to G(\mathbb{Q}_p)\backslash V(\mathbb{Q}_p)$.

7.3 Some stacks

For technical purposes related to the proof of Theorem 7.2.4, we need to introduce some stacks relevant to our setup. This can be seen as an attempt to 'geometrise' the set of G-orbits of V, and allows for more flexibility in glueing and descent arguments. Hopefully we soothe the reader by mentioning that we will not need any serious properties of stacks, and we mainly think of them as collections of groupoids where one can glue objects suitably. All stacks introduced in this thesis are considered in the étale topology. Recall from §7.2 that we have fixed an admissible integer N and we have set $S = \mathbb{Z}[1/N]$.

Definition 7.3.1. *Let* $\mathsf{B}G = [\operatorname{Spec} S/G]$ *be the* classifying stack *of G. By definition, for any S-scheme X the groupoid $\mathsf{B}G(X)$ has as objects G-torsors over X. Morphisms are given by isomorphisms of G-torsors.*

Definition 7.3.2. *Let $\mathscr{M} = [G\backslash V]$ be the quotient stack of V by the natural G-action on V. By definition, for any S-scheme X an object of $\mathscr{M}(X)$ consists of a G-torsor $T \to X$ together with a G-equivariant morphism $\phi\colon T \to V$. A morphism between two objects (T,ϕ) and (T',ϕ') consists of an isomorphism $\alpha\colon T \to T'$ of G-torsors satisfying $\phi' \circ \alpha = \phi$.*

Finally, recall that $Z \to B$ denotes the centraliser of the Kostant section κ, an extension of the group scheme of Definition 3.8.1 to S. Consider the quotient stack $[B/Z]$, where Z acts trivially on B. For any B-scheme X, an X-point of $[B/Z](X)$ consists of a Z-torsor on X.

These stacks come with a few natural maps between them:

- $\mathscr{M} \to \mathsf{B}G$: sends a pair (T,ϕ) to the G-torsor T.
- $\mathscr{M} \to B$: sends a pair $(T \xrightarrow{\alpha} X, T \xrightarrow{\phi} V)$ to the unique morphism $X \xrightarrow{f} B$ fitting in the commutative diagram:

$$\begin{array}{ccc} T & \xrightarrow{\phi} & V \\ \big\downarrow{\scriptstyle\alpha} & & \big\downarrow{\scriptstyle\pi} \\ X & \xrightarrow{f} & B \end{array}$$

  (Here π denotes the invariant map, and the existence and uniqueness of f follows from étale descent.) We will often regard $\mathscr{M}$ as a stack over B. In particular, if $b \in B(X)$ is an X-point we write $\mathscr{M}_b$ for the pullback of $\mathscr{M}$ along this point; it is isomorphic to $[G\backslash V_b]$.

- $V \to \mathscr{M}$: sends an X-point $X \xrightarrow{v} V$ to $(G \times X, \phi_v)$, where $\phi_v\colon G \times X \to V$ sends (g,x) to $g \cdot v(x)$.
- There is a substack $[B/Z] \hookrightarrow \mathscr{M}$ obtained by 'twisting' the Kostant section. For any B-scheme X, its image consists of those elements of $\mathscr{M}$ that are étale locally conjugate to κ_b. (Or rather its image under $V \to \mathscr{M}$.)

If $\mathscr{G}$ is a groupoid, we write $\pi_0\mathscr{G}$ for its set[1] of isomorphism classes.

[1]Assuming it is a set, which will always be the case in this thesis.

Lemma 7.3.3. *Let b be an X-point of B. The map $V_b(X) \to \mathscr{M}_b(X)$ induces a bijection between the $G(X)$-orbits of $V_b(X)$ and elements of $\pi_0(\mathscr{M}_b(X))$ that map to the trivial element in $\pi_0(\mathsf{B}G(X))$.*

Proof. This follows formally from the definitions. Indeed, if $v, v' \in V_b(X)$ give rise to isomorphic elements $(G \times X, \phi_v)$ and $(G \times X, \phi_{v'})$ in $\mathscr{M}_b(X)$, then there exists an isomorphism $G \times X \xrightarrow{\sim} G \times X$ of G-torsors mapping ϕ_v to $\phi_{v'}$. Such an isomorphism is defined by multiplying an element of $G(X)$, so v and v' are $G(X)$-conjugate. The argument can be reversed, so we obtain an injection $G(X)\backslash V_b(X) \hookrightarrow \pi_0(\mathscr{M}_b(X))$. Since an object (T, ϕ) of $\mathscr{M}_b(X)$ is isomorphic to $(G \times X, \phi_v)$ for some $v \in V_b(X)$ if and only if T is the trivial torsor, we conclude. □

The next lemma can be interpreted as a categorical version of Corollary 6.3.1.

Lemma 7.3.4. *The inclusion $[B/Z] \hookrightarrow \mathscr{M}$ induces an isomorphism of stacks $[B^{\mathrm{rs}}/Z^{\mathrm{rs}}] \simeq \mathscr{M}^{\mathrm{rs}}$ over B^{rs}.*

Proof. It suffices to prove that for any B-scheme X and $b \in B^{\mathrm{rs}}(X)$, every two objects in $\mathscr{M}_b(X)$ are étale locally isomorphic. (For then every object will be étale locally isomorphic to the Kostant section.) By passing to an étale extension, we may assume that these objects map to the trivial element in $\pi_0(\mathsf{B}G(X))$. It therefore suffices to prove that every two elements of $V_b^{\mathrm{rs}}(X)$ are étale locally $G(X)$-conjugate. This is true, since $G \times B^{\mathrm{rs}} \to V^{\mathrm{rs}}$ is smooth and surjective so has sections étale locally; see Part 9 of §7.2. □

Let $\mathscr{M}^{reg} \subset \mathscr{M}$ be the open substack consisting of those objects (T, ϕ) of $\mathscr{M}(X)$ such that ϕ lands in the locus of regular elements V^{reg}, and all morphisms between them. Note that the map $[B/Z] \to \mathscr{M}$ factors through $\mathscr{M}^{\mathrm{reg}}$ by (a spreading out of) Part 2 of Proposition 3.6.1.

Lemma 7.3.5. *The inclusion $[B/Z] \hookrightarrow \mathscr{M}^{reg}$ induces an isomorphism of stacks $[B^1/Z^1] \simeq \mathscr{M}^{reg}|_{B^1}$ over B^1.*

Proof. By the same reasoning as the proof of Lemma 7.3.4, it suffices to prove that $G \times B^1 \to V^{1,reg}$ is smooth and surjective. This follows from Part 9 of §7.2, which is a spreading out of Propositions 3.6.1 and 4.2.4. □

The next useful lemma is a purity result for the stack $\mathscr{M}$.

Lemma 7.3.6. *Let X be a regular integral 2-dimensional scheme, let $U \subset X$ be an open subscheme whose complement is finite and let $b \in B(X)$. Then the restriction $\mathscr{M}_b(X) \to \mathscr{M}_{b|_U}(U)$ is an equivalence of categories.*

Proof. We will use the following fact [29, Lemme 2.1(iii)] repeatedly: if Y is an affine X-scheme of finite type, then restriction of sections $Y(X) \to Y(U)$ is bijective. To prove essential surjectivity, let $(T_U, T_U \xrightarrow{\phi_U} V_b)$ be an object of $\mathscr{M}_{b|_U}(U)$. By [29, Théoreme 6.13], the G-torsor $T_U \to U$ extends to a G-torsor T on X. By the fact above applied to $Y = V_b$, ϕ_U uniquely extends to a morphism $\phi\colon T \to V_b$. The uniqueness of ϕ guarantees that ϕ is G-equivariant. Since the scheme of isomorphisms $\mathrm{Isom}_{\mathscr{M}}(\mathscr{A}, \mathscr{A}')$ between two objects of $\mathscr{M}_b(X)$ is X-affine, fully faithfulness follows from the fact applied to this isomorphism scheme. □

7.4 Orbits of square-free discriminant

In this subsection we study orbits of square-free discriminant, which will be useful in the proof of Theorem 7.2.4 and in Chapter 9. For the remainder of §7.4, we fix a discrete valuation ring R with fraction field K, uniformiser π, residue field k and normalised discrete valuation $\mathrm{ord}_K : K^\times \twoheadrightarrow \mathbb{Z}$. We assume that the integer N fixed in §7.2 is a unit in R.

Lemma 7.4.1. *Suppose that $b \in B(R)$ satisfies $\mathrm{ord}_K(\Delta(b)) = 1$. Then $b_k \in D^1(k)$.*

Proof. We may assume that R is complete. Since $\Delta(b)$ reduces to $0 \in k$, we have $b_k \in D$. Since $\Delta(b)$ is a uniformiser of R, the quotient of the regular ring $\mathrm{H}^0(B_R, \mathscr{O}_{B_R}) = R[p_{d_1}, \dots, p_{d_r}]$ by the maximal ideal $(p_{d_1} - p_{d_1}(b), \dots, p_{d_r} - p_{d_r}(b), \Delta)$ is isomorphic to k. Therefore the elements $\{p_{d_1} - p_{d_1}(b), \dots, p_{d_r} - p_{d_r}(b), \Delta\}$ form a regular system of parameters at b_k. Hence $D_R = \mathrm{Spec}\, R[\{p_{d_i}\}]/(\Delta)$ is regular at b_k. We conclude that b_k is a regular point of D_R. To prove the lemma, it suffices to prove that the regular locus of D_R coincides with the smooth locus D^1_R of $D_R \to \mathrm{Spec}\, R$.

Indeed, let $Z \subset D$ be the nonsmooth locus of $D \to \mathrm{Spec}\, S$, which coincides with the nonregular locus of D and is S-flat by Part 2 of §7.2. Let Z' be the nonregular locus of D_R, which is closed by the excellence of R. Since taking the smooth locus commutes with base change, Z_R agrees with the nonsmooth locus of $D_R \to \mathrm{Spec}\, R$. It therefore suffices to show that $Z_R = Z'$. Since every smooth point of $D_R \to \mathrm{Spec}\, R$ is regular, $Z' \subset Z_R$. To prove the opposite inclusion, let L be the prime subfield of K, in other words the residue field of the image of $\mathrm{Spec}\, K \to \mathrm{Spec}\, S$. Since L is perfect, Z_L is the nonregular locus of D_L and every point of $D_L \setminus Z_L$ is geometrically regular. It follows that Z_K is the nonregular locus of D_K and so $Z_K = Z'_K$. Since Z is S-flat by assumption, Z_R is R-flat so Z_K is dense in Z_R. Since Z' contains the closure of $Z'_K = Z_K$ which is Z_R, we conclude that $Z_R \subset Z'$. □

Lemma 7.4.2. *Suppose that $b \in B(R)$ satisfies $\mathrm{ord}_K(\Delta(b)) = 1$. Then the scheme V_b is regular.*

Proof. The idea of the proof is to reduce the statement to $\mathfrak{sl}_2$; this will be achieved by a sequence of standard but somewhat technical reduction steps. Since regularity can be checked after étale extensions and completion, we may assume that R is complete and k is separably closed. By Lemma 7.4.1, $b_k \in D^1(k)$. Let $v \in V_b(k)$ be a semisimple element. Then the centraliser $Z_H(v)$ is a reductive group of semisimple rank one (Part 5 of §7.2).

We claim that there exists a lift $\tilde{v} \in V(R)$ of v such that $\tilde{v}_K \in V(K) \subset \mathfrak{h}(K)$ is semisimple and such that the group scheme $Z_H(\tilde{v}) \to \operatorname{Spec} R$ is smooth with connected fibres. Indeed, let $\mathfrak{c} \subset V_k$ be a Cartan subspace containing v (here we use the extension of Vinberg theory to positive characteristic of [51]). Let $x \in V(R)$ be a lift of some regular semisimple element in $\mathfrak{c}$. Then x_K is regular semisimple (this being an open condition) and its centraliser $\tilde{\mathfrak{c}} := \mathfrak{z}_{\mathfrak{h}}(x) \subset V_R$ is a Cartan subspace lifting $\mathfrak{c}$. Since k is separably closed, $\mathfrak{c}$ is a split Cartan subalgebra; since R is complete the same is true for $\tilde{\mathfrak{c}}$. We may therefore choose an element $\tilde{v} \in \tilde{\mathfrak{c}}$ lifting v that vanishes on the same roots of $\mathfrak{c}$ as v; this $\tilde{v}$ will satisfy the desired properties. The smoothness of the centraliser $L := Z_H(\tilde{v}) \to \operatorname{Spec} R$ follows from the fact that it coincides with the centraliser of a subtorus (of the form considered in [30, Lemma 4.1.3]) and that torus centralisers are smooth [30, Lemma 2.2.4]. The connectedness of the fibres follows from Lemma 2.1.2, whose proof continues to hold if the characteristic of k is not a torsion prime for $\mathfrak{h}$, which is weaker than our assumption that the order of the Weyl group is invertible in k (Part 1 of §7.2).

The involution $\theta\colon \mathfrak{h} \to \mathfrak{h}$ restricts to a stable involution of the Lie algebra $\mathfrak{l}$ of L by [83, Lemma 2.5]. We claim that the morphism of R-schemes $G \times \mathfrak{l}^{\theta=-1} \to V_R, (g,x) \mapsto g \cdot x$ is smooth. Since the domain and target are R-flat, it suffices to check this R-fibrewise [34, (I.7.4)]. This then follows from [83, Proposition 4.5] (noting that $X^1 = \mathfrak{l}^{\theta=-1}$ in this case), whose proof continues to hold when the characteristic of k does not divide the order of the Weyl group of H.

Let $\mathfrak{l} \xrightarrow{\pi_L} B_L := \mathfrak{l} /\!\!/ L$ be the GIT quotient and let $\phi\colon B_L \to B$ the map induced by the inclusion $\mathfrak{l} \subset \mathfrak{h}$. Since ϕ is étale at $\pi_L(v) \in B_L(k)$ (Lemma 2.1.3), the R-point $b \in B(R)$ uniquely lifts to an R-point $b_L \in B_L(R)$ satisfying $b_{L,k} = \pi_L(v)$. Since b_L is open in the fibre $\phi^{-1}(b)$, $\mathfrak{l}_{b_L} := \pi_L^{-1}(b_L)$ is an open subscheme of $\mathfrak{l} \cap \mathfrak{h}_b$. Using the previous paragraph, this implies that the action map $m\colon G \times \mathfrak{l}_{b_L}^{\theta=-1} \to V_b$ is smooth. We claim that m is also surjective. By Part 9 of §7.2, the image of m contains the set V_b^{reg} of regular elements (in the sense of Lie theory). The complement $V_b \setminus V_b^{reg}$ consists of the semisimple elements of the special fibre $V_{b,k}$. Since all such semisimple elements are $G(\bar{k})$-conjugate and since the image of m contains v, we conclude that m is surjective.

Since regularity is a smooth-local property [79, Tag 036D], the smooth surjective morphism m shows that it suffices to prove that $\mathfrak{l}_{b_L}^{\theta=-1}$ is a regular scheme. We now make $\mathfrak{l}$ more explicit. Since 2 is invertible in R and since L is reductive of semisimple rank 1, $\mathfrak{l} = Z(\mathfrak{l}) \oplus \mathfrak{l}^{der}$, where $Z(\mathfrak{l})$ and $\mathfrak{l}^{der}$ are the centre and the derived subalgebra of $\mathfrak{l}$ respectively. Since k is separably closed, $\mathfrak{l}^{der} \simeq \mathfrak{sl}_{2,R}$. We claim that any two stable involutions on $\mathfrak{l}$ are étale locally conjugate. Indeed, the subscheme of elements of L mapping one such involution to another is smooth, so to prove that it has sections étale locally we merely have to show it surjects on $\operatorname{Spec} R$, which follows from a spreading out of Lemma 2.3.2. (See [47, Proposition 5.6] for the proof of a similar statement.) Therefore we may assume that in the decomposition $\mathfrak{l} \simeq Z(\mathfrak{l}) \oplus \mathfrak{sl}_{2,R}$, θ corresponds to the standard stable involution $\operatorname{Ad}((1,-1))$ of $\mathfrak{sl}_{2,R}$ and to -1 on $Z(\mathfrak{l})$. Moreover if Δ_L denotes the discriminant polynomial of $\mathfrak{l}$ then $\Delta_L(b_L)$ equals $\Delta(b)$ up to a unit in R (Lemma 2.1.3). We may now calculate that $\mathfrak{l}_{b_L}^{\theta=-1}$ is isomorphic to the scheme $(xy = \Delta_L(b_L))$. This scheme is regular since $\Delta(b)$ and hence $\Delta_L(b_L)$ is a uniformiser of R. □

Lemma 7.4.3. *Let $b \in B(R)$ with $\operatorname{ord}_K(\Delta(b)) = 1$. Then C_b is regular and its geometric special fibre is integral and has a unique singularity, which is a node. Moreover, the group scheme $J_b^1 \to \operatorname{Spec} R$ (where J^1 is introduced in §4.3) is the Néron model of its generic fibre.*

Proof. By Lemma 7.4.2 the scheme V_b is regular. Moreover since C° is (the spreading out of) a transverse slice of the G-action on V, the map $G \times C_b^\circ \to V_b$ is smooth (Part 4 of §7.2). Since regularity is smooth-local, it follows that C_b° is a regular scheme. Since C_b is smooth in a Zariski neighbourhood of the marked points $\infty_{i,b}$, the scheme C_b is regular too. We have $b_k \in D^1(k)$ by Lemma 7.4.1. Therefore the special fibre C_{b_k} is geometrically integral and has a unique nodal singularity (Part 5 of §7.2). The claim about J_b^1 follows from the regularity of C_b and a result of Raynaud [23, §9.5, Theorem 1]. □

The next theorem is not necessary for the proof of Theorem 7.2.4, but completely determines the integral orbits in the case of square-free discriminant and will be useful in §8.10 and Chapter 9.

Theorem 7.4.4. *Let R be a discrete valuation ring in which N is a unit. Let $K = \operatorname{Frac} R$ and let $\operatorname{ord}_K : K^\times \twoheadrightarrow \mathbb{Z}$ be the normalised discrete valuation. Let $b \in B(R)$ and suppose that $\operatorname{ord}_K \Delta(b) \leq 1$. Then:*

1. *If $x \in V_b(R)$, then $Z_G(x)(K) = Z_G(x)(R)$.*
2. *The natural map $\alpha\colon G(R)\backslash V_b(R) \to G(K)\backslash V_b(K)$ is injective and its image contains $\eta_b\,(J_b(K)/2J_b(K))$.*
3. *If furthermore R is complete and has finite residue field then the image of α equals $\eta_b\,(J_b(K)/2J_b(K))$.*

Proof. If $\mathrm{ord}_K \Delta(b) = 0$, J_b is smooth and proper over R. Since $Z_G(x)$ is finite étale over R, the first part follows. By Proposition 7.2.2 and Lemma 7.4.5 below, α is injective. Proposition 7.2.3 and the equality $J_b(K) = J_b(R)$ implies that $\eta_b\colon J_b(K)/2J_b(K) \to G(K)\backslash V_b(K)$ factors through $G(R)\backslash V_b(R)$, so the second part follows. If R is complete and the residue field k is finite, the pointed sets $\mathrm{H}^1(R,G)$ and $\mathrm{H}^1(R,J_b)$ are trivial by [54, III.3.11(a)] and Lang's theorem. The third part then follows from the fact that the 2-descent map $J_b(R)/2J_b(R) \to \mathrm{H}^1(R,J_b[2])$ is an isomorphism.

We now assume that $\mathrm{ord}_K \Delta(b) = 1$. Then $b_k \in D^1(k)$ by Lemma 7.4.1. By Lemma 7.4.3, C_b/R is regular, has geometrically integral fibres and its special fibre has a unique nodal singularity. By the same lemma the group scheme J_b^1/R introduced in §4.3 is the Néron model of its generic fibre. Moreover we have an isomorphism $Z_b^1 \simeq J_b^1[2]$ of quasi-finite étale group schemes over R by Theorem 4.4.2 (or rather its spreading out, Part 10 of §7.2).

By Lemmas 7.4.2 and 3.1.2 (and the spreading out of the latter, Part 7 of §7.2) the scheme V_b is regular and the smooth locus of the morphism $V_b \to \mathrm{Spec}\, R$ coincides with the locus V_b^{reg} of regular elements of V_b (this time in the sense of Lie theory). Since a section of a morphism between regular schemes lands in the smooth locus [23, §3.1, Proposition 2], we see that $V_b(R) = V_b^{reg}(R)$. By Part 9 of §7.2, the morphism $G \times \mathrm{Spec}\, R \to V_b^{reg}, (g,b) \mapsto g \cdot \kappa_b$ is a torsor under the group scheme Z_b^1 from §4.2. By Lemma 2.4.2 we obtain a bijection of pointed sets

$$G(R)\backslash V_b(R) = G(R)\backslash V_b^{reg}(R) \simeq \ker(\mathrm{H}^1(R,J_b^1[2]) \to \mathrm{H}^1(R,G)). \tag{7.4.1}$$

We now prove the first part of the theorem. Since $x \in V_b^{reg}(R)$ is étale locally G-conjugate to κ_b by the previous paragraph, we may assume that $x = \kappa_b$. But then $Z_G(\kappa_b) = Z_b^1 \simeq J_b^1[2]$ and J_b^1 satisfies the Néron mapping property, so $J_b^1[2](R) = J_b^1[2](K)$.

To prove the remaining parts, note that the map $\mathrm{H}^1(R,J_b^1[2]) \to \mathrm{H}^1(K,J_b^1[2]))$ is injective (Lemma 7.4.5 below), so by (7.4.1) the map $G(R)\backslash V_b(R) \to G(K)\backslash V_b(K)$ is injective too. To show that the image of $G(R)\backslash V_b(R) \to G(K)\backslash V_b(K)$ contains $\eta_b\,(J_b(K)/2J_b(K))$, note that we have an exact sequence of smooth group schemes

$$0 \to J_b^1[2] \to J_b^1 \xrightarrow{\times 2} J_b^1 \to 0,$$

since J_b^1 has connected fibres. This implies the existence of a commutative diagram:

$$\begin{tikzcd} J_b^1(R)/2J_b^1(R) \arrow[r, "="] \arrow[d] & J_b(K)/2J_b(K) \arrow[d] \\ \mathrm{H}^1(R,J_b^1[2]) \arrow[r] & \mathrm{H}^1(K,J_b[2]) \end{tikzcd}$$

It therefore suffices to prove that every element in the image of the map $J_b^1(R)/2J_b^1(R) \to \mathrm{H}^1(R, J_b^1[2])$ has trivial image in $\mathrm{H}^1(R,G)$. This is true, since the pointed kernel of the map $\mathrm{H}^1(R,G) \to \mathrm{H}^1(K,G)$ is trivial (Proposition 2.5.3).

If R has finite residue field then [54, III.3.11(a)] and Lang's theorem imply that $\mathrm{H}^1(R,G) = \{1\}$. In this case the $G(R)$-orbits of $V_b(R)$ are in bijection with $\mathrm{H}^1(R, J_b^1[2])$ by (7.4.1). The triviality of $\mathrm{H}^1(R, J_b^1)$ (again by Lang's theorem) shows that $\mathrm{H}^1(R, J_b^1[2])$ is in bijection with $J_b^1(R)/2J_b^1(R) = J_b(K)/2J_b(K)$. This proves Part 3, completing the proof of the proposition. □

Lemma 7.4.5. *Let Γ be a quasi-finite étale commutative group scheme over* $\operatorname{Spec} R$. *Suppose that Γ is a Néron model of its generic fibre: for every étale extension $R \to R'$ of discrete valuation rings, we have $\Gamma(R') = \Gamma(\operatorname{Frac} R')$. Then the map $\mathrm{H}^1(R,\Gamma) \to \mathrm{H}^1(K,\Gamma)$ is injective.*

Proof. Let $j\colon \operatorname{Spec} K \to \operatorname{Spec} R$ denote the natural inclusion. Then the Néron mapping property translates into the equality of étale sheaves $j_*j^*\Gamma = \Gamma$. The map $\mathrm{H}^1(R,\Gamma) \to \mathrm{H}^1(K,\Gamma)$ is therefore injective because it is the first term in the five-term exact sequence associated to the Leray spectral sequence $\mathrm{H}^p(R, \mathrm{R}^q j_* j^*\Gamma) \Rightarrow \mathrm{H}^{p+q}(K,\Gamma)$. □

7.5 Proof of Theorem 7.2.4

In this section we use the results from §7.3 and §7.4 to complete the proof of Theorem 7.2.4. We will do this by deforming to the case of square-free discriminant, with the help of the following Bertini type theorem over $\mathbb{Z}_p$.

Proposition 7.5.1. *Let p be a prime number. Let $\mathscr{Y} \to \mathbb{Z}_p$ be a smooth, quasiprojective morphism of relative dimension $d \geq 1$ with geometrically integral fibres. Let $\mathscr{D} \subset \mathscr{Y}$ be an effective Cartier divisor. Assume that $\mathscr{Y}_{\mathbb{F}_p}$ is not contained in $\mathscr{D}$ (i.e. $\mathscr{D}$ is horizontal) and that $\mathscr{D}_{\mathbb{Q}_p}$ is reduced. Let $P \in \mathscr{Y}(\mathbb{Z}_p)$ be a section such that $P_{\mathbb{Q}_p} \notin \mathscr{D}_{\mathbb{Q}_p}$. Then there exists a closed subscheme $\mathscr{X} \hookrightarrow \mathscr{Y}$ containing the image of P satisfying the following properties.*

- *$\mathscr{X} \to \mathbb{Z}_p$ is smooth of relative dimension 1 with geometrically integral fibres.*
- *$\mathscr{X}_{\mathbb{F}_p}$ is not contained in $\mathscr{D}$ and the (scheme-theoretic) intersection $\mathscr{X}_{\mathbb{Q}_p} \cap \mathscr{D}_{\mathbb{Q}_p}$ is reduced.*

Proof. If $d = 1$ we can take $\mathscr{X} = \mathscr{Y}$ and there is nothing to prove. Thus for the rest of the proof we may assume that $d \geq 2$. Fix a locally closed embedding $\mathscr{Y} \subset \mathbb{P}^n_{\mathbb{Z}_p}$. We will induct on d by finding a suitable hypersurface section using Bertini theorems over $\mathbb{F}_p$ and $\mathbb{Q}_p$. Combining [62, Theorem 1.2] and [26, Theorem 1.1], there exists a hypersurface H in $\mathbb{P}^n_{\mathbb{F}_p}$

such that the (scheme-theoretic) intersection $\mathscr{Y}_{\mathbb{F}_p} \cap H$ is smooth, geometrically irreducible of codimension 1 in $\mathscr{Y}_{\mathbb{F}_p}$, contains the point $P_{\mathbb{F}_p}$ and is not contained in $\mathscr{D}$.

We will lift this hypersurface to a hypersurface in $\mathbb{P}^n_{\mathbb{Z}_p}$ with similar properties, as follows. Let M be the projective space over $\mathbb{Q}_p$ parametrizing hypersurfaces of degree $\deg H$ in $\mathbb{P}^n_{\mathbb{Q}_p}$ containing the point $P_{\mathbb{Q}_p}$. By the classical Bertini theorem over $\mathbb{Q}_p$, there exists an open dense subscheme U of M such that every hypersurface H' in U has the property that $H' \cap \mathscr{Y}_{\mathbb{Q}_p}$ is smooth, geometrically irreducible of codimension 1 and that $H' \cap \mathscr{D}_{\mathbb{Q}_p}$ is reduced. The subset of $M(\mathbb{Q}_p)$ whose reduction mod p is the hypersurface H is an open p-adic ball of $M(\mathbb{Q}_p)$. Consequently, it intersects $U(\mathbb{Q}_p)$ nontrivially. (Since an open p-adic ball in a projective $\mathbb{Q}_p$-space cannot be contained in a proper Zariski closed subscheme.) So there exists a hypersurface $\mathscr{H} \subset \mathbb{P}^n_{\mathbb{Z}_p}$ lifting H such that $\mathscr{H}_{\mathbb{Q}_p} \in U(\mathbb{Q}_p)$.

By [52, Theorem 22.6], the scheme $\mathscr{Y} \cap \mathscr{H}$ is flat over $\mathbb{Z}_p$. It follows that the scheme $\mathscr{Y} \cap \mathscr{H} \to \mathbb{Z}_p$ is smooth with geometrically integral fibres. By construction the special fibre of $\mathscr{Y} \cap \mathscr{H}$ is not contained in $\mathscr{D}$ and the generic fibre of $\mathscr{H} \cap \mathscr{D}$ is reduced. The proposition now follows by replacing $\mathscr{Y}$ by $\mathscr{Y} \cap \mathscr{H}$ and induction on the relative dimension of $\mathscr{Y} \to \mathbb{Z}_p$. $\square$

Recall that $\bar{J}$ denotes the compactified Jacobian introduced in §5, which has been spread out in §7.2 to a scheme over $\mathbb{Z}[1/N]$.

Corollary 7.5.2. *Let p be a prime not dividing N. Let $b \in B(\mathbb{Z}_p) \cap B^{\mathrm{rs}}(\mathbb{Q}_p)$ and $P \in J_b(\mathbb{Q}_p)$. Then there exists a morphism $\mathscr{X} \to \mathbb{Z}_p$ which is of finite type, smooth of relative dimension 1 and has geometrically integral fibres, together with a morphism $\mathscr{X} \to \bar{J}_{\mathbb{Z}_p}$ satisfying the following properties.*

1. *Let $\tilde{b}$ be the composition $\mathscr{X} \to \bar{J}_{\mathbb{Z}_p} \to B_{\mathbb{Z}_p}$. Then the discriminant of $\tilde{b}$, seen as a map $\mathscr{X} \to \mathbb{A}^1_{\mathbb{Z}_p}$, is square-free on the generic fibre of $\mathscr{X}$ and not identically zero on the special fibre.*
2. *There exists a section $x \in \mathscr{X}(\mathbb{Z}_p)$ such that the composition $\operatorname{Spec} \mathbb{Q}_p \xrightarrow{x_{\mathbb{Q}_p}} \mathscr{X} \to \bar{J}_{\mathbb{Z}_p}$ coincides with P.*

Proof. We apply Proposition 7.5.1 with $\mathscr{Y} = \bar{J}_{\mathbb{Z}_p}$. We define $\mathscr{D}$ to be the pullback of the discriminant locus $\{\Delta = 0\} \subset \underline{B}_{\mathbb{Z}_p}$ under the morphism $\bar{J}_{\mathbb{Z}_p} \to \underline{B}_{\mathbb{Z}_p}$. Since the latter morphism is proper, we can extend $P \in J_b(\mathbb{Q}_p)$ to an element of $\bar{J}_b(\mathbb{Z}_p)$, still denoted by P.

We claim that the triple $(\mathscr{Y}, \mathscr{D}, P)$ satisfies the assumptions of Proposition 7.5.1. Indeed, the properties of $\mathscr{Y}$ follow Part 11 of §7.2. Moreover $\mathscr{Y}_{\mathbb{F}_p}$ is not contained in $\mathscr{D}$ since Δ is nonzero mod p by Part 1 of §7.2. Since $\bar{J}_{\mathbb{Q}_p} \to \underline{B}_{\mathbb{Q}_p}$ is smooth outside a subset of codimension 2 in $\bar{J}_{\mathbb{Q}_p}$ and $\{\Delta = 0\}_{\mathbb{Q}_p} \subset B_{\mathbb{Q}_p}$ is reduced, the scheme $\mathscr{D}_{\mathbb{Q}_p}$ is reduced too. Finally, $P_{\mathbb{Q}_p} \notin \mathscr{D}_{\mathbb{Q}_p}$ since b has nonzero discriminant.

We obtain a closed subscheme $\mathscr{X} \hookrightarrow \bar{J}_{\mathbb{Z}_p}$ satisfying the conclusion of Proposition 7.5.1. Write $x \in \mathscr{X}(\mathbb{Z}_p)$ for the section corresponding to P and $\widetilde{b}$ for the restriction of $\bar{J}_{\mathbb{Z}_p} \to \underline{B}_{\mathbb{Z}_p}$ to $\mathscr{X}$. We claim that the pair $(\mathscr{X}, x)$ satisfies the conclusion of the corollary. This follows readily from Proposition 7.5.1, except perhaps the statement that the discriminant map $\mathscr{X} \to \mathbb{A}^1_{\mathbb{Z}_p}$ is square-free on the generic fibre. This statement is equivalent to the pullback of the discriminant locus $\{\Delta = 0\} \subset B_{\mathbb{Q}_p}$ along $\tilde{b}_{\mathbb{Q}_p} \colon \mathscr{X}_{\mathbb{Q}_p} \to B_{\mathbb{Q}_p}$ being reduced. Since this pullback is $\mathscr{X}_{\mathbb{Q}_p} \cap \mathscr{D}_{\mathbb{Q}_p}$ which is reduced by Proposition 7.5.1, the statement is true and the corollary follows. $\square$

Proof of Theorem 7.2.4. Choose a relative curve $\mathscr{X} \to \mathbb{Z}_p$, a map $\mathscr{X} \to \bar{J}_{\mathbb{Z}_p}$ and a section $x \in \mathscr{X}(\mathbb{Z}_p)$ satisfying the conclusions of Corollary 7.5.2, and let $\tilde{b}$ be the composition $\mathscr{X} \to \bar{J}_{\mathbb{Z}_p} \to B_{\mathbb{Z}_p}$. Recall that J^1 is an open subscheme of $\bar{J}$; let $\mathscr{X}^1$ denote the open subscheme of $\mathscr{X}$ landing in $J^1_{\mathbb{Z}_p}$.

We claim that the complement of $\mathscr{X}^1$ in $\mathscr{X}$ is a union of finitely many closed points. Indeed, by Lemma 7.4.3 and the fact that the discriminant of $\tilde{b}_{\mathbb{Q}_p}$ is square-free, the group scheme $J^1_{\tilde{b}_{\mathbb{Q}_p}} \to \mathscr{X}_{\mathbb{Q}_p}$ is a Néron model of its generic fibre. By the Néron mapping property, the section $\mathscr{X}_{\mathbb{Q}_p} \to \bar{J}^1_{\mathbb{Q}_p}$ must land in $J^1_{\mathbb{Q}_p}$. Since the discriminant of $\mathscr{X}$ is nonzero on the special fibre, it follows that $\mathscr{X}^1_{\mathbb{F}_p}$ is nonempty. Combining the last two sentences and the fact that $\mathscr{X}_{\mathbb{F}_p}$ is irreducible proves the claim.

To finish the proof, we will use the stacks introduced in §7.3. Pulling back the $J^1[2]$-torsor $J^1 \xrightarrow{\times 2} J^1$ along $\mathscr{X}^1 \to J^1$ and using the isomorphism $J^1[2] \simeq Z^1$, we obtain a Z^1-torsor on $\mathscr{X}^1$, which determines a point $\mathscr{X}^1 \to [B/Z]$. Postcomposing with the morphism $[B/Z] \hookrightarrow \mathscr{M}$ determines a morphism $\mathscr{X}^1 \to \mathscr{M}_{\tilde{b}}$. By Lemma 7.3.6 — and this is the key point — this morphism extends (uniquely) to a morphism $\mathscr{X} \to \mathscr{M}_{\tilde{b}}$. Precomposing with $x \in \mathscr{X}(\mathbb{Z}_p)$ defines an object $\mathscr{A}$ of $\mathscr{M}_b(\mathbb{Z}_p)$, whose $\mathbb{Q}_p$-fibre corresponds to $\eta_b(P)$ via Lemma 7.3.3. Since $\mathrm{H}^1(\mathbb{Z}_p, G) = \{1\}$ ([54, III.3.11(a)] and Lang's theorem), every G-torsor on $\operatorname{Spec}\mathbb{Z}_p$ is trivial, so again by Lemma 7.3.3 the object $\mathscr{A}$ of $\mathscr{M}_b(\mathbb{Z}_p)$ arises from an element of $V_b(\mathbb{Z}_p)$. This proves that $\eta_b(P)$ has a representative in $V_b(\mathbb{Z}_p)$, completing the proof. $\square$

7.6 Orbits over $\mathbb{Z}$

Recall that $\mathscr{E}_p = \underline{B}(\mathbb{Z}_p) \cap B^{\mathrm{rs}}(\mathbb{Q}_p)$ for all p. Define $\mathscr{E} := \underline{B}(\mathbb{Z}) \cap B^{\mathrm{rs}}(\mathbb{Q})$. We state the following corollary, whose proof is completely analogous to the proof of [72, Corollary 5.8] and uses the fact that $\underline{G}$ has class number 1 (Proposition 7.1.2).

Corollary 7.6.1. *Let $b_0 \in \mathscr{E}$. Then for each prime p dividing N we can find an open compact neighbourhood W_p of b_0 in $\mathscr{E}_p$ and an integer $n_p \geq 0$ with the following property. Let $M = \prod_{p|N} p^{n_p}$. Then for all $b \in \mathscr{E} \cap \left(\prod_{p|N} W_p\right)$ and for all $y \in \mathrm{Sel}_2(J_{M \cdot b})$, the orbit $\eta_{M \cdot b}(y) \in G(\mathbb{Q}) \backslash V_{M \cdot b}(\mathbb{Q})$ contains an element of $\underline{V}_{M \cdot b}(\mathbb{Z})$.*

This statement about integral representatives will be strong enough to obtain the main theorems in §8.

Chapter 8

Geometry-of-numbers

In this chapter we will apply the counting techniques of Bhargava to provide estimates for the integral orbits of bounded height in the representation $(\underline{G}, \underline{V})$. We will follow the arguments of [47, §6] very closely. We keep the notation from the previous chapters and continue to assume that H is not of type A_1.

8.1 Heights

Recall that $\underline{B} = \operatorname{Spec} \mathbb{Z}[p_{d_1}, \dots, p_{d_r}]$ and that $\pi : \underline{V} \to \underline{B}$ denotes the morphism of taking invariants. For any $b \in B(\mathbb{R})$ we define the *height* of b by the formula

$$\operatorname{ht}(b) := \sup_{1 \le i \le r} |p_i(b)|^{1/i}.$$

We define $\operatorname{ht}(v) = \operatorname{ht}(\pi(v))$ for any $v \in V(\mathbb{R})$. We have $\operatorname{ht}(\lambda \cdot b) = |\lambda| \operatorname{ht}(b)$ for all $\lambda \in \mathbb{R}$ and $b \in B(\mathbb{R})$. If A is a subset of $V(\mathbb{R})$ or $B(\mathbb{R})$ and $X \in \mathbb{R}_{>0}$ we write $A_{<X} \subset A$ for the subset of elements of height $< X$. For every such X, the set $\underline{B}(\mathbb{Z})_{<X}$ is finite.

The next lemma records a numerological fact, which implies that $\underline{B}(\mathbb{Z})_{<X}$ has order of magnitude $X^{\dim V}$.

Lemma 8.1.1. *We have $d_1 + \cdots + d_r = \dim_{\mathbb{Q}} V$.*

Proof. Recall from §3.1 that Φ_H denotes a root system of H. We prove the two equalities $d_1 + \cdots + d_r = \frac{1}{2}\#\Phi_H + \operatorname{rank} H = \dim V$. The first one is classical, see [24, Corollary 10.2.4]; the second one follows from [83, Lemma 2.21] applied to $x = 0$. $\square$

8.2 Measures on G

Let ω_G be a generator for the $\mathbb{Q}$-vector space of left-invariant top differential forms on $\underline{G}$ over $\mathbb{Q}$. It is well-defined up to an element of $\mathbb{Q}^\times$ and it determines Haar measures dg on $G(\mathbb{R})$ and $G(\mathbb{Q}_p)$ for each prime p.

Recall from §3.7 that m denotes the number of marked points of the family of curves $C \to B$.

Proposition 8.2.1. *The product* $\mathrm{vol}\,(\underline{G}(\mathbb{Z})\backslash\underline{G}(\mathbb{R}))\cdot\prod_p \mathrm{vol}\,(\underline{G}(\mathbb{Z}_p))$ *converges absolutely and equals* 2^m*, the Tamagawa number of* G*.*

Proof. Proposition 7.1.2 implies that the product equals the Tamagawa number $\tau(G)$ of G. By Proposition 3.4.1, the group G is semisimple and its fundamental group has order $2\#\pi_0(H^\theta)$; let $G_{sc} \to G$ be its simply connected cover. The proof of Proposition 6.5.1 (more precisely the isomorphism between (6.5.3) and (6.5.4)) shows that $\#\pi_0(H^\theta)$ has order 2^{m-1}. Now use the identities $\tau(G) = 2^m\tau(G_{sc})$ [57, Theorem 2.1.1] and $\tau(G_{sc}) = 1$ [50]. $\square$

We study the measure dg on $G(\mathbb{R})$ using the Iwasawa decomposition, after introducing some notation. Recall from §3.1 that we have fixed a maximal torus $T \subset H$ with set of roots Φ_H. Moreover we have fixed a Borel subgroup P containing T, which determines a root basis $S_H \subset \Phi_H$ and a set of positive roots Φ_H^+. Then T^θ is a maximal torus of G and P^θ a Borel subgroup of G [69, Lemma 5.1]. Let $\Phi_G = \Phi(G, T^\theta)$ be its set of roots, $S_G = \{b_1, \dots, b_k\}$ the corresponding root basis and $\Phi_G^\pm$ the subset of positive/negative roots. Fix, once and for all, a maximal compact subgroup $K \subset G(\mathbb{R})$. If N is the unipotent radical of P^θ we have a decomposition $P^\theta = T^\theta N \subset G$. Let $\bar{P} = T\bar{N} \subset G$ be the opposite Borel subgroup. Then the natural product maps

$$\bar{N}(\mathbb{R}) \times T^\theta(\mathbb{R})^\circ \times K \to G(\mathbb{R}),\ T^\theta(\mathbb{R})^\circ \times \bar{N}(\mathbb{R}) \times K \to G(\mathbb{R})$$

are diffeomorphisms. If $t \in T^\theta(\mathbb{R})$, let $\delta_G(t) = \prod_{\beta\in\Phi_G^-}\beta(t) = \det \mathrm{Ad}(t)|_{\mathrm{Lie}\,\bar{N}(\mathbb{R})}$. The following result follows from well-known properties of the Iwasawa decomposition; see [49, Chapter 3;§1].

Lemma 8.2.2. *Let* dt, dn, dk *be Haar measures on* $T^\theta(\mathbb{R})^\circ, \bar{N}(\mathbb{R}), K$ *respectively. Then the assignment*

$$f \mapsto \int_{t\in T^\theta(\mathbb{R})^\circ}\int_{n\in\bar{N}(\mathbb{R})}\int_{k\in K} f(tnk)\,dk\,dn\,dt = \int_{t\in T^\theta(\mathbb{R})^\circ}\int_{n\in\bar{N}(\mathbb{R})}\int_{k\in K} f(ntk)\delta_G(t)^{-1}\,dk\,dn\,dt$$

defines a Haar measure on $G(\mathbb{R})$*.*

We now fix Haar measures on the groups $T^\theta(\mathbb{R})^\circ, K$ and $\bar{N}(\mathbb{R})$, as follows. We give $T^\theta(\mathbb{R})^\circ$ the measure pulled back from the isomorphism $\prod_{\beta\in S_G}\beta\colon T^\theta(\mathbb{R})^\circ \to \mathbb{R}_{>0}^{\#S_G}$, where $\mathbb{R}_{>0}$ gets its standard Haar measure $d^\times\lambda = d\lambda/\lambda$. We give K the probability Haar measure. Finally we give $\bar{N}(\mathbb{R})$ the unique Haar measure dn such that the Haar measure on $G(\mathbb{R})$ from Lemma 8.2.2 coincides with dg.

8.3 Measures on V

Let ω_V be a generator of the free rank one $\mathbb{Z}$-module of left-invariant top differential forms on $\underline{V}$. Then ω_V is uniquely determined up to sign and it determines Haar measures dv on $V(\mathbb{R})$ and $V(\mathbb{Q}_p)$ for every prime p. We define the top form $\omega_B = dp_{d_1}\wedge\cdots\wedge dp_{d_r}$ on $\underline{B}$. It defines measures db on $B(\mathbb{R})$ and $B(\mathbb{Q}_p)$ for every prime p.

Lemma 8.3.1. *There exists a unique rational number $W_0 \in \mathbb{Q}^\times$ with the following property. Let $k/\mathbb{Q}$ be a field extension, let $\mathfrak{c}$ a Cartan subalgebra of $\mathfrak{h}_k$ contained in V_k, and let $\mu_{\mathfrak{c}}\colon G_k\times\mathfrak{c}\to V_k$ be the action map. Then $\mu_{\mathfrak{c}}^*\omega_V = W_0\omega_G\wedge\pi|_{\mathfrak{c}}^*\omega_B$.*

Proof. The proof is identical to that of [84, Proposition 2.13]. Here we use the fact that the sum of the invariants equals the dimension of the representation: $d_1+\cdots d_r = \dim_{\mathbb{Q}} V$ (Lemma 8.1.1). □

Lemma 8.3.2. *Let $W_0\in\mathbb{Q}^\times$ be the constant of Lemma 8.3.1. Then:*

1. *Let $\underline{V}(\mathbb{Z}_p)^{\mathrm{rs}} := \underline{V}(\mathbb{Z}_p)\cap V^{\mathrm{rs}}(\mathbb{Q}_p)$ and define a function $m_p : \underline{V}(\mathbb{Z}_p)^{\mathrm{rs}} \to \mathbb{R}_{\geq 0}$ by the formula*
$$m_p(v) = \sum_{v'\in \underline{G}(\mathbb{Z}_p)\backslash\left(G(\mathbb{Q}_p)\cdot v\cap\underline{V}(\mathbb{Z}_p)\right)} \frac{\#Z_{\underline{G}}(v')(\mathbb{Q}_p)}{\#Z_{\underline{G}}(v')(\mathbb{Z}_p)}. \tag{8.3.1}$$
Then m_p is locally constant.

2. *Let $\underline{B}(\mathbb{Z}_p)^{\mathrm{rs}} := \underline{B}(\mathbb{Z}_p)\cap B^{\mathrm{rs}}(\mathbb{Q}_p)$ and let $\psi_p : \underline{V}(\mathbb{Z}_p)^{\mathrm{rs}}\to\mathbb{R}_{\geq 0}$ be a bounded, locally constant function which satisfies $\psi_p(v) = \psi_p(v')$ when $v, v'\in\underline{V}(\mathbb{Z}_p)^{\mathrm{rs}}$ are conjugate under the action of $G(\mathbb{Q}_p)$. Then we have the formula*
$$\int_{v\in\underline{V}(\mathbb{Z}_p)^{\mathrm{rs}}}\psi_p(v)\mathrm{d}v = |W_0|_p\,\mathrm{vol}\left(\underline{G}(\mathbb{Z}_p)\right)\int_{b\in\underline{B}(\mathbb{Z}_p)^{\mathrm{rs}}}\sum_{g\in G(\mathbb{Q}_p)\backslash\underline{V}_b(\mathbb{Z}_p)}\frac{m_p(v)\psi_p(v)}{\#Z_{\underline{G}}(v)(\mathbb{Q}_p)}\mathrm{d}b. \tag{8.3.2}$$

Proof. The proof is identical to that of [71, Proposition 3.3], using Lemma 8.3.1. □

8.4 Fundamental sets

Let $K \subset G(\mathbb{R})$ be the maximal compact subgroup fixed in §8.2. For any $c \in \mathbb{R}_{>0}$, define $T_c := \{t \in T^\theta(\mathbb{R})^\circ \mid \forall \beta \in S_G, \beta(t) \leq c\}$. A *Siegel set* is, by definition, any subset $\mathfrak{S}_{\omega,c} := \omega \cdot T_c \cdot K$, where $\omega \subset \bar{N}(\mathbb{R})$ is a compact subset and $c > 0$.

Proposition 8.4.1. *1. For every $\omega \subset \bar{N}(\mathbb{R})$ and $c > 0$, the set*

$$\{\gamma \in \underline{G}(\mathbb{Z}) \mid \gamma \cdot \mathfrak{S}_{\omega,c} \cap \mathfrak{S}_{\omega,c} \neq \emptyset\}$$

is finite.

2. We can choose $\omega \subset \bar{N}(\mathbb{R})$ and $c > 0$ such that $\underline{G}(\mathbb{Z}) \cdot \mathfrak{S}_{\omega,c} = G(\mathbb{R})$.

Proof. The first part follows from the Siegel property [21, Corollaire 15.3]. By [61, Theorem 4.15], the second part is reduced to proving that $G(\mathbb{Q}) = P(\mathbb{Q}) \cdot \underline{G}(\mathbb{Z})$. This follows from [20, §6, Lemma 1(b)], using that (in the terminology of that paper) the lattice $\underline{V}$ is special with respect to the pinning $(T^\theta, P^\theta, \{X_\alpha\})$. $\square$

Now fix $\omega \subset \bar{N}(\mathbb{R})$ and $c > 0$ so that $\mathfrak{S}_{\omega,c}$ satisfies the conclusions of Proposition 8.4.1. By enlarging ω, we may assume that $\mathfrak{S}_{\omega,c}$ is semialgebraic. We drop the subscripts and for the remainder of §8 we write $\mathfrak{S}$ for this fixed Siegel set. The set $\mathfrak{S}$ will serve as a fundamental domain for the action of $\underline{G}(\mathbb{Z})$ on $G(\mathbb{R})$.

A $\underline{G}(\mathbb{Z})$-coset of $G(\mathbb{R})$ may be represented more than once in $\mathfrak{S}$, but by keeping track of the multiplicities this will not cause any problems. The surjective map $\varphi \colon \mathfrak{S} \to \underline{G}(\mathbb{Z}) \backslash G(\mathbb{R})$ has finite fibres and if $g \in \mathfrak{S}$ we define $\mu(g) := \#\varphi^{-1}(\varphi(g))$. The function $\mu \colon \mathfrak{S} \to \mathbb{N}$ is uniformly bounded by $\mu_{\max} := \#\{\gamma \in \underline{G}(\mathbb{Z}) \mid \gamma\mathfrak{S} \cap \mathfrak{S} \neq \emptyset\}$ and has semialgebraic fibres. By pushing forward measures via φ, we obtain the formula

$$\int_{g \in \mathfrak{S}} \mu(g)^{-1}\, dg = \operatorname{vol}\left(\underline{G}(\mathbb{Z}) \backslash G(\mathbb{R})\right). \tag{8.4.1}$$

We now construct special subsets of $V^{\mathrm{rs}}(\mathbb{R})$ which serve as our fundamental domains for the action of $G(\mathbb{R})$ on $V^{\mathrm{rs}}(\mathbb{R})$. By the same reasoning as in [84, §2.9], we can find open subsets $L_1, \ldots, L_k$ of $\{b \in B^{\mathrm{rs}}(\mathbb{R}) \mid \mathrm{ht}(b) = 1\}$ and sections $s_i \colon L_i \to V(\mathbb{R})$ of the map $\pi \colon V \to B$ satisfying the following properties:

- For each i, L_i is connected and semialgebraic and s_i is a semialgebraic map with bounded image.

- Set $\Lambda = \mathbb{R}_{>0}$. Then we have an equality

$$V^{\mathrm{rs}}(\mathbb{R}) = \bigcup_{i=1}^{k} G(\mathbb{R}) \cdot \Lambda \cdot s_i(L_i). \tag{8.4.2}$$

If $v \in s_i(L_i)$ let $r_i = \# Z_G(v)(\mathbb{R})$; this integer is independent of the choice of v. We record the following change-of-measure formula, which follows from Lemma 8.3.1.

Lemma 8.4.2. *Let $f\colon V(\mathbb{R}) \to \mathbb{C}$ be a continuous function of compact support and $i \in \{1, \ldots, k\}$. Let $G_0 \subset G(\mathbb{R})$ be a measurable subset and let $m_\infty(v)$ be the cardinality of the fibre of the map $G_0 \times \Lambda \times L_i \to V(\mathbb{R}), (g, \lambda, l) \mapsto g \cdot \lambda \cdot s_i(l)$ above $v \in V(\mathbb{R})$. Then*

$$\int_{v \in G_0 \cdot \Lambda \cdot s_i(L_i)} f(v) m_\infty(v)\, dv = |W_0| \int_{b \in \Lambda \cdot L_i} \int_{g \in G_0} f(g \cdot s_i(b))\, dg\, db,$$

where $W_0 \in \mathbb{Q}^\times$ is the scalar of Lemma 8.3.1.

8.5 Counting integral orbits of V

For any $\underline{G}(\mathbb{Z})$-invariant subset $A \subset \underline{V}(\mathbb{Z})$, define

$$N(A, X) := \sum_{v \in \underline{G}(\mathbb{Z}) \backslash A_{<X}} \frac{1}{\# Z_{\underline{G}}(v)(\mathbb{Z})}.$$

(Recall that $A_{<X}$ denotes the elements of A of height $< X$.) Let k be a field of characteristic not dividing N. We say an element $v \in V(k)$ with $b = \pi(v)$ is:

- *k-reducible* if $\Delta(b) = 0$ or if it is $G(k)$-conjugate to a Kostant section, and *k-irreducible* otherwise.
- *k-soluble* if $\Delta(b) \neq 0$ and v lies in the image of the map $\eta_b : J_b(k)/2J_b(k) \to G(k) \backslash V_b(k)$ of Proposition 7.2.3.

For any $A \subset \underline{V}(\mathbb{Z})$, write $A^{irr} \subset A$ for the subset of $\mathbb{Q}$-irreducible elements. Write $V(\mathbb{R})^{sol} \subset V(\mathbb{R})$ for the subset of $\mathbb{R}$-soluble elements. Write g for the common arithmetic genus of the curves $C \to B$.

Theorem 8.5.1. *We have*

$$N(\underline{V}(\mathbb{Z})^{irr} \cap V(\mathbb{R})^{sol}, X) = \frac{|W_0|}{2^g} \operatorname{vol}(\underline{G}(\mathbb{Z}) \backslash G(\mathbb{R})) \operatorname{vol}(B(\mathbb{R})_{<X}) + o\left(X^{\dim V}\right),$$

where $W_0 \in \mathbb{Q}^\times$ is the scalar of Lemma 8.3.1.

We first explain how to reduce Theorem 8.5.1 to Proposition 8.5.2. Recall that there exists $\mathbb{G}_m$-actions on V and B such that the morphism $\pi : V \to B$ is $\mathbb{G}_m$-equivariant and that we write $\Lambda = \mathbb{R}_{>0}$. By an argument identical to [48, Lemma 5.5], the subset $V(\mathbb{R})^{sol} \subset V^{\mathrm{rs}}(\mathbb{R})$ is open and closed in the Euclidean topology. Therefore by discarding some of the subsets $L_1, \dots, L_k$ of §8.4, we may write $V(\mathbb{R})^{sol} = \bigcup_{i \in J} G(\mathbb{R}) \cdot \Lambda \cdot s_i(L_i)$ for some $J \subset \{1, \dots, k\}$. Moreover for every $b \in B^{\mathrm{rs}}(\mathbb{R})$ we have equalities

$$\#\left(G(\mathbb{R})\backslash V_b(\mathbb{R})^{sol}\right)/\#Z_G(\kappa_b)(\mathbb{R}) = \#\left(J_b(\mathbb{R})/2J_b(\mathbb{R})\right)/\#J_b[2](\mathbb{R}) = 1/2^g,$$

where the first follows from the definition of $\mathbb{R}$-solubility and Proposition 3.8.6, and the second is a general fact about real abelian varieties. Therefore by the inclusion-exclusion principle, to prove Theorem 8.5.1 it suffices to prove the following proposition.

For any subset I of $\{1, \dots, k\}$, write $L_I = \pi\left(\cap_{i \in I} G(\mathbb{R}) \cdot s_i(L_i)\right)$. Write s_I for the restriction of s_i to L_I and write $r_I = r_i$ for some choice of $i \in I$. (The section s_I may depend on i but the number r_I does not if L_I is nonempty.)

Proposition 8.5.2. *In the above notation, let (L, s, r) be (L_I, s_I, r_I) for some $I \subset \{1, \dots, k\}$. Then*

$$N(G(\mathbb{R}) \cdot \Lambda \cdot s(L) \cap \underline{V}(\mathbb{Z})^{irr}, X) = \frac{|W_0|}{r} \mathrm{vol}\left(\underline{G}(\mathbb{Z})\backslash G(\mathbb{R})\right) \mathrm{vol}((\Lambda \cdot L)_{<X}) + o\left(X^{\dim V}\right).$$

So to prove Theorem 8.5.1 it remains to prove Proposition 8.5.2. For the latter we will follow the general orbit-counting techniques established by Bhargava, Shankar and Gross [16, 9] closely. The only notable differences are that we work with a Siegel set instead of a true fundamental domain and that we have to carry out a case-by-case analysis for cutting off the cusp in §8.11. For the remainder of §8 we fix a triple (L, s, r) as above with $L \neq \emptyset$.

8.6 First reductions

We first reduce Proposition 8.5.2 to estimating the number of (weighted) lattice points in a region of $V(\mathbb{R})$. Recall that $\mathfrak{S}$ denotes the Siegel set fixed in §8.4 which comes with a multiplicity function $\mu \colon \mathfrak{S} \to \mathbb{N}$. Because $\underline{G}(\mathbb{Z}) \cdot \mathfrak{S} = G(\mathbb{R})$, every element of $G(\mathbb{R}) \cdot \Lambda \cdot s(L)$ is $\underline{G}(\mathbb{Z})$-equivalent to an element of $\mathfrak{S} \cdot \Lambda \cdot s(L)$. In fact, we can be more precise about how often a $\underline{G}(\mathbb{Z})$-orbit will be represented in $\mathfrak{S} \cdot \Lambda \cdot s(L)$. Let $\nu \colon \mathfrak{S} \cdot \Lambda \cdot s(L) \to \mathbb{R}_{>0}$ be the 'weight' function defined by

$$x \mapsto \nu(x) := \sum_{\substack{g \in \mathfrak{S} \\ x \in g \cdot \Lambda \cdot s(L)}} \mu(g)^{-1}. \tag{8.6.1}$$

Then ν takes only finitely many values and has semialgebraic fibres. We now claim that if every element of $\mathfrak{S} \cdot \Lambda \cdot s(L)$ is weighted by ν, then the $\underline{G}(\mathbb{Z})$-orbit of an element $x \in G(\mathbb{R}) \cdot \Lambda \cdot s(L)$ is represented exactly $\#Z_G(x)(\mathbb{R})/\#Z_{\underline{G}}(x)(\mathbb{Z})$ times. More precisely, for any $x \in G(\mathbb{R}) \cdot \Lambda \cdot s(L)$ we have

$$\sum_{x' \in \underline{G}(\mathbb{Z}) \cdot x \cap \mathfrak{S} \cdot \Lambda \cdot s(L)} \nu(x') = \frac{\#Z_G(x)(\mathbb{R})}{\#Z_{\underline{G}}(x)(\mathbb{Z})}. \tag{8.6.2}$$

Indeed, suppose that $x = g \cdot x_L$ with $g \in \mathfrak{S}$ and $x_L \in \Lambda \cdot s(L)$. Then for any $g' \in G(\mathbb{R})$, $g'x_L$ is $\underline{G}(\mathbb{Z})$-conjugate to x if and only if g and g' represent the same element in the double coset

$$\underline{G}(\mathbb{Z}) \backslash G(\mathbb{R}) / Z_G(x_L)(\mathbb{R}).$$

This implies that the left-hand-side of (8.6.2) equals the sum of $\mu(g')^{-1}$ over all $g' \in \mathfrak{S}$ which represent the same element as g in this double coset. Now consider the natural maps

$$\mathfrak{S} \xrightarrow{\varphi} \underline{G}(\mathbb{Z}) \backslash G(\mathbb{R}) \xrightarrow{\psi} \underline{G}(\mathbb{Z}) \backslash G(\mathbb{R}) / Z_G(x_L)(\mathbb{R}).$$

The left-hand-side of (8.6.2) equals the cardinality of $\psi^{-1}(g)$ by definition of μ. By the orbit-stabiliser lemma, $\#\psi^{-1}(g)$ equals $\#Z_G(x)(\mathbb{R})/\#Z_{\underline{G}}(x)(\mathbb{Z})$, proving (8.6.2).

In conclusion, for any $\underline{G}(\mathbb{Z})$-invariant subset $A \subset \underline{V}(\mathbb{Z}) \cap G(\mathbb{R}) \cdot \Lambda \cdot s(L)$ we have

$$N(A, X) = \frac{1}{r} \# [A \cap (\mathfrak{S} \cdot \Lambda \cdot s(L))_{<X}], \tag{8.6.3}$$

with the caveat that elements on the right-hand side are weighted by ν. (Recall that $r = \#Z_G(v)(\mathbb{R})$ for some $v \in s(L)$.)

8.7 Averaging and counting lattice points

We consider an averaged version of (8.6.3) and obtain a useful expression for $N(A, X)$ (Lemma 8.7.1) using a trick due to Bhargava. Then we use this expression to count orbits lying in the 'main body' of V using geometry-of-numbers techniques, see Proposition 8.7.4.

Fix a compact, semialgebraic subset $G_0 \subset G(\mathbb{R}) \times \Lambda$ of nonempty interior, that in addition satisfies $K \cdot G_0 = G_0$, $\mathrm{vol}(G_0) = 1$ and the projection of G_0 onto Λ is contained in $[1, K_0]$ for some $K_0 > 1$. Moreover we suppose that G_0 is of the form $G_0' \times [1, K_0]$ where G_0' is a subset of $G(\mathbb{R})$. Equation (8.6.3) still holds when L is replaced by hL for any $h \in G(\mathbb{R})$, by the same argument given above. Thus for any $\underline{G}(\mathbb{Z})$-invariant $A \subset \underline{V}(\mathbb{Z}) \cap G(\mathbb{R}) \cdot \Lambda \cdot s(L)$ we obtain

$$N(A,X) = \frac{1}{r} \int_{h \in G_0} \#[A \cap (\mathfrak{S} \cdot \Lambda \cdot hs(L))_{<X}]\, dh. \tag{8.7.1}$$

We use Equation (8.7.1) to *define* $N(A,X)$ for any subset $A \subset \underline{V}(\mathbb{Z}) \cap G(\mathbb{R}) \cdot \Lambda \cdot s(L)$ which is not necessarily $\underline{G}(\mathbb{Z})$-invariant.

For any subset A, the integral on the right-hand side of (8.7.1) equals by definition:

$$\int_{h \in G_0} \#\{\nu\text{-weighted elements of } A \cap (\mathfrak{S} \cdot \Lambda \cdot hs(L))_{<X}\}\, dh = \sum_{x \in A_{<X}} \int_{h \in G_0} \sum_{\substack{g \in \mathfrak{S} \\ x \in g\Lambda hs(L)}} \mu(g)^{-1}\, dh. \tag{8.7.2}$$

Let $x \in A_{<X}$ and let $x_L \in s(L)$ be the unique point that is $(G(\mathbb{R}) \times \Lambda)$-conjugate to x. There exists a finite number of elements $(g_1, \lambda_1), \ldots, (g_m, \lambda_m) \in G(\mathbb{R}) \times \Lambda$ satisfying $x = g_i \lambda_i \cdot x_L$. We have $x \in g\lambda hs(L)$ if and only if $gh\lambda = g_i \lambda_i$ for some i. Therefore the summand on the right-hand side of (8.7.2) corresponding to x equals

$$\int_{h \in G_0} \sum_{i=1}^{m} \#\{(g,\lambda) \in \mathfrak{S} \times \Lambda \mid g = g_i h^{-1} \lambda_i \lambda^{-1}\} \mu(g_i h^{-1})^{-1}\, dh = \sum_{i=1}^{m} \int_{h \in G_0 \cap (\mathfrak{S}^{-1} g_i \times \Lambda)} \mu(g_i h^{-1})^{-1}\, dh. \tag{8.7.3}$$

(Here we define $\mu((g,\lambda)) := \mu(g)$ if $(g,\lambda) \in \mathfrak{S} \times \Lambda$.) Since the Haar measure on $G(\mathbb{R}) \times \Lambda$ is unimodular, the transformation $h \mapsto g_i h^{-1}$ is measure preserving. So the right-hand side of (8.7.3) equals

$$\sum_{i=1}^{m} \int_{g \in g_i G_0^{-1} \cap (\mathfrak{S} \times \Lambda)} \mu(g)^{-1}\, dh = \sum_{i=1}^{m} \int_{g \in \mathfrak{S} \times \Lambda} \#\{h \in G_0 \mid gh = g_i \lambda_i\} \mu(g)^{-1}\, dh.$$

Since $gh = g_i \lambda_i$ if and only if $x = gh \cdot x_L$, we conclude that for any subset $A \subset \underline{V}(\mathbb{Z}) \cap G(\mathbb{R}) \cdot \Lambda \cdot s(L)$ we have

$$N(A,X) = \frac{1}{r} \int_{g \in \mathfrak{S} \times \Lambda} \#[A \cap (gG_0 \cdot s(L))_{<X}]\, \mu(g)^{-1}\, dg, \tag{8.7.4}$$

where an element of $v \in A \cap gG_0 \cdot s(L)$ is counted with weight $\#\{h \in G_0 \mid v \in gh \cdot s(L)\}$. Note that the weight of an element of $gG_0 \cdot s(L)$ is a positive integer $\leq r$ and that $gG_0 \cdot s(L)$ is partitioned into semialgebraic subsets of constant weight.

We can rewrite the integral of (8.7.4) using the decomposition $\mathfrak{S} = \omega \cdot T_c \cdot K$ and Lemma 8.2.2. Using the fact that $\mu(gk) = \mu(g)$ for all $k \in K$ and $K \cdot G_0 = G_0$, we obtain:

Lemma 8.7.1. *Given $X \geq 1$, $n \in \bar{N}(\mathbb{R})$, $t \in T^\theta(\mathbb{R})$ and $\lambda \in \Lambda$, define $B(n,t,\lambda,X) := (nt\lambda G_0 \cdot s(L))_{<X}$. Then for any subset $A \subset \underline{V}(\mathbb{Z}) \cap (G(\mathbb{R}) \cdot \Lambda \cdot s(L))$ we have*

$$N(A,X) = \frac{1}{r}\int_{\lambda=K_0^{-1}}^{X} \int_{t\in T_c} \int_{n\in\omega} \#[A \cap B(n,t,\lambda,X)]\, \mu(nt)^{-1}\delta_G(t)^{-1}\, dn\, dt\, d^\times\lambda, \qquad (8.7.5)$$

where an element $v \in A \cap B(n,t,\lambda,X)$ on the right-hand side is counted with weight $\#\{h \in G_0 \mid v \in nt\lambda h \cdot s(L))\}$.

Before estimating the integrand of (8.7.5) by counting lattice points in the bounded regions $B(n,t,\lambda,X)$, we first need to handle the so-called cuspidal region after introducing some notation.

Let Φ_V be the set of weights of the T^θ-action on V. Any $v \in V(\mathbb{Q})$ can be decomposed as $\sum v_a$ where v_a lies in the weight space corresponding to $a \in \Phi_V$. For a subset $M \subset \Phi_V$, let $V(M) \subset V$ be the subspace of elements v with $v_a = 0$ for all $a \in M$. Define $S(M) := V(M)(\mathbb{Q}) \cap \underline{V}(\mathbb{Z})$.

Let $a_0 \in X^*(T^\theta)$ denote the restriction of the highest root $\alpha_0 \in \Phi_H$ to T^θ. It turns out that $a_0 \in \Phi_V$: if H is not of type A_{2n}, this follows from the fact that the Coxeter number of H is even so the root height of α_0 with respect to S_H is odd; if H is of type A_{2n}, this can be checked explicitly.

We define $S(a_0)$ as the *cuspidal region* and $\underline{V}(\mathbb{Z}) \setminus S(a_0)$ as the *main body* of V. The next proposition, proved in §8.11, says that the number of irreducible elements in the cuspidal region is negligible.

Proposition 8.7.2. *There exists $\delta > 0$ such that $N(S(a_0)^{irr},X) = O(X^{\dim V - \delta})$.*

Having dealt with the cuspidal region, we may now count lattice points in the main body using the following proposition [3, Theorem 1.3], which strengthens a well-known result of Davenport [32]. We prefer to cite [3] since the possibility of applying [32] to a general semialgebraic set rests implicitly on the Tarski–Seidenberg principle (see [33]).

Proposition 8.7.3. *Let $m,n \geq 1$ be integers, and let $Z \subset \mathbb{R}^{m+n}$ be a semialgebraic subset. For $T \in \mathbb{R}^m$, let $Z_T = \{x \in \mathbb{R}^n \mid (T,x) \in Z\}$, and suppose that all such subsets Z_T are bounded.*

Then for any unipotent upper-triangular matrix $u \in \mathrm{GL}_n(\mathbb{R})$, we have

$$\#(Z_T \cap u\mathbb{Z}^n) = \mathrm{vol}(Z_T) + O(\max\{1, \mathrm{vol}(Z_{T,j}\}),$$

where $Z_{T,j}$ runs over all orthogonal projections of Z_T to any j-dimensional coordinate hyperplane $(1 \leq j \leq n-1)$. Moreover, the implied constant depends only on Z.

Proposition 8.7.4. *Let $A = \underline{V}(\mathbb{Z}) \cap (G(\mathbb{R}) \cdot \Lambda \cdot s(L))$. Then*

$$N(A \setminus S(a_0), X) = \frac{|W_0|}{r} \mathrm{vol}\left(\underline{G}(\mathbb{Z}) \backslash G(\mathbb{R})\right) \mathrm{vol}((\Lambda \cdot L)_{<X}) + o(X^{\dim V}).$$

Proof. Choose generators for the weight space $\underline{V}_a$ (as a finite free $\mathbb{Z}$-module) for every $a \in \Phi_V$ and let $\|\cdot\|$ denote the supremum norm of $V(\mathbb{R})$ with respect to this choice of basis. Since the set $\omega \cdot G_0 \cdot s(L)$ is bounded, we can choose a constant $J > 0$ such that $\|v\| \leq J$ for all $v \in \omega \cdot G_0 \cdot s(L)$. Let $F(n,t,\lambda,X) = \{v \in B(n,t,\lambda,X) \mid v_{a_0} \neq 0\}$. If $F(n,t,\lambda,X) \cap \underline{V}(\mathbb{Z}) \neq \emptyset$, there exists an element $v \in B(n,t,\lambda,X)$ such that $\|v_{a_0}\| \geq 1$, hence $\lambda a_0(t) \geq 1/J$.

We wish to estimate $\#[(A \setminus S(a_0)) \cap B(n,t,\lambda,X)] = \#[\underline{V}(\mathbb{Z}) \cap F(n,t,\lambda,X)]$ for all $t \in T_c, n \in \omega, \lambda \geq K_0^{-1}$ and X using Proposition 8.7.3. An element $v \in F(n,t,\lambda,X)$ has weight $\#\{h \in G_0 \mid v \in nt\lambda h \cdot s(L))\}$, and $F(n,t,\lambda,X)$ is partitioned into finitely many bounded semi-algebraic subsets of constant weight. Moreover we have an equality of (weighted) volumes $\mathrm{vol}(F(n,t,\lambda,X)) = \mathrm{vol}(B(n,t,\lambda,X))$. Since t and λ stretch the elements of $\underline{V}_a$ by a factor $a(t)$ and λ respectively, for any $M \subset \Phi_V$ the volume of the projection of $F(n,t,\lambda,X)$ to $V(M)(\mathbb{R})$ is bounded above by $O\left(\lambda^{\dim V - \#M} \prod_{a \in \Phi_V \setminus M} a(t)\right)$. Since Φ_V is closed under inversion, we have $\prod_{a \in \Phi_V} a(t) = 1$. Moreover since a_0 is the highest weight of the representation V, we know that for every $a \in \Phi_V$ we can write $a = a_0 - \sum_{\beta \in S_G} n_\beta \beta$ for some nonnegative rationals n_β. Since $t \in T_c$ by assumption, we have $a(t) \geq c^{-\sum n_\beta} a_0(t)$. It follows that

$$\lambda^{\dim V - \#M} \prod_{a \in \Phi_V \setminus M} a(t) = \lambda^{\dim V - \#M} \prod_{a \in M} a(t)^{-1} \ll \lambda^{\dim V - \#M} a_0(t)^{-\#M}.$$

Putting the results from the previous paragraph together, we conclude by Proposition 8.7.3 that the number of weighted elements of $[(A \setminus S(a_0)) \cap B(n,t,\lambda,X)]$ is given by:

$$\begin{cases} 0 & \text{if } \lambda a_0(t) < 1/J, \\ \mathrm{vol}(B(n,t,\lambda,X)) + O(\lambda^{\dim V - 1} a_0(t)^{-1}) & \text{otherwise.} \end{cases}$$

By that same proposition, the implied constant in this estimate is independent of $t \in T_c, n \in \omega, \lambda \geq K_0^{-1}$ and X. Therefore by Lemma 8.7.1 $N(A \setminus S(a_0), X)$ equals

$$\frac{1}{r}\int_{\lambda=K_0^{-1}}^{X}\int_{t\in T_c, a_0(t)\geq 1/\lambda J}\int_{n\in\omega}\Big(\mathrm{vol}(B(n,t,\lambda,X)) + O(\lambda^{\dim V-1}a_0(t)^{-1})\Big)\,\mu(nt)^{-1}\delta_G(t)^{-1}\,dn\,dt\,d^\times\lambda. \tag{8.7.6}$$

We first show that the integral of the second summand is $o(X^{\dim V})$. One easily reduces to showing that

$$\int_{\lambda=K_0^{-1}}^{X}\int_{t\in T_c, a_0(t)\geq 1/\lambda J}\lambda^{\dim V-1}a_0(t)^{-1}\delta_G(t)^{-1}\,dt\,d^\times\lambda = o(X^{\dim V}). \tag{8.7.7}$$

Write $S_G = \{\beta_1, \ldots, \beta_k\}$ and identify $T^\theta(\mathbb{R})^\circ$ with $\mathbb{R}^k_{>0}$ using the isomorphism $t \mapsto (\beta_i(t))$. Write $a_0 = \sum h_i\beta_i$ and $\sum_{\Phi_G^+}\beta = \sum \delta_i\beta_i$ with $h_i, \delta_i \in \mathbb{Q}$. Since the coefficients δ_i are strictly positive, there exists an $0 < \varepsilon < 1$ such that $\delta_i - \varepsilon h_i > 0$ for all i. Since $\lambda^{1-\varepsilon}a_0(t)^{1-\varepsilon} \gg 1$ on $\{t \in T_c \mid a_0(t) \geq 1/\lambda J\}$, it follows that

$$\int_{\lambda=K_0^{-1}}^{X}\int_{t\in T_c, a_0(t)\geq 1/\lambda J}\lambda^{\dim V-1}a_0(t)^{-1}\delta_G(t)^{-1}\,dt\,d^\times\lambda \tag{8.7.8}$$

$$\ll \int_{\lambda=K_0^{-1}}^{X}\lambda^{\dim V-\varepsilon}\int_{t\in T_c, a_0(t)\geq 1/\lambda J}a_0(t)^{-\varepsilon}\delta_G(t)^{-1}\,dt\,d^\times\lambda. \tag{8.7.9}$$

Since the exponents of t_i in $a_0(t)^{-\varepsilon}\delta_G(t)^{-1}$ are strictly positive, the inner integral of the right-hand side of (8.7.9) bounded independently of λ. It follows that (8.7.9) is $\ll \int_{\lambda=K_0^{-1}}^{X}\lambda^{\dim V-\varepsilon}d^\times\lambda = O(X^{\dim V-\varepsilon})$, as claimed.

On the other hand, the integral of the first summand in (8.7.6) is

$$\frac{1}{r}\int_{g\in\mathfrak{S}}\mathrm{vol}\left((g\cdot\Lambda\cdot G_0\cdot s(L))_{<X}\right)\mu(g)^{-1}\,dg + o(X^{\dim V}),$$

using the fact that $\mathrm{vol}(B(n,t,\lambda,X)) = O(\lambda^{\dim V})$. Lemma 8.4.2 shows that

$$\mathrm{vol}\left((g\cdot\Lambda\cdot G_0\cdot s(L))_{<X}\right) = |W_0|\,\mathrm{vol}\left((\Lambda\cdot L)_{<X}\right)\mathrm{vol}(G_0) = |W_0|\,\mathrm{vol}\left((\Lambda\cdot L)_{<X}\right).$$

The proposition follows from Formula (8.4.1). □

8.8 End of the proof of Proposition 8.5.2

The following proposition is proven in §8.10.

Proposition 8.8.1. *Let V^{red} denote the subset of $\mathbb{Q}$-reducible elements $v \in \underline{V}(\mathbb{Z})$ with $v \notin S(a_0)$. Then $N(V^{red}, X) = o(X^{\dim V})$.*

We now finish the proof of Proposition 8.5.2. Again let $A = \underline{V}(\mathbb{Z}) \cap (G(\mathbb{R}) \cdot \Lambda \cdot s(L))$. Then

$$N(A^{irr}, X) = N(A^{irr} \setminus S(a_0), X) + N(S(a_0)^{irr}, X)$$

The second term on the right-hand side is $o(X^{\dim V})$ by Proposition 8.7.2, and $N(A^{irr} \setminus S(a_0), X) = N(A \setminus S(a_0), X) + o(X^{\dim V})$ by Proposition 8.8.1. Using Proposition 8.7.4, we obtain

$$N(A^{irr}, X) = \frac{|W_0|}{r} \operatorname{vol}(\underline{G}(\mathbb{Z}) \backslash G(\mathbb{R})) \operatorname{vol}((\Lambda \cdot L)_{<X}) + o(X^{\dim V}).$$

This completes the proof of Proposition 8.5.2, hence also that of Theorem 8.5.1.

8.9 Congruence conditions

We now introduce a weighted version of Theorem 8.5.1. If $w \colon \underline{V}(\mathbb{Z}) \to \mathbb{R}$ is a function and $A \subset \underline{V}(\mathbb{Z})$ is a $\underline{G}(\mathbb{Z})$-invariant subset we define

$$N_w(A, X) := \sum_{\substack{v \in \underline{G}(\mathbb{Z}) \backslash A \\ \mathrm{ht}(v) < X}} \frac{w(v)}{\# Z_{\underline{G}}(v)(\mathbb{Z})}. \tag{8.9.1}$$

We say a function w is *defined by finitely many congruence conditions* if w is obtained from pulling back a function $\bar{w} \colon \underline{V}(\mathbb{Z}/M\mathbb{Z}) \to \mathbb{R}$ along the projection $\underline{V}(\mathbb{Z}) \to \underline{V}(\mathbb{Z}/M\mathbb{Z})$ for some $M \geq 1$. For such a function write μ_w for the average of $\bar{w}$ where we put the uniform measure on $\underline{V}(\mathbb{Z}/M\mathbb{Z})$. The following theorem follows immediately from the proof of Theorem 8.5.1, compare [16, §2.5].

Theorem 8.9.1. *Let $w \colon \underline{V}(\mathbb{Z}) \to \mathbb{R}$ be defined by finitely many congruence conditions. Then*

$$N_w(\underline{V}(\mathbb{Z})^{irr} \cap V(\mathbb{R})^{sol}, X) = \mu_w \frac{|W_0|}{2^g} \operatorname{vol}(\underline{G}(\mathbb{Z}) \backslash G(\mathbb{R})) \operatorname{vol}(B(\mathbb{R})_{<X}) + o\left(X^{\dim V}\right),$$

where $W_0 \in \mathbb{Q}^\times$ is the scalar of Lemma 8.3.1.

Next we will consider infinitely many congruence conditions. Suppose we are given for each prime p a $\underline{G}(\mathbb{Z}_p)$-invariant function $w_p : \underline{V}(\mathbb{Z}_p) \to [0,1]$ with the following properties:

- The function w_p is locally constant outside the closed subset $\{v \in \underline{V}(\mathbb{Z}_p) \mid \Delta(v) = 0\} \subset \underline{V}(\mathbb{Z}_p)$.
- For p sufficiently large, we have $w_p(v) = 1$ for all $v \in \underline{V}(\mathbb{Z}_p)$ such that $p^2 \nmid \Delta(v)$.

In this case we can define a function $w : \underline{V}(\mathbb{Z}) \to [0,1]$ by the formula $w(v) = \prod_p w_p(v)$ if $\Delta(v) \neq 0$ and $w(v) = 0$ otherwise. Call a function $w : \underline{V}(\mathbb{Z}) \to [0,1]$ defined by this procedure *acceptable*.

Theorem 8.9.2. *Let $w : \underline{V}(\mathbb{Z}) \to [0,1]$ be an acceptable function. Then*

$$N_w(\underline{V}(\mathbb{Z})^{irr} \cap V^{sol}(\mathbb{R}), X) \leq \frac{|W_0|}{2^g} \left(\prod_p \int_{\underline{V}(\mathbb{Z}_p)} w_p(v) \mathrm{d}v \right) \mathrm{vol}\,(\underline{G}(\mathbb{Z}) \backslash G(\mathbb{R}))\, \mathrm{vol}\,(B(\mathbb{R})_{<X}) + o(X^{\dim V}).$$

Proof. This inequality follows from Theorem 8.9.1; the proof is identical to the first part of the proof of [16, Theorem 2.21]. □

To obtain a lower bound in Theorem 8.9.2 when infinitely many congruence conditions are imposed, one needs a uniformity estimate that bounds the number of irreducible $\underline{G}(\mathbb{Z})$-orbits whose discriminant is divisible by the square of a large prime. The following conjecture is the direct analogue of [16, Theorem 2.13].

Conjecture 8.9.3. *For a prime p, let $\mathscr{W}_p(V)$ denote the subset of $v \in \underline{V}(\mathbb{Z})^{irr}$ such that $p^2 \mid \Delta(v)$. Then for any $M > 0$, we have*

$$\lim_{X \to +\infty} \frac{N(\cup_{p>M} \mathscr{W}_p(V), X)}{X^{\dim V}} = O\left(\frac{1}{\log M} \right),$$

where the implied constant is independent of M.

Conjecture 8.9.3 is related to computing the density of square-free values of polynomials. See [6] for some remarks about similar questions, for known results and why these uniformity estimates seem difficult in general. By an identical proof to that of [16, Theorem 2.21], we obtain:

Proposition 8.9.4. *Assume that Conjecture 8.9.3 holds for (G,V). Let $w : \underline{V}(\mathbb{Z}) \to [0,1]$ be an acceptable function. Then*

$$N_w(\underline{V}(\mathbb{Z})^{irr} \cap V^{sol}(\mathbb{R}), X) = \frac{|W_0|}{2^g} \left(\prod_p \int_{\underline{V}(\mathbb{Z}_p)} w_p(v) \mathrm{d}v \right) \mathrm{vol}\,(\underline{G}(\mathbb{Z}) \backslash G(\mathbb{R}))\, \mathrm{vol}\,(B(\mathbb{R})_{<X}) + o(X^{\dim V}).$$

8.10 Estimates on reducibility and stabilisers

In this subsection we give the proof of Proposition 8.8.1 and the following proposition, which will be useful in §9.

Proposition 8.10.1. *Let $V^{bigstab}$ denote the subset of $\mathbb{Q}$-irreducible elements $v \in \underline{V}(\mathbb{Z})$ with $\#Z_G(v)(\mathbb{Q}) > 1$. Then $N(V^{bigstab}, X) = o(X^{\dim V})$.*

By the same reasoning as [9, §10.7] it will suffice to prove Lemma 8.10.2 below, after having introduced some notation.

Let N be the integer of §7.1 and let p be a prime not dividing N. We define $V_p^{red} \subset V(\mathbb{Z}_p)$ to be the set of vectors whose reduction mod p is $\mathbb{F}_p$-reducible. We define $V_p^{bigstab} \subset V(\mathbb{Z}_p)$ to be the set of vectors $v \in V(\mathbb{Z}_p)$ such that $p|\Delta(v)$ or the image of v in $V(\mathbb{F}_p)$ has nontrivial stabiliser in $G(\mathbb{F}_p)$.

Lemma 8.10.2. *We have*

$$\lim_{Y \to +\infty} \prod_{N<p<Y} \int_{V_p^{red}} dv = 0,$$

and similarly

$$\lim_{Y \to +\infty} \prod_{N<p<Y} \int_{V_p^{bigstab}} dv = 0.$$

Proof. The proof is very similar to the proof of [72, Proposition 6.9] using the root lattice calculations of §3.9. We first treat the case of $V_p^{bigstab}$. Let p be a prime not dividing N. We have the formula

$$\int_{V_p^{bigstab}} dv = \frac{1}{\#V(\mathbb{F}_p)} \#\{v \in V(\mathbb{F}_p) \mid \Delta(v) = 0 \text{ or } Z_G(v)(\mathbb{F}_p) \neq 1\}.$$

Since $\{\Delta = 0\}$ is a hypersurface we have

$$\frac{1}{\#V(\mathbb{F}_p)} \#\{v \in V(\mathbb{F}_p) \mid \Delta(v) = 0\} = O(p^{-1}). \tag{8.10.1}$$

If $v \in V^{\mathrm{rs}}(\mathbb{F}_p)$ then $\#Z_G(v)(\mathbb{F}_p)$ depends only on $\pi(v)$ by (the $\mathbb{Z}[1/N]$-analogue of) Lemma 3.8.2. Therefore if $b \in B^{\mathrm{rs}}(\mathbb{F}_p)$, Proposition 7.2.2 and Lang's theorem imply that $\#V_b(\mathbb{F}_p)$ is partitioned into $\#\mathrm{H}^1(\mathbb{F}_p, J_b[2])$ many orbits under $G(\mathbb{F}_p)$, each of size $\#G(\mathbb{F}_p)/\#J_b[2](\mathbb{F}_p)$. Since $\#J_b[2](\mathbb{F}_p) = \#(J_b(\mathbb{F}_p)/2J_b(\mathbb{F}_p)) = \#\mathrm{H}^1(\mathbb{F}_p, J_b[2])$, we have $\#V^{\mathrm{rs}}(\mathbb{F}_p) = \#G(\mathbb{F}_p)\#B^{\mathrm{rs}}(\mathbb{F}_p)$.

So to prove the lemma in case of $V_p^{bigstab}$ it suffices to prove that there exists a $0 < \delta < 1$ such that

$$\frac{1}{\#B^{\mathrm{rs}}(\mathbb{F}_p)} \#\{b \in B^{\mathrm{rs}}(\mathbb{F}_p) \mid J_b[2](\mathbb{F}_p) \neq 1\} \to \delta$$

as $p \to +\infty$. We will achieve this using the results of [73, §9.3]. Recall from §3.1 that T is a split maximal torus of H with Lie algebra $\mathfrak{t}$ and Weyl group W. These objects spread out to objects $\underline{T}, \underline{H}, \underline{\mathfrak{t}}$ over $\mathbb{Z}$. In §3.9 we have defined a W-torsor $f\colon \mathfrak{t}^{\mathrm{rs}} \to B^{\mathrm{rs}}$ which extends to a W-torsor $\underline{\mathfrak{t}}_S^{\mathrm{rs}} \to \underline{B}_S^{\mathrm{rs}}$, still denoted by f. The group scheme $J[2] \to \underline{B}_S^{\mathrm{rs}}$ is trivialised along f and the monodromy action is given by the natural action of W on N_L using the same logic and notation as Proposition 3.9.1. Let $C \subset W$ be the subset of elements of W which fix some nonzero element of N_L. Then [73, Proposition 9.15] implies that

$$\frac{1}{\#B^{\mathrm{rs}}(\mathbb{F}_p)}\#\{b \in B^{\mathrm{rs}}(\mathbb{F}_p) \mid J_b[2](\mathbb{F}_p) \neq 1\} = \frac{\#C}{\#W} + O(p^{-1/2}). \tag{8.10.2}$$

Since $C \neq W$ by Part 3 of Proposition 3.9.2, we conclude the proof of the lemma in this case.

We now treat the case V_p^{red}. Again by (8.10.1) it suffices to prove that there exists a nonnegative $\delta < 1$ such that

$$\frac{1}{\#V^{\mathrm{rs}}(\mathbb{F}_p)}\#\{v \in V^{\mathrm{rs}}(\mathbb{F}_p) \mid v \text{ is } \mathbb{F}_p\text{-reducible}\} < \delta \tag{8.10.3}$$

for all sufficiently large p. By the first paragraph of the proof of this lemma, there are exactly $\#J_b[2]$ orbits of $V_b(\mathbb{F}_p)$ for all $b \in B^{\mathrm{rs}}(\mathbb{F}_p)$, each of size $\#G(\mathbb{F}_p)/\#J_b[2](\mathbb{F}_p)$. Since exactly one of these orbits consists of $\mathbb{F}_p$-reducible elements, the left-hand-side of (8.10.3) equals

$$\frac{1}{\#B^{\mathrm{rs}}(\mathbb{F}_p)} \sum_{b \in B^{\mathrm{rs}}(\mathbb{F}_p)} \frac{1}{\#J_b[2](\mathbb{F}_p)} \tag{8.10.4}$$

Each summand in (8.10.4) is the inverse of an integer; let η_p be the proportion of $b \in B^{\mathrm{rs}}(\mathbb{F}_p)$ for which this summand equals 1. The the quantity in (8.10.4) is $\leq \eta_p + (1-\eta_p)/2 = 1/2 + \eta_p/2$. By (8.10.2), $\eta_p \to \eta := 1 - \#C/\#W$ as p tends to infinity. Since $1 \in C$, we see that $\eta < 1$, completing the proof of the lemma. $\square$

We explain why Lemma 8.10.2 implies Propositions 8.8.1 and 8.10.1. We first claim that if $v \in \underline{V}(\mathbb{Z})$ with $b = \pi(v)$ is $\mathbb{Q}$-reducible, then for each prime p not dividing N the reduction of v in $V(\mathbb{F}_p)$ is $\mathbb{F}_p$-reducible. Indeed, either $\Delta(b) = 0$ in $\mathbb{F}_p$ (in which case v is $\mathbb{F}_p$-reducible), or $p \nmid \Delta(b)$ and v is $G(\mathbb{Q})$-conjugate to κ'_b for some Kostant section κ'. In the latter case Part 2 of Theorem 7.4.4 implies that v is $G(\mathbb{Z}_p)$-conjugate to κ'_b, so their reductions are $G(\mathbb{F}_p)$-conjugate, proving the claim. By a congruence version of Proposition 8.7.4, for every subset $L \subset B(\mathbb{R})$ considered in Proposition 8.5.2 and for every $Y > 0$ we obtain the estimate:

$$N(V^{red} \cap G(\mathbb{R}) \cdot \Lambda \cdot s(L), X) \leq C \left(\prod_{N<p<Y} \int_{V_p^{red}} dv \right) \cdot X^{\dim V} + o(X^{\dim V}),$$

where $C > 0$ is a constant independent of Y. By Lemma 8.10.2, the product of the integrals converges to zero as Y tends to infinity, so $N(V^{red} \cap G(\mathbb{R}) \cdot \Lambda \cdot s(L), X) = o(X^{\dim V})$. Since this holds for every such subset L, we obtain Proposition 8.8.1.

Note that we have not used Theorem 8.5.1 in this argument, but we may use it now to prove Proposition 8.10.1. Again the reduction of an element of $V^{bigstab}$ modulo p lands in $V_p^{bigstab}$ if p does not divide N, by Part 1 of Theorem 7.4.4. Since $\lim_{X \to +\infty} N(V^{bigstab}, X)/X^{\dim V}$ is $O(\prod_{N<p<Y} \int_{V_p^{red}} dv)$ by Theorem 8.9.1 and the product of the integrals converges to zero by Lemma 8.10.2, this proves Proposition 8.10.1.

8.11 Cutting off the cusp

In this section we consider the only remaining unproved assertion of this chapter, namely Proposition 8.7.2. This is the only substantial part of this thesis where we rely on previous papers treating specific cases. Case A_{2g} is treated in [9, Proposition 10.5]; Case A_{2g+1} ($g \geq 1$) is [75, Proposition 21]; Case D_{2g+1} ($g \geq 2$) is [76, Proposition 7.6]; Case E_6 is [84, Proposition 3.6]; Case E_7, E_8 is [71, Proposition 4.5]. Note that these authors sometimes use a power of the height that we use. It remains to consider the case where H is of type D_{2n} and $n \geq 2$. We first reduce the statement to a combinatorial result, after introducing some notation. This reduction step is valid for any H, and we do not yet assume that H is of type D_{2n}.

Recall that every element $a \in X^*(T^\theta) \otimes \mathbb{Q}$ can be uniquely written as $\sum_{i=1}^k n_i(a)\beta_i$ for some rational numbers $n_i(a)$. We define a partial ordering on $X^*(T^\theta) \otimes \mathbb{Q}$ by declaring that $a \geq b$ if $n_i(a-b) \geq 0$ for all $i = 1, \dots, k$. By restriction, this induces a partial ordering on Φ_V. The restriction of the highest root $a_0 \in \Phi_V$ is the unique maximal element with respect to this partial ordering.

If (M_0, M_1) is a pair of disjoint subsets of Φ_V we define $S(M_0, M_1) := \{v \in \underline{V}(\mathbb{Z}) \mid \forall a \in M_0, v_a = 0; \forall a \in M_1, v_a \neq 0\}$. Let $\mathscr{C}$ be the collection of nonempty subsets $M_0 \subset \Phi_V$ with the property that if $a \in M_0$ and $b \geq a$ then $b \in M_0$. Given a subset $M_0 \in \mathscr{C}$ we define $\lambda(M_0) := \{a \in \Phi_V \setminus M_0 \mid M_0 \cup \{a\} \in \mathscr{C}\}$, i.e. the set of maximal elements of $\Phi_V \setminus M_0$.

By definition of $\mathscr{C}$ and λ we see that $S(\{a_0\}) = \cup_{M_0 \in \mathscr{C}} S(M_0, \lambda(M_0))$. Therefore to prove Proposition 8.7.2, it suffices to prove that for each $M_0 \in \mathscr{C}$, either $S(M_0, \lambda(M_0))^{irr} = \emptyset$ or $N(S(M_0, \lambda(M_0)), X) = O(X^{\dim V - \varepsilon})$ for some $\varepsilon > 0$. By the same logic as [84, Proposition 3.6 and §5] (itself based on a trick due to Bhargava), the latter estimate holds if there exists a subset $M_1 \subset \Phi_V \setminus M_0$ and a function $f\colon M_1 \to \mathbb{R}_{\geq 0}$ with $\sum_{a\in M_1} f(a) < \#M_0$ such that

$$\sum_{\beta\in\Phi_G^+} \beta - \sum_{a\in M_0} a + \sum_{a\in M_1} f(a)a$$

has strictly positive coordinates with respect to the basis S_G. It will thus suffice to prove the following combinatorial proposition, which is the analogue of [9, Proposition 29].

Proposition 8.11.1. *Let $M_0 \in \mathscr{C}$ be a subset such that $V(M_0)(\mathbb{Q})$ contains $\mathbb{Q}$-irreducible elements. Then there exists a subset $M_1 \subset \Phi_V \setminus M_0$ and a function $f\colon M_1 \to \mathbb{R}_{\geq 0}$ satisfying the following conditions:*

- *We have $\sum_{a\in M_1} f(a) < \#M_0$.*
- *For each $i = 1,\ldots,k$ we have $\sum_{\beta\in\Phi_G^+} n_i(\beta) - \sum_{a\in M_0} n_i(a) + \sum_{a\in M_1} f(a)n_i(a) > 0$.*

We will prove Proposition 8.11.1 in the remaining case D_{2n} in Appendix A.

Chapter 9

The average size of the 2-Selmer group

9.1 An upper bound

In this chapter we prove Theorem 1.2.3 stated in the introduction. Recall that we write $\mathscr{E}$ for the set of elements $b \in \underline{B}(\mathbb{Z})$ of nonzero discriminant. We recall that we have defined a height function ht for $\mathscr{E}$ in §8.1. We say a subset $\mathscr{F} \subset \mathscr{E}$ is defined by *finitely many congruence conditions* if $\mathscr{F}$ is the preimage of a subset of $\underline{B}(\mathbb{Z}/N\mathbb{Z})$ under the reduction map $\mathscr{E} \to \underline{B}(\mathbb{Z}/N\mathbb{Z})$ for some $N \geq 1$.

Theorem 9.1.1. *Let $\mathscr{F} \subset \mathscr{E}$ be a subset defined by finitely many congruence conditions. Let m be the number of marked points. Then we have*

$$\limsup_{X \to +\infty} \frac{\sum_{b \in \mathscr{F},\, \mathrm{ht}(b) < X} \# \mathrm{Sel}_2 J_b}{\#\{b \in \mathscr{F} \mid \mathrm{ht}(b) < X\}} \leq 3 \cdot 2^{m-1}.$$

The proof is along the same lines as the discussion in [72, §7].

We first prove a 'local' result. Recall that $\mathscr{E}_p$ denotes the set of elements $b \in \underline{B}(\mathbb{Z}_p)$ of nonzero discriminant. Define $\mathscr{F}_p$ as the closure of $\mathscr{F}$ in $\mathscr{E}_p$, equivalently $\mathscr{F}_p$ is the preimage in $\mathscr{E}_p$ of a subset of $\underline{B}(\mathbb{Z}/N\mathbb{Z})$ that defines $\mathscr{F}$.

For every $b \in B^{\mathrm{rs}}(\mathbb{Q})$, consider the subgroup of $J_b(\mathbb{Q})/2J_b(\mathbb{Q})$ generated by differences of the marked points $\{\infty_1 - \infty_2, \dots, \infty_1 - \infty_m\}$. The image of this subgroup under the map $J_b(\mathbb{Q})/2J_b(\mathbb{Q}) \hookrightarrow \mathrm{Sel}_2 J_b$ is by definition the subgroup $\mathrm{Sel}_2^{triv} J_b$ of 'marked' elements. Its complement $\mathrm{Sel}_2^{\cancel{\mathrm{triv}}} J_b$ is the subset of 'nonmarked' elements.

Proposition 9.1.2. *Let $b_0 \in \mathscr{F}$. Then we can find for each prime p dividing N an open compact neighbourhood W_p of b_0 in $\mathscr{E}_p$ such that the following condition holds. Let $\mathscr{F}_W =$*

$\mathscr{F} \cap \left(\prod_{p|N} W_p\right)$. *Then we have*

$$\limsup_{X\to+\infty} \frac{\sum_{b\in\mathscr{F}_W,\,\mathrm{ht}(b)<X} \#\mathrm{Sel}_2^{\cancel{triv}} J_b}{\#\{b\in\mathscr{F}_W \mid \mathrm{ht}(b)<X\}} \leq 2^m.$$

Proof. Choose the sets W_p and integers $n_p \geq 0$ for $p|N$ satisfying the conclusion of Corollary 7.6.1. If p does not divide N, set $W_p = \mathscr{F}_p$ and $n_p = 0$. Let $M := \prod_p p^{n_p}$.

For $v \in \underline{V}(\mathbb{Z})$ with $\pi(v) = b$, define $w(v) \in \mathbb{Q}_{\geq 0}$ by the following formula:

$$w(v) = \begin{cases} \left(\sum_{v'\in \underline{G}(\mathbb{Z})\backslash(\underline{G}(\mathbb{Q})\cdot v\cap \underline{V}(\mathbb{Z}))} \frac{\#Z_{\underline{G}}(v')(\mathbb{Q})}{\#Z_{\underline{G}}(v')(\mathbb{Z})}\right)^{-1} & \text{if } b\in p^{n_p}\cdot W_p \text{ and } G(\mathbb{Q}_p)\cdot v \in \eta_b(J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)) \text{ for all } p, \\ 0 & \text{otherwise.}\end{cases}$$

Define $w'(v)$ by the formula $w'(v) = \#Z_{\underline{G}}(v)(\mathbb{Q})w(v)$. Corollaries 6.4.2 and 7.6.1 and Proposition 6.5.1 imply that if $b \in M\cdot\mathscr{F}_W$, nonmarked elements in the 2-Selmer group of J_b correspond bijectively to $G(\mathbb{Q})$-orbits of $V_b(\mathbb{Q})$ that intersect $\underline{V}(\mathbb{Z})$ nontrivially, that are $\mathbb{Q}$-irreducible and that are soluble at $\mathbb{R}$ and $\mathbb{Q}_p$ for all p. In other words, in the notation of (8.9.1) we have the formula:

$$\sum_{\substack{b\in\mathscr{F}_W\\ \mathrm{ht}(b)<X}} \#\mathrm{Sel}_2^{\cancel{triv}} J_b = \sum_{\substack{b\in M\cdot\mathscr{F}_W\\ \mathrm{ht}(b)<MX}} \#\mathrm{Sel}_2^{\cancel{triv}} J_b = N_{w'}(\underline{V}(\mathbb{Z})^{irr}\cap V(\mathbb{R})^{sol}, MX). \tag{9.1.1}$$

Proposition 8.10.1 implies that

$$N_{w'}(\underline{V}(\mathbb{Z})^{irr}\cap V(\mathbb{R})^{sol}, MX) = N_{w}(\underline{V}(\mathbb{Z})^{irr}\cap V(\mathbb{R})^{sol}, MX) + o(X^{\dim V}). \tag{9.1.2}$$

It is more convenient to work with $w(v)$ than with $w'(v)$ because $w(v)$ is an acceptable function in the sense of §8.9. Indeed, for $v \in \underline{V}(\mathbb{Z}_p)$ with $\pi(v) = b$, define $w_p(v) \in \mathbb{Q}_{\geq 0}$ by the following formula

$$w_p(v) = \begin{cases} \left(\sum_{v'\in \underline{G}(\mathbb{Z}_p)\backslash\left(\underline{G}(\mathbb{Q}_p)\cdot v\cap \underline{V}(\mathbb{Z}_p)\right)} \frac{\#Z_{\underline{G}}(v')(\mathbb{Q}_p)}{\#Z_{\underline{G}}(v')(\mathbb{Z}_p)}\right)^{-1} & \text{if } b\in p^{n_p}\cdot W_p \text{ and } G(\mathbb{Q}_p)\cdot v \in \eta_b(J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)), \\ 0 & \text{otherwise.}\end{cases}$$

Then an argument identical to [16, Proposition 3.6] (using that $\underline{G}$ has class number 1 by Proposition 7.1.2) shows that $w(v) = \prod_p w_p(v)$ for all $v \in \underline{V}(\mathbb{Z})$. The remaining properties for $w(v)$ to be acceptable follow from Part 1 of Lemma 8.3.2 and Theorem 7.4.4. Using

Lemma 8.3.2 we obtain the formula

$$\int_{v\in\underline{V}(\mathbb{Z}_p)} w_p(v)dv = |W_0|_p \operatorname{vol}(\underline{G}(\mathbb{Z}_p)) \int_{b\in p^{n_p}\cdot W_p} \frac{\# J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)}{\# J_b[2](\mathbb{Q}_p)} db. \tag{9.1.3}$$

Using the equality $\# J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p) = |1/2^g|_p \# J_b[2](\mathbb{Q}_p)$ for all $b \in \mathscr{E}_p$ (which is a general fact about abelian varieties), we see that the integral on the right-hand side equals $|1/2^g|_p \operatorname{vol}(p^{n_p}\cdot W_p) = |1/2^g|_p p^{-n_p \dim_{\mathbb{Q}} V} \operatorname{vol}(W_p)$. Combining the identities (9.1.1) and (9.1.2) shows that

$$\limsup_{X\to+\infty} X^{-\dim V} \sum_{\substack{b\in\mathscr{F}_W \\ \mathrm{ht}(b)<X}} \#\mathrm{Sel}_2^{\cancel{\mathrm{triv}}} J_b = \limsup_{X\to+\infty} X^{-\dim V} N_w(\underline{V}(\mathbb{Z})^{irr} \cap V(\mathbb{R})^{sol}, MX).$$

This in turn by Theorem 8.9.2 is less then or equal to

$$\frac{|W_0|}{2^g}\left(\prod_p \int_{\underline{V}(\mathbb{Z}_p)} w_p(v)dv\right) \operatorname{vol}(\underline{G}(\mathbb{Z})\backslash G(\mathbb{R}))\, 2^{\dim B} M^{\dim V}.$$

Using (9.1.3) this simplifies to

$$\operatorname{vol}(\underline{G}(\mathbb{Z})\backslash\underline{G}(\mathbb{R})) \prod_p \operatorname{vol}(\underline{G}(\mathbb{Z}_p))\, 2^{\dim B} \prod_p \operatorname{vol}(W_p).$$

On the other hand, an elementary point count shows that

$$\lim_{X\to+\infty} \frac{\#\{b\in\mathscr{F}_W \mid ht(b)<X\}}{X^{\dim V}} = 2^{\dim B}\prod_p \operatorname{vol}(W_p).$$

We conclude that

$$\limsup_{X\to+\infty} \frac{\sum_{b\in\mathscr{F}_W,\, ht(b)<X} \#\mathrm{Sel}_2^{\cancel{\mathrm{triv}}} J_b}{\#\{b\in\mathscr{F}_W \mid ht(b)<X\}} \leq \operatorname{vol}(\underline{G}(\mathbb{Z})\backslash\underline{G}(\mathbb{R}))\cdot\prod_p \operatorname{vol}(\underline{G}(\mathbb{Z}_p)).$$

Since the Tamagawa number of $\underline{G}$ is 2^m (Proposition 8.2.1), the proposition follows. □

To deduce Theorem 9.1.1 from Proposition 9.1.2, choose for each $i \geq 1$ sets $W_{p,i} \subset \mathscr{E}_p$ (for p dividing N) such that if $W_i = \mathscr{E} \cap \left(\prod_{p|N} W_{p,i}\right)$, then W_i satisfies the conclusion of Proposition 9.1.2 and we have a countable partition $\mathscr{F} = \mathscr{F}_{W_1} \sqcup \mathscr{F}_{W_1} \sqcup \cdots$. By an argument identical to the proof of Theorem 7.1 in [72], we see that for any $\varepsilon > 0$, there exists $k \geq 1$ such that

$$\limsup_{X\to+\infty} \frac{\sum_{b\in\sqcup_{i\geq k}\mathscr{F}_{W_i},\mathrm{ht}(b)<X} \#\mathrm{Sel}_2^{\cancel{\mathrm{triv}}} J_b}{\#\{b\in\mathscr{F} \mid \mathrm{ht}(b)<X\}} < \varepsilon.$$

This implies that

$$\begin{aligned}\limsup_{X\to+\infty}\frac{\sum_{b\in\mathscr{F},\mathrm{ht}(b)<X}\#\mathrm{Sel}_2^{\cancel{triv}}J_b}{\#\{b\in\mathscr{F}\mid \mathrm{ht}(b)<X\}}&\leq 2^m\limsup_{X\to+\infty}\frac{\#\{b\in\sqcup_{i<k}\mathscr{F}_{W_i}\mid \mathrm{ht}(b)<X\}}{\#\{b\in\mathscr{F}\mid \mathrm{ht}(b)<X\}}+\varepsilon\\&\leq 2^m+\varepsilon.\end{aligned}$$

Since the above inequality is true for any $\varepsilon>0$, it is true for $\varepsilon=0$. Since the subgroup $\mathrm{Sel}^{triv}J_b$ has size at most 2^{m-1}, we conclude the proof of Theorem 9.1.1.

Remark 9.1.3. *A small modification of the above argument shows that Theorem 9.1.1 remains valid when $\mathscr{F}\subset\mathscr{E}$ is the subset of so-called 'minimal' elements, namely those elements $b\in\mathscr{E}$ with $N^{-1}\cdot b\notin\underline{B}(\mathbb{Z})$ for all integers $N\geq 1$.*

9.2 A conditional lower bound

We show that the upper bound in Theorem 9.1.1 is sharp if we assume Conjecture 8.9.3. We first need to establish (unconditionally) a lower bound for the subgroup of marked elements $\mathrm{Sel}^{triv}J_b$.

Proposition 9.2.1. *Let $\mathscr{F}\subset\mathscr{E}$ be a subset defined by finitely many congruence conditions. Then the limit*

$$\lim_{X\to+\infty}\frac{\#\{b\in\mathscr{F}\mid \mathrm{ht}(b)<X,\#\mathrm{Sel}_2(J_b)^{triv}=2^{m-1}\}}{\#\{b\in\mathscr{F}\mid \mathrm{ht}(b)<X\}}$$

exists and equals 1.

Proof. Let $b\in\mathscr{F}$ and consider the maximal torus $Z_H(\kappa_b)$ of H. By Proposition 6.5.1, $\#\mathrm{Sel}_2(J_b)^{triv}=2^{m-1}$ if and only if the map $Z_G(\kappa_b)\to Z_{H^\theta}(\kappa_b)$ is surjective on $\mathbb{Q}$-points. The Galois action on $Z_H(\kappa_b)$ induces a homomorphism $\mathrm{Gal}(\mathbb{Q}^s\mid\mathbb{Q})\to W$ by Proposition 3.9.1, where W is the Weyl group of the split torus $T\subset H$ with character group L. If this homomorphism is surjective, then $Z_{H^\theta}(\kappa_b)(\mathbb{Q})=T[2]^W=(L^\vee/2L^\vee)^W=\{0\}$ by Part 1 of Proposition 3.9.2, so $Z_G(\kappa_b)\to Z_{H^\theta}(\kappa_b)$ is automatically surjective on $\mathbb{Q}$-points.

It therefore suffices to prove that the limit

$$\lim_{X\to+\infty}\frac{\#\{b\in\mathscr{F}\mid \mathrm{ht}(b)<X,\mathrm{Gal}(\mathbb{Q}^s\mid\mathbb{Q})\to W\text{ surjective}\}}{\#\{b\in\mathscr{F}\mid \mathrm{ht}(b)<X\}}$$

exists and equals 1. This follows from a version of Hilbert's irreducibility theorem; see [27, Theorem 2.1], adapted as in [27, §5, Notes (iii)] to account for the fact that the coordinates of B have unequal weights. $\square$

Theorem 9.2.2. *Assume that Conjecture 8.9.3 holds for* (G,V). *Let* $\mathscr{F} \subset \mathscr{E}$ *be a subset defined by finitely many congruence conditions. Then the limit*

$$\lim_{X \to +\infty} \frac{\sum_{b \in \mathscr{F},\, \mathrm{ht}(b) < X} \# \mathrm{Sel}_2^{\cancel{triv}} J_b}{\#\{b \in \mathscr{F} \mid \mathrm{ht}(b) < X\}}$$

exists and equals 2^m. *Moreover, the average size of the* 2*-Selmer group* $\mathrm{Sel}_2 J_b$ *exists and equals* $3 \cdot 2^{m-1}$.

Proof. The proof of the first statement is identical to the proof of Theorem 9.1.1, using Proposition 8.9.4 instead of Theorem 8.9.2. The second statement follows from the first and Proposition 9.2.1. $\square$

References

[1] Altman, A. B. and Kleiman, S. L. (1980). Compactifying the Picard scheme. *Adv. in Math.*, 35(1):50–112.

[2] Artin, M., Bertin, J. E., Demazure, M., Gabriel, P., Grothendieck, A., Raynaud, M., and Serre, J.-P. (1964). *Schémas en groupes. Fasc. 3: Exposés 8 à 11*. Institut des Hautes Études Scientifiques, Paris. Troisième édition, Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques, 1963/64, dirigé par Michel Demazure et Alexander Grothendieck.

[3] Barroero, F. and Widmer, M. (2014). Counting lattice points and O-minimal structures. *Int. Math. Res. Not. IMRN*, (18):4932–4957.

[4] Beauville, A. (1999). Counting rational curves on $K3$ surfaces. *Duke Math. J.*, 97(1):99–108.

[5] Bektemirov, B., Mazur, B., Stein, W., and Watkins, M. (2007). Average ranks of elliptic curves: tension between data and conjecture. *Bull. Amer. Math. Soc. (N.S.)*, 44(2):233–254.

[6] Bhargava, M. (2014a). The geometric sieve and the density of squarefree values of invariant polynomials. Arxiv Preprint, available at https://arxiv.org/abs/1402.0031v1.

[7] Bhargava, M. (2014b). Rational points on elliptic and hyperelliptic curves. In *Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. 1*, pages 657–684. Kyung Moon Sa, Seoul.

[8] Bhargava, M., Elkies, N., and Shnidman, A. (2020). The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$. *Journal of the London Mathematical Society*, 101(1):299–327.

[9] Bhargava, M. and Gross, B. H. (2013). 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.

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

[11] Bhargava, M., Gross, B. H., and Wang, X. (2017). A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension. *J. Amer. Math. Soc.*, 30(2):451–493. With an appendix by Tim Dokchitser and Vladimir Dokchitser.

[12] Bhargava, M. and Ho, W. (2013). On average sizes of Selmer groups and ranks in families of elliptic curves having marked points. Preprint, available at http://www-personal.umich.edu/~weiho/papers/.

[13] Bhargava, M. and Ho, W. (2016). Coregular spaces and genus one curves. *Camb. J. Math.*, 4(1):1–119.

[14] Bhargava, M. and Shankar, A. (2013a). The average number of elements in the 4-Selmer groups of elliptic curves is 7. Arxiv Preprint, available at https://arxiv.org/abs/1312.7333v1.

[15] Bhargava, M. and Shankar, A. (2013b). The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1. Arxiv Preprint, available at https://arxiv.org/abs/1312.7859v1.

[16] Bhargava, M. and Shankar, A. (2015a). Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math. (2)*, 181(1):191–242.

[17] Bhargava, M. and Shankar, A. (2015b). Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math. (2)*, 181(2):587–621.

[18] Bialynicki-Birula, A. (1973). Some theorems on actions of algebraic groups. *Ann. of Math. (2)*, 98:480–497.

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

[20] Borel, A. (1966). Density and maximality of arithmetic subgroups. *J. Reine Angew. Math.*, 224:78–89.

[21] Borel, A. (1969). *Introduction aux groupes arithmétiques*. Publications de l'Institut de Mathématique de l'Université de Strasbourg, XV. Actualités Scientifiques et Industrielles, No. 1341. Hermann, Paris.

[22] Borel, A. (1970). Properties and linear representations of Chevalley groups. In *Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69)*, Lecture Notes in Mathematics, Vol. 131, pages 1–55. Springer, Berlin.

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

[24] Carter, R. W. (1972). *Simple groups of Lie type*. John Wiley & Sons, London-New York-Sydney. Pure and Applied Mathematics, Vol. 28.

[25] Cesnavicius, K. (2021). Grothendieck-Serre in the quasi-split unramified case. Arxiv Preprint, available at https://arxiv.org/abs/2009.05299v3.

[26] Charles, F. and Poonen, B. (2016). Bertini irreducibility theorems over finite fields. *J. Amer. Math. Soc.*, 29(1):81–94.

[27] Cohen, S. D. (1981). The distribution of Galois groups and Hilbert's irreducibility theorem. *Proc. London Math. Soc. (3)*, 43(2):227–250.

[28] Colliot-Thélène, J.-L. (1980). Formes quadratiques multiplicatives et variétés algébriques: deux compléments. *Bull. Soc. Math. France*, 108(2):213–227.

[29] Colliot-Thélène, J.-L. and Sansuc, J.-J. (1979). Fibrés quadratiques et composantes connexes réelles. *Math. Ann.*, 244(2):105–134.

[30] Conrad, B. (2014). Reductive group schemes. In *Autour des schémas en groupes. Vol. I*, volume 42/43 of *Panor. Synthèses*, pages 93–444. Soc. Math. France, Paris.

[31] Cremona, J. E., Fisher, T. A., O'Neil, C., Simon, D., and Stoll, M. (2008). Explicit n-descent on elliptic curves. I. Algebra. *J. Reine Angew. Math.*, 615:121–155.

[32] Davenport, H. (1951). On a principle of Lipschitz. *J. London Math. Soc.*, 26:179–183.

[33] Davenport, H. (1964). Corrigendum: "On a principle of Lipschitz". *J. London Math. Soc.*, 39:580.

[34] Deligne, P. and Rapoport, M. (1973). Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349.

[35] Dwyer, W. G. and Wilkerson, C. W. (2001). Centers and Coxeter elements. In *Homotopy methods in algebraic topology (Boulder, CO, 1999)*, volume 271 of *Contemp. Math.*, pages 53–75. Amer. Math. Soc., Providence, RI.

[36] Esteves, E. (2001). Compactifying the relative Jacobian over families of reduced curves. *Trans. Amer. Math. Soc.*, 353(8):3045–3095.

[37] Fedorov, R. and Panin, I. (2015). A proof of the Grothendieck-Serre conjecture on principal bundles over regular local rings containing infinite fields. *Publ. Math. Inst. Hautes Études Sci.*, 122:169–193.

[38] Gross, B. H. (2011). On Bhargava's representation and Vinberg's invariant theory. In *Frontiers of mathematical sciences*, pages 317–321. Int. Press, Somerville, MA.

[39] Grothendieck, A. (1966). Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III. *Inst. Hautes Études Sci. Publ. Math.*, (28):255.

[40] Guo, N. (2020). The Grothendieck—Serre conjecture over semilocal Dedekind rings. *Transform. Groups*.

[41] Ho, W. (2014). How many rational points does a random curve have? *Bull. Amer. Math. Soc. (N.S.)*, 51(1):27–52.

[42] Humphreys, J. E. (1995). *Conjugacy classes in semisimple algebraic groups*, volume 43 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI.

[43] Jelisiejew, J. and Sienkiewicz, L. u. (2019). Białynicki-Birula decomposition for reductive groups. *J. Math. Pures Appl. (9)*, 131:290–325.

[44] Knörrer, H. (1987). Cohen-Macaulay modules on hypersurface singularities. I. *Invent. Math.*, 88(1):153–164.

[45] Kostant, B. (1963). Lie group representations on polynomial rings. *Amer. J. Math.*, 85:327–404.

[46] Kostant, B. and Rallis, S. (1971). Orbits and representations associated with symmetric spaces. *Amer. J. Math.*, 93:753–809.

[47] Laga, J. (2020a). Arithmetic statistics of Prym surfaces. Preprint, available at https://www.dpmms.cam.ac.uk/~jcsl5/.

[48] Laga, J. (2020b). The average size of the 2-Selmer group of a family of non-hyperelliptic curves of genus 3. To appear in Algebra & Number Theory. Arxiv preprint available at https://arxiv.org/abs/2008.13158v3.

[49] Lang, S. (1975). $\mathrm{SL}_2(\mathbf{R})$. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam.

[50] Langlands, R. P. (1966). The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 143–148. Amer. Math. Soc., Providence, R.I.

[51] Levy, P. (2009). Vinberg's θ-groups in positive characteristic and Kostant-Weierstrass slices. *Transform. Groups*, 14(2):417–461.

[52] Matsumura, H. (1986). *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge. Translated from the Japanese by M. Reid.

[53] Melo, M., Rapagnetta, A., and Viviani, F. (2017). Fine compactified Jacobians of reduced curves. *Trans. Amer. Math. Soc.*, 369(8):5341–5402.

[54] Milne, J. S. (1980). *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J.

[55] Mumford, D. (2007). *Tata lectures on theta. III*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA. With collaboration of Madhav Nori and Peter Norman, Reprint of the 1991 original.

[56] Nisnevich, Y. A. (1984). Espaces homogènes principaux rationnellement triviaux et arithmétique des schémas en groupes réductifs sur les anneaux de Dedekind. *C. R. Acad. Sci. Paris Sér. I Math.*, 299(1):5–8.

[57] Ono, T. (1965). On the relative theory of Tamagawa numbers. *Ann. of Math. (2)*, 82:88–111.

[58] Panin, I. (2017). Proof of Grothendieck–Serre conjecture on principal bundles over regular local rings containing a finite field. Preprint, available at https://arxiv.org/abs/1707.01767v1.

[59] Panin, I. (2018). On Grothendieck-Serre conjecture concerning principal bundles. In *Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. II. Invited lectures*, pages 201–221. World Sci. Publ., Hackensack, NJ.

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

[61] Platonov, V. and Rapinchuk, A. (1994). *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press, Inc., Boston, MA. Translated from the 1991 Russian original by Rachel Rowen.

[62] Poonen, B. (2004). Bertini theorems over finite fields. *Ann. of Math. (2)*, 160(3):1099–1127.

[63] Poonen, B. (2017). *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI.

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

[65] Poonen, B. and Stoll, M. (2014). Most odd degree hyperelliptic curves have only one rational point. *Ann. of Math. (2)*, 180(3):1137–1166.

[66] Raghunathan, M. S. and Ramanathan, A. (1984). Principal bundles on the affine line. *Proc. Indian Acad. Sci. Math. Sci.*, 93(2-3):137–145.

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

[68] Reeder, M., Levy, P., Yu, J.-K., and Gross, B. H. (2012). Gradings of positive rank on simple Lie algebras. *Transform. Groups*, 17(4):1123–1190.

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

[70] Riche, S. (2017). Kostant section, universal centralizer, and a modular derived Satake equivalence. *Math. Z.*, 286(1-2):223–261.

[71] Romano, B. and Thorne, J. A. (2018). On the arithmetic of simple singularities of type E. *Res. Number Theory*, 4(2):Art. 21, 34.

[72] Romano, B. and Thorne, J. A. (2020). E_8 and the average size of the 3-Selmer group of the Jacobian of a pointed genus-2 curve. *Proceedings of the London Mathematical Society*.

[73] Serre, J.-P. (2012). *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL.

[74] Seshadri, C. S. (1977). Geometric reductivity over arbitrary base. *Advances in Math.*, 26(3):225–274.

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

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

[77] Slodowy, P. (1980). *Simple singularities and simple algebraic groups*, volume 815 of *Lecture Notes in Mathematics*. Springer, Berlin.

[78] Springer, T. A. (2009). *Linear algebraic groups*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, second edition.

[79] Stacks Project Authors, T. (2018). *Stacks Project*. https://stacks.math.columbia.edu.

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

[81] Steinberg, R. (1975). Torsion in reductive groups. *Advances in Math.*, 15:63–92.

[82] Thorne, J. A. (2012). *The Arithmetic of Simple Singularities*. ProQuest LLC, Ann Arbor, MI. Thesis (Ph.D.)–Harvard University.

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

[84] Thorne, J. A. (2015). E_6 and the arithmetic of a family of non-hyperelliptic curves of genus 3. *Forum Math. Pi*, 3:e1, 41.

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

[86] Thorne, J. A. (2019). On the average number of 2-Selmer elements of elliptic curves over $\mathbb{F}_q(X)$ with two marked points. *Doc. Math.*, 24:1179–1223.

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

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

[89] Wang, X. (2018). Maximal linear spaces contained in the based loci of pencils of quadrics. *Algebr. Geom.*, 5(3):359–397.

Appendix A

Cutting off the cusp for D_{2n}

In this appendix chapter we prove Proposition 8.7.2 in the case that H is of type D_{2n} for all $n \geq 2$. The methods employed here are fairly standard but somewhat intricate, and are sometimes inspired by [76, §7.2.1]. In §A.1 we recall some results and notation on groups of type D_n. In §A.2 we make the representation (G,V) in the case D_{2n} and some related objects explicit. In §A.3 we establish sufficient conditions for a vector $v \in V(\mathbb{Q})$ to be $\mathbb{Q}$-reducible. In §A.4 we finish the proof of Proposition 8.7.2.

A.1 Recollections on even orthogonal groups

Let $n \geq 2$ be an integer. Let W be a $2n$-dimensional $\mathbb{Q}$-vector space with basis $\mathscr{B} = \{e_1, \dots, e_n, e_n^*, \dots, e_1^*\}$. Let b be the symmetric bilinear form with the property that $b(e_i, e_j) = b(e_i^*, e_j^*) = 0$ and $b(e_i, e_j^*) = \delta_{ij}$ for all $1 \leq i, j \leq n$. For every linear map $f \colon W \to W$, there is a unique adjoint linear map $f^* \colon W \to W$ satisfying $b(fv, w) = b(v, f^*w)$ for all $v, w \in W$. We define the $\mathbb{Q}$-algebraic group $H := \mathrm{SO}(W, b) = \{g \in \mathrm{SL}(W) \mid gg^* = 1\}$. Then $\mathfrak{h} := \mathrm{Lie}\, H$ can be naturally identified with $\{f \in \mathrm{End}(W) \mid f + f^* = 0\}$. Below we will make various aspects of the semisimple group H explicit.

Using $\mathscr{B}$ to represent an element $f \colon W \to W$ as a $(2n) \times (2n)$-matrix A, f^* corresponds to reflecting A along its antidiagonal. Consider the maximal torus $T = \{\mathrm{diag}(t_1, \dots, t_n, t_n^{-1}, \dots, t_1^{-1})\} \subset H$. Its character group $X^*(T)$ is freely generated by the characters $(t_1, \dots) \mapsto t_i$ with $1 \leq i \leq n$, and we abusively denote these characters by $t_i \in X^*(T)$ too.

Root system The roots of $\mathfrak{h}$ with respect to T are given by

$$\Phi_H = \{\pm t_i \pm t_j \mid 1 \leq i \neq j \leq n\} \subset X^*(T). \tag{A.1.1}$$

The standard upper triangular Borel subgroup of GL_{2n} (with respect to the basis $\mathscr{B}$ of W) determines a root basis of Φ_H, given by

$$S_H = \{t_1 - t_2, \dots, t_{n-1} - t_n, t_{n-1} + t_n\} \tag{A.1.2}$$

We denote the elements of this root basis by $\alpha_1, \dots, \alpha_n$. The highest root of Φ_H with respect to S_H is $t_1 + t_2$, which has height $2n-3$.

Weyl group The Weyl group W_H is isomorphic to $S_n \rtimes (\mathbb{Z}/2\mathbb{Z})^{n-1}$. Explicitly, elements of W_H correspond to pairs $(\sigma, (\varepsilon_i))$, where $\sigma \in S_n$ is a permutation and $\varepsilon_i \in \{\pm 1\}$ is a sign for each $1 \leq i \leq n$, with the property that $\prod_i \varepsilon_i = 1$. An element $(\sigma, (\varepsilon_i))$ acts on $X^*(T)$ via the rule $t_i \mapsto \varepsilon_i t_{\sigma(i)}$. In particular, $-1 \in W_H$ if and only if n is even.

Stable involution To describe the stable involution of H in §A.2 in the case that n is even, we determine the elements $s \in T$ with the property that $\alpha(s) = -1$ for every simple root $\alpha \in S_H$. Such an s is not uniquely determined since H is not adjoint, but it is uniquely determined up to multiplication by the element $(-1, \dots, -1) \in T$ of the centre of H. Using the description (A.1.2) we see that s is of the form

$$\pm(1, -1, 1, -1, \dots, (-1)^n). \tag{A.1.3}$$

Change of variables We record the following computation which will be useful in §A.4:

$$\begin{cases} t_i = \alpha_i + \cdots + \alpha_{n-2} + \frac{1}{2}(\alpha_{n-1} + \alpha_n), & (1 \leq i \leq n-2) \\ t_{n-1} = \frac{1}{2}(\alpha_{n-1} + \alpha_n), \\ t_n = \frac{1}{2}(-\alpha_{n-1} + \alpha_n). \end{cases} \tag{A.1.4}$$

Sum of positive roots The sum of the positive roots of Φ_H with respect to S_H is

$$\sum_{\alpha \in \Phi_H^+} \alpha = 2(n-1)t_1 + 2(n-2)t_2 + \cdots + 2t_{n-1} \tag{A.1.5}$$

$$= \sum_{k=1}^{n-2} k(2n-k-1)\alpha_k + \frac{n(n-1)}{2}(\alpha_{n-1} + \alpha_n) \tag{A.1.6}$$

Discriminant Let $\mathfrak{t} := \operatorname{Lie} T$ and write an element of $\mathfrak{t}$ as $\operatorname{diag}(t_1, \dots, t_n, -t_n, \dots, -t_1)$. Let $\Delta \in \mathbb{Q}[\mathfrak{h}]^H$ be the discriminant polynomial of H, defined as the image of $\prod_{\alpha \in \Phi_H} \alpha$ under the Chevalley isomorphism $\mathbb{Q}[\mathfrak{t}]^{W_H} \to \mathbb{Q}[\mathfrak{h}]^H$ of Proposition 2.1.1. Let $\mathrm{Pff} \in \mathbb{Q}[\mathfrak{h}]^H$ be the image of the product $\prod_{i=1}^{n} t_i \in k[\mathfrak{t}]^{W_H}$ under the Chevalley isomorphism. If we write $t_i := t_{2n+1-i}$ for $n+1 \leq i \leq 2n$, then we may compute that

$$\prod_{1 \leq i < j \leq 2n} (t_i - t_j)^2 = \prod_{\alpha \in \Phi_H} \alpha(t)^2 \prod_{i=1}^{n} t_i^2. \tag{A.1.7}$$

It follows that if we write χ_v for the characteristic polynomial of a square matrix v and $\operatorname{disc}(\chi_v)$ for its discriminant, we have the identity

$$\operatorname{disc}(\chi_v) = \Delta(v)^2 \operatorname{Pff}(v)^2 \tag{A.1.8}$$

for every $v \in \mathfrak{h}$.

A.2 An explicit model for the split stable involution of D_{2n}

Let $n \geq 2$ be an integer. Let W_1 be the $\mathbb{Q}$-vector space with basis $\{e_1, \ldots, e_n, e_n^*, \ldots, e_1^*\}$, and let b_1 be the symmetric bilinear form with the property that $b_1(e_i, e_j) = b_1(e_i^*, e_j^*) = 0$ and $b_1(e_i, e_j^*) = \delta_{ij}$ for all $1 \leq i, j \leq n$. Let W_2 be the $\mathbb{Q}$-vector space with basis $\{f_1, \ldots, f_n, f_n^*, \ldots, f_1^*\}$, and let b_2 be the bilinear form of W_2 constructed similarly to b_1 with e_i and e_i^* replaced by f_i and f_i^*. Let $(W, b) := (W_1, b_1) \oplus (W_2, b_2)$. Let $H' := \mathrm{SO}(W, b)$, let H be the quotient of H' by its centre of order 2 and let $\mathfrak{h} := \operatorname{Lie} H = \operatorname{Lie} H'$. With respect to the basis

$$\{e_1, \ldots, e_n, e_n^*, \ldots, e_1^*, f_1, \ldots, f_n, f_n^*, \ldots, f_1^*\}, \tag{A.2.1}$$

the adjoint of a $(4n) \times (4n)$-block matrix

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \tag{A.2.2}$$

with respect to b is given by

$$\begin{pmatrix} A^* & C^* \\ B^* & D^* \end{pmatrix}. \tag{A.2.3}$$

Here if X is a $(2n)\times(2n)$-matrix we write X^* for its reflection around the antidiagonal. It follows that in this basis $\mathfrak{h}$ is given by

$$\left\{ \begin{pmatrix} B & A \\ -A^* & C \end{pmatrix} \mid B^* = -B, C^* = -C \right\}. \tag{A.2.4}$$

Stable involution The ordered basis

$$\{e_1, f_1, \dots, e_n, f_n, f_n^*, e_n^*, \dots, f_1^*, e_1^*\} \tag{A.2.5}$$

of W determines a maximal torus and root basis of H as in §A.1. Let θ be the involution of H constructed using the recipe in §3.1 with respect to this root basis. Since -1 is contained in the Weyl group of H (as observed in §A.1), θ is inner. The description of (A.1.3) shows that with respect to the first basis (A.2.1) of W, θ is given by conjugating by the element $s' = \mathrm{diag}(1,\dots,1,-1,\dots,-1)$, where the first $2n$ entries are 1's and the last $2n$ entries are -1's. Using this description, it is easy to see that

$$\mathfrak{g} := \mathfrak{h}^\theta = \left\{ \begin{pmatrix} B & 0 \\ 0 & C \end{pmatrix} \mid B^* = -B, C^* = -C \right\},$$
$$V := \mathfrak{h}^{\theta=-1} = \left\{ \begin{pmatrix} 0 & A \\ -A^* & 0 \end{pmatrix} \mid A \in \mathrm{Mat}_{2n,2n} \right\}.$$

Moreover $G := (H^\theta)^\circ$ is isomorphic to $(\mathrm{SO}(W_1)\times\mathrm{SO}(W_2))/\Delta(\mu_2)$, where $\Delta(\mu_2)$ denotes the image of the diagonal inclusion of μ_2 into the centre $\mu_2\times\mu_2$ of $\mathrm{SO}(W_1)\times\mathrm{SO}(W_2)$. Using these identifications, we see that the map

$$\begin{pmatrix} 0 & A \\ -A^* & 0 \end{pmatrix} \mapsto A$$

establishes a bijection between V and the representation $\mathrm{Hom}(W_2, W_1)$, where $(g,h) \in \mathrm{SO}(W_1)\times\mathrm{SO}(W_2)$ acts on $f\colon W_2 \to W_1$ via $g\circ f\circ h^{-1}$. In terms of matrices, the action is given by $(g,h)\cdot A = gAh^{-1}$. We will typically view an element of $V(\mathbb{Q})$ as a $(2n)\times(2n)$-matrix A or a linear operator $f\colon W_2 \to W_1$.

Roots Let T' be the maximal torus $\mathrm{diag}(t_1,\dots,t_n,t_n^{-1},\dots,t_1^{-1},s_1,\dots,s_n,s_n^{-1},\dots,s_1^{-1})$ of H' (again using the basis (A.2.1)), and let T be its image in H. Then T is a maximal torus of H and G; let Φ_H and Φ_G be the corresponding sets of roots. Let $W_H = N_H(T)/T$ and $W_G = N_G(T)/T$ be the respective Weyl groups. The basis (A.2.5) determines a set of positive roots Φ_H^+ of H (as in §A.1) and by restriction a set of positive roots Φ_G^+ of G. The corresponding simple roots are given by:

$$S_H = \{t_1 - s_1, s_1 - t_2, \dots, s_{n-1} - t_n, t_n - s_n, t_n + s_n\},$$
$$S_G = \{t_1 - t_2, \dots, t_{n-1} - t_n, t_{n-1} + t_n\} \cup \{s_1 - s_2, \dots, s_{n-1} - s_n, s_{n-1} + s_n\}.$$

We label the elements of S_G by $\{\beta_1, \dots, \beta_{n-1}, \beta_n\} \cup \{\gamma_1, \dots, \gamma_{n-1}, \gamma_n\}$. We have $\Phi_H = \Phi_G \sqcup \Phi_V$ and $\Phi_V = \{\pm t_i \pm s_j \mid 1 \le i, j \le n\}$.

Component group Let s be the image of s' in $T(\mathbb{Q})$. Lemma 3.3.1 shows that the inclusion $N_{H^\theta}(T) \hookrightarrow H^\theta$ induces an isomorphism $Z_{W_H}(s)/W_G \simeq H^\theta/G$. In fact, let

$$\Omega := \{w \in W_H \mid w(S_G) = S_G\}. \tag{A.2.6}$$

Then using the description of the Weyl group of H and G from §A.1 we see that $Z_{W_H}(s) = W_G \rtimes \Omega$ and $\Omega \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$. Explicit generators of Ω are given by ω_1, ω_2, where

$$\omega_1 : t_i \leftrightarrow s_i,$$
$$\omega_2 : \begin{cases} s_i \mapsto s_i, t_i \mapsto t_i, & (1 \le i \le n-1) \\ t_n \mapsto -t_n, s_n \mapsto -s_n. \end{cases}$$

Weights Using the description of elements of V as $(2n) \times (2n)$ matrices, we organise the weights Φ_V using the position of their eigenspaces:

$$\left(\begin{array}{cc:c|c:cc} t_1 - s_1 & \cdots & t_1 - s_n & t_1 + s_n & \cdots & t_1 + s_1 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \hdashline t_n - s_1 & \cdots & t_n - s_n & t_n + s_n & \cdots & t_n + s_1 \\ \hline -t_n - s_1 & \cdots & -t_n - s_n & -t_n + s_n & \cdots & -t_n + s_1 \\ \hdashline \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ -t_1 - s_1 & \cdots & -t_1 - s_n & -t_1 + s_n & \cdots & -t_1 + s_1 \end{array}\right) \tag{A.2.7}$$

The group Ω acts on the set of weights Φ_V as follows: ω_1 flips the elements of Φ_V along the antidiagonal of (A.2.7), and ω_2 swaps the two middle rows and the two middle columns.

The partial ordering Recall from §8.11 that we have defined a partial ordering on $X^*(T')$ by declaring that $a \ge b$ if and only if $a - b$ has nonnegative coordinates with respect to the basis S_G. Note that this partial ordering is preserved by the action of Ω on $X^*(T')$.

We describe the induced partial ordering on the subset Φ_V using the organisation (A.2.7). We first consider the restriction of the partial ordering to the rows and columns of (A.2.7). Let $1 \leq i \leq 2n$ and write $t_i := -t_{2n+1-i}, s_i := -s_{2n+1-i}$ if $i \geq n+1$. The Hasse diagram of the partial ordering restricted to the weights of row i is given by:

$$
\begin{tikzcd}
 & & & \boxed{t_i - s_n} \arrow[dr, dash] & & & \\
\boxed{t_i - s_1} \arrow[r, dash, dashed] & \cdots \arrow[r, dash, dashed] & \boxed{t_i - s_{n-1}} \arrow[ur, dash] \arrow[dr, dash] & & \boxed{t_i + s_{n-1}} \arrow[r, dash, dashed] & \cdots \arrow[r, dash, dashed] & \boxed{t_i + s_1} \\
 & & & \boxed{t_i + s_n} \arrow[ur, dash] & & &
\end{tikzcd}
$$

(In this diagram, $a \leq b$ if and only if b is to the right of a.) The Hasse diagram of column $2n+1-i$ is given by swapping the roles of s_j and t_j in the above diagram for every $1 \leq j \leq 2n$. The partial ordering Φ_V is the one generated by the relations between two elements lying in the same row or column.

For example, $t_1 + s_1$ is the maximal element of Φ_V, and the restriction of the partial ordering to the four $n \times n$ blocks is given by: $a \leq b$ if and only if b is to the top right of a.

Regular nilpotent element For $\alpha \in \Phi_V$, let X_α be the $(2n) \times (2n)$-matrix with coefficient 1 at the entry corresponding to α using (A.2.7) and zeroes elsewhere. The element $E := \sum_{\alpha \in S_H} X_\alpha$ is a regular nilpotent element of $V(\mathbb{Q})$ and gives rise to an $\mathfrak{sl}_2$-triple (E, X, F) and Kostant section $\kappa = E + \mathfrak{z}_{\mathfrak{h}}(F)$, see §3.6. Since elements of $\mathfrak{z}_{\mathfrak{h}}(F)$ are supported on $\Phi_V \cap \Phi_H^-$ (where $\Phi_H^- = \Phi_H \setminus \Phi_H^+$), every element of κ is of the form

$$
\left(\begin{array}{cccc|cccc}
1 & 0 & \cdots & 0 & 0 & \cdots & \cdots & 0 \\
* & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots & 0 & \ddots & \ddots & \vdots \\
* & \cdots & * & 1 & 1 & 0 & \cdots & 0 \\
\hline
* & \cdots & \cdots & * & * & 1 & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & 1 \\
* & \cdots & \cdots & * & * & \cdots & \cdots & *
\end{array}\right) \tag{A.2.8}
$$

If $\omega \in \Omega$, then $E_\omega := \sum_{\alpha \in \omega(S_H)} X_\alpha$ is again regular nilpotent and gives rise to a Kostant section κ_ω. Then $\{\kappa_\omega \mid \omega \in \Omega\}$ is a full set of representatives of $G(\mathbb{Q})$-orbits of Kostant sections.

A.3 Reducibility conditions

Recall that if A is a $(2n)\times(2n)$-matrix then A^* denotes its reflection along the antidiagonal.

Proposition A.3.1. *Let $k/\mathbb{Q}$ be a field and $A \in V(k)$. The following are equivalent:*

1. *A is a regular semisimple element of $V(k)$;*
2. *AA^* is a regular semisimple $(2n)\times(2n)$-matrix (in other words, the characteristic polynomial of AA^* has distinct roots in k^s);*
3. *A^*A is a regular semisimple $(2n)\times(2n)$-matrix.*

Proof. Let $\Delta \in \mathbb{Q}[V]^G$ be the discriminant polynomial of $\mathfrak{h} \simeq \mathfrak{so}_{4n}$ restricted to V. Let B be the block matrix $\begin{pmatrix} 0 & A \\ -A^* & 0 \end{pmatrix}$. If C is a square matrix, write $\chi_C \in k[X]$ for its characteristic polynomial. If f is a polynomial, write $\mathrm{disc}(f)$ for its discriminant in the usual sense. The identity (A.1.8) implies that $\mathrm{disc}(\chi_B) = \Delta(A)^2 \cdot \mathrm{Pff}(B)^2$. We have $\mathrm{Pff}(B) = \pm\det(A)$ since both square to $\det(B)$, so

$$\mathrm{disc}(\chi_B) = \Delta(A)^2 \cdot \det(A)^2. \tag{A.3.1}$$

On the other hand, if $f(X) = g(X^2)$ for some polynomial $g \in k[X]$, then it is elementary to check that $\mathrm{disc}(f) = \pm\,\mathrm{disc}(g)^2 f(0)$. Moreover, by calculating determinants of block matrices we have $\chi_B(X) = \chi_{-AA^*}(X^2)$. Therefore

$$\mathrm{disc}(\chi_B) = \pm\,\mathrm{disc}(\chi_{-AA^*})^2 \cdot \det(A)^2. \tag{A.3.2}$$

Both identities (A.3.1) and (A.3.2) hold in $\mathbb{Q}[V][X]$, i.e. they hold when the coefficients of A are interpreted as variables. Since $\det \in \mathbb{Q}[V]$ is not identically zero, it follows that $\Delta(A) = \pm\,\mathrm{disc}(\chi_{-AA^*}) = \pm\,\mathrm{disc}(\chi_{AA^*})$. Since $\chi_{AA^*} = \chi_{A^*A}$ we have $\Delta(A) = \pm\,\mathrm{disc}(\chi_{A^*A})$. Since A is a regular semisimple element of $V(k)$ if and only if $\Delta(A) \neq 0$, the proposition follows. □

In the next lemma, we organise the set Φ_V using the matrix (A.2.7), and we recall from §8.7 that for a subset $M \subset \Phi_V$ we have defined $V(M)$ as the subspace of $v = \sum_{a\in\Phi_V} v_a \in V$ with the property that $v_a = 0$ for all $a \in M$.

Corollary A.3.2. *Suppose that a subset $M \subset \Phi_V$ satisfies at least one of the following conditions:*

1. *M contains a top right $i \times (2n+1-i)$ block for some $1 \leq i \leq 2n$;*

2. *M contains the top right $i \times j$ and $j \times i$ blocks for some $i, j \geq 1$ satisfying $i + j = 2n$.*

Then every element of $V(M)(\mathbb{Q})$ is not regular semisimple.

Proof. 1. We may suppose (using the fact that $A \mapsto A^*$ preserves regular semisimplicity) that $i \leq n$. Let $X_1 = \operatorname{span}\{e_1, \dots, e_n\} \subset W_1$. Then $\mathrm{GL}(X_1)$ embeds inside $\mathrm{SO}(W_1)$, using the map $g \mapsto \begin{pmatrix} g & 0 \\ 0 & (g^*)^{-1} \end{pmatrix}$. Suppose that $A \in V(M)(\mathbb{Q})$. Using the $\mathrm{GL}(X_1)$-action to put the top left $i \times (i-1)$ block of A in row echelon form, we may suppose that M contains the top right $1 \times 2n$ block; in other words, we may suppose that $i = 1$. In that case, the matrix AA^* has zeroes on the first row and the last column. This implies that the characteristic polynomial of AA^* is divisible by X^2, which implies that A is not regular semisimple by Proposition A.3.1.

2. Assume that $i \leq j$ and let $A \in V(M)(\mathbb{Q})$. Then the matrix $B = AA^*$ is of the form:

$$\left(\begin{array}{c|c|c} B_1 & 0 & 0 \\ \hline * & B_2 & 0 \\ \hline * & * & B_3 \end{array}\right). \tag{A.3.3}$$

Here B_1, B_3 are $i \times i$ matrices and B_2 is a $(j-i) \times (j-i)$ matrix (it is possible that $i = j$). Recall that χ_C denotes the characteristic polynomial of a square matrix C. Then we have $\chi_{AA^*} = \chi_{B_1}\chi_{B_2}\chi_{B_3}$. Since $B_3 = B_1^*$, the polynomial $\chi_{AA^*} = \chi_{B_1}^2\chi_{B_2}$ has repeated roots. By Proposition A.3.1, this shows that A is not regular semisimple.

□

Recall from §A.2 that we may interpret an element $A \in V(\mathbb{Q})$ as a linear map $W_2 \to W_1$. Using the perfect pairings b_i on W_i we may thus interpret A^* as a linear map $W_1 \to W_2$, and AA^* as a linear map $W_1 \to W_1$.

Proposition A.3.3. *Let $k/\mathbb{Q}$ be a field and $A \in V(k)$. Assume that there exists an $(n-1)$-dimensional subspace $X \subset W_1$ such that $\operatorname{span}\{X, AA^*(X)\}$ is an n-dimensional isotropic subspace of (W_1, b_1). Then A is k-reducible.*

Proof. If A is not regular semisimple then A is k-reducible by definition, so assume that A has invariants $b \in B^{\mathrm{rs}}(k)$. (Recall that $B = V /\!\!/ G$.) The Grassmannian of n-dimensional isotropic subspaces of (W_1, b_1) has two connected components called rulings of (W_1, b_1), and the subspaces spanned by $\{e_1^*, \dots, e_n^*\}$ and $\{e_1^*, \dots, e_{n-1}^*, e_n\}$ lie in distinct rulings [89, §2.2]; let $\mathscr{R}$ be the ruling containing the subspace $X_1 := \operatorname{span}\{e_1^*, \dots, e_n^*\}$. Using the Ω-action we may assume that $\operatorname{span}\{X, AA^*(X)\}$ lies in $\mathscr{R}$. To prove the proposition, it suffices to prove the claim that $G(k)$ acts simply transitively on the set of pairs (D,Y), where $D \in V_b(k)$ and $Y \subset W_1$ is an $(n-1)$-dimensional subspace such that $\mathrm{span}\{Y, DD^*(Y)\}$ is an n-dimensional isotropic subspace of (W_1, b_1) contained in the ruling $\mathscr{R}$. Indeed, the description of the Kostant section κ_b from (A.2.8) shows that (κ_b, X_1) is such a pair, so the claim implies that (A,X) and (κ_b, X_1) are $G(k)$-conjugate. The proof of the claim is identical to the proof of [76, Proposition 4.4] using the results of [89, §2.2.2]; we omit the details. □

Corollary A.3.4. *Suppose that M contains the top right $(n-1)\times(n+1)$ and $n\times(n-1)$ blocks. Then every element of $V(M)(\mathbb{Q})$ is $\mathbb{Q}$-reducible.*

Proof. If $A \in V(M)(\mathbb{Q})$, a computation shows that the entries of AA^* in the top right $(n-1)\times n$ and $n\times(n-1)$ blocks are zero. In other words, AA^* looks like:

$$\left(\begin{array}{cc:c|c:cc} * & * & * & 0 & 0 & 0 \\ * & * & * & 0 & 0 & 0 \\ \hdashline * & * & * & * & 0 & 0 \\ \hline * & * & * & * & * & * \\ \hdashline * & * & * & * & * & * \\ * & * & * & * & * & * \end{array}\right). \tag{A.3.4}$$

It follows that the subspace $X = \mathrm{span}\{e^*_{n-1}, \dots, e^*_1\}$ satisfies the assumptions of Proposition A.3.3. □

Recall that $\mathscr{C}$ denotes the collection of subsets M of Φ_V with the property that for all $a,b \in \Phi_V$ with $b \in M$ and $a \geq b$ it follows that $a \in M$. Also recall the description of the partial ordering on Φ_V in §A.2.

Proposition A.3.5. *Let $M \in \mathscr{C}$ and suppose that $V(M)(\mathbb{Q})$ contains $\mathbb{Q}$-irreducible elements. Then the following properties hold:*

1. *$\{t_i - s_i, s_i - t_i\} \subset \Phi_V \setminus M$ for all $1 \leq i \leq n-1$;*
2. *$\{t_n - s_n, t_n + s_n, -t_n + s_n, -t_n - s_n\} \subset \Phi_V \setminus M$;*
3. *for every $1 \leq i \leq n-2$, either $t_i - s_{i+1}$ or $s_i - t_{i+1}$ lies in $\Phi_V \setminus M$;*
4. *$\#(\{t_{n-1} - s_n, t_{n-1} + s_n, t_n + s_{n-1}, -t_n + s_{n-1}\} \cap M) \leq 2$.*

Proof. Note that if $\omega \in \Omega$ then $V(M)(\mathbb{Q})$ contains $\mathbb{Q}$-irreducible elements if and only if $V(\omega(M))(\mathbb{Q})$ does. The first three parts follow from applying Corollary A.3.2 to $\omega(M)$ for all $\omega \in \Omega$ and properties of the partial ordering of Φ_V. Part 4 follows from applying Corollary A.3.4 to $\omega(M)$ for $\omega \in M$. □

The reader is invited to visualise the conditions of Proposition A.3.5 using the organisation of the weights Φ_V of (A.2.7).

A.4 Bounding the remaining cusp integrals

Let $\mathscr{C}^{good}$ be the subset of $\mathscr{C}$ consisting of those $M \in \mathscr{C}$ that satisfy Condiditions 1–4 of Proposition A.3.5. Note that $\omega(M) \in \mathscr{C}^{good}$ if $M \in \mathscr{C}^{good}$ and $\omega \in \Omega$.

Lemma A.4.1. *If $M \in \mathscr{C}^{good}$, then every element of S_G is of the form $a_1 + a_2$ for some $a_1, a_2 \in \Phi_V \setminus M$.*

Proof. Using the Ω-action it suffices to consider $\beta_1, \dots, \beta_{n-1}$. For $1 \le i \le n-2$, we have identities

$$\begin{aligned} \beta_i = t_i - t_{i+1} &= (t_i - s_i) + \boxed{(s_i - t_{i+1})} \\ &= \boxed{(t_i - s_{i+1})} + (s_{i+1} - t_{i+1}). \end{aligned}$$

At least one of the two boxed terms is in $\Phi_V \setminus M$ by Part 3 of Proposition A.3.5, and the black terms are always in $\Phi_V \setminus M$ by Part 1 of that proposition. To treat β_{n-1}, consider the identities

$$\begin{aligned} \beta_{n-1} = t_{n-1} - t_n &= \boxed{(t_{n-1} - s_n)} + (s_n - t_n) \\ &= \boxed{(t_{n-1} + s_n)} + (-s_n - t_n) \\ &= (t_{n-1} - s_{n-1}) + \boxed{(s_{n-1} - t_n)}. \end{aligned}$$

One of the three boxed terms must be contained in $\Phi_V \setminus M$ by Part 4 of Proposition A.3.5, and all the black terms are contained in $\Phi_V \setminus M$ by Parts 1 and 2 of that proposition. $\square$

The discussion in §8.11 and Proposition A.3.5 show that in order to prove Proposition 8.7.2 when H is of type D_{2n} for all $n \ge 2$, it suffices to prove the following proposition.

Proposition A.4.2. *For every $M \in \mathscr{C}^{good}$, there exists a function $f \colon \Phi_V \setminus M \to \mathbb{R}_{\ge 0}$ with the following properties:*

1. $\sum_{a \in \Phi_V \setminus M} f(a) < \#M$;
2. *the vector*

$$\sum_{\beta \in \Phi_G^+} \beta - \sum_{a \in M} a + \sum_{a \in \Phi_V \setminus M} f(a) a \tag{A.4.1}$$

has strictly positive coefficients with respect to the basis S_G.

We prove Proposition A.4.2 using induction on n. The base case $n = 2$ is easy to check explicitly, and also follows from Case 1 of the proof of Proposition A.4.3 below (which only assumes $n \geq 2$). See [86, p. 1217] which considers the D_4 case in detail and also proves this induction step.

To perform the induction step, let $\Phi_V^{[1]}$ be the subset of Φ_V of vectors of the form $\{\pm t_1 \pm s_i\} \cup \{\pm t_i \pm s_1\}$; in other words, $\Phi_V^{[1]}$ consists of the first and last rows and columns of (A.2.7). Similarly let $\Phi_G^{[1]}$ for the subset of roots of Φ_G that have a nonzero coordinate at β_1 or γ_1 in the root basis S_G. Write $\Phi_V = \Phi_V^{[1]} \sqcup \Phi_V^{[n-1]}$ and $\Phi_G = \Phi_G^{[1]} \sqcup \Phi_G^{[n-1]}$. Then $\Phi_V^{[n-1]}$ and $\Phi_G^{[n-1]}$ arise from the constructions of §A.2 with n replaced by $n-1$. Moreover $\sum_{\beta \in \Phi_G^{[1],+}} \beta = (2n-2)t_1 + (2n-2)s_1$. To prove Proposition A.4.2, it therefore suffices to prove the following statement.

Proposition A.4.3. *Let $n \geq 3$ be an integer, let $M \in \mathscr{C}^{good}$ and write $M^{[1]} := M \cap \Phi_V^{[1]}$. Then there exists a function $f^{[1]} \colon \Phi_V \setminus M \to \mathbb{R}_{\geq 0}$ with the following properties:*

1. $\sum_{a \in \Phi_V \setminus M} f^{[1]}(a) < \#M^{[1]}$;
2. *the vector*

$$(2n-2)t_1 + (2n-2)s_1 - \sum_{a \in M^{[1]}} a + \sum_{a \in \Phi_V \setminus M} f^{[1]}(a)a \tag{A.4.2}$$

has strictly positive coefficients with respect to the basis S_G.

Proof. Note that if the proposition is true for M, it is also true for $\omega(M)$ for every $\omega \in \Omega$. We may therefore replace M by a Ω-conjugate in what follows. We also note that it suffices to find for each $M \in \mathscr{C}^{good}$ a function $f^{[1]} \colon \Phi_V \setminus M \to \mathbb{R}_{\geq 0}$ that satisfies the first property and such that (A.4.2) has nonnegative (instead of positive) coefficients with respect to S_G. Indeed, by Lemma A.4.1, every element of $\beta \in S_G$ is a sum $a_1 + a_2$ of two elements of $\Phi_V \setminus M$ so by adding to $f^{[1]}$ the function $a_1 \mapsto \varepsilon, a_2 \mapsto \varepsilon$ for some very small ε, we may ensure that $f^{[1]}$ has strictly positive coefficient at every element of S_G.

We will distinguish three cases, after introducing some notation. We say $M \in \mathscr{C}^{good}$ is *bounded* if there exists a function $f^{[1]} \colon \Phi_V \setminus M \to \mathbb{R}_{\geq 0}$ satisfying the conclusions of Proposition A.4.3. If $M \in \mathscr{C}^{good}$ we write $w_1(M) := (2n-2)t_1 + (2n-2)s_1 - \sum_{a \in M^{[1]}} a$. Recall that if $n+1 \leq i \leq 2n$ then we write $t_i := -t_{2n+1-i}$ and $s_i := -s_{2n+1-i}$. We use $O(\geq 0)$ as a shorthand for an element of $X^*(T')$ that has nonnegative coordinates with respect to S_G. We also recall the useful formulae (A.1.4).

Case 1. Suppose that $M^{[1]} \subset \{t_1 - s_n, t_1 + s_n, \dots, t_1 + s_1, \dots, t_n + s_1, -t_n + s_1\}$. Let a (respectively b) be the number of elements of $M^{[1]}$ contained in the first row (respectively last column). Then $1 \le a, b \le n+1$ and since we may switch the roles of t_n and $-t_n$ and similarly for $\pm s_n$, we may assume that $M^{[1]} = \{t_1 + s_a, \dots, t_1 + s_1, \dots, t_b + s_1\}$. Using the Ω-action we may assume that $a \ge b$. We have

$$\begin{aligned} w_1(M) = {} & (2n-2-a)t_1 - t_2 - \cdots - t_b \\ & + (2n-2-b)s_1 - s_2 - \cdots - s_a. \end{aligned}$$

If $a, b \le n-1$, then (A.1.4) shows that $w_1(M)$ has positive S_G coefficients, so M is evidently bounded. We may therefore assume that $a = n$ or $n+1$. A computation shows that the coefficients of $w_1(M)$ at $\{\beta_1, \dots, \beta_{n-2}\} \cup \{\gamma_1, \dots, \gamma_{n-2}\}$ are nonnegative (in fact at least $n+1-a$), so we focus on the coefficients at $\beta_{n-1}, \beta_n, \gamma_{n-1}, \gamma_n$. If $b \le n-1$, then $w_1(M) = O(\ge 0) + \frac{1}{2}(n-a)(\beta_{n-1} + \beta_n)$. This is negative only when $a = n+1$, so assume that this is the case. Using Lemma A.4.1, write $\beta_{n-1} = a_1 + a_2, \beta_n = a_3 + a_4$ for some $a_i \in \Phi_V \setminus M$. Choose a function $f^{[1]}\colon \Phi_V \setminus M \to \mathbb{R}_{\ge 0}$ such that $f^{[1]}$ supported on $\{a_1, \dots, a_4\}$, such that $\sum_{a \in \Phi_V \setminus M} f^{[1]}(a)a = \frac{1}{2}(\beta_{n-1} + \beta_n)$ and such that $\sum_{a \in \Phi_V \setminus M} f^{[1]}(a) < \#M^{[1]}$. Such a function exists since $2 < \#M^{[1]}$ and shows that M is bounded in this case.

It remains to treat the case where $n \le a, b \le n+1$. A calculation shows that

$$w_1(M) = \begin{cases} O(\ge 0) - \frac{1}{2}\beta_n - \frac{1}{2}\gamma_n & \text{if } (a,b) = (n,n), \\ O(\ge 0) - \beta_n & \text{if } (a,b) = (n+1,n), \\ O(\ge 0) - \frac{1}{2}(\beta_{n-1} + \beta_n + \gamma_{n-1} + \gamma_n) & \text{if } (a,b) = (n+1,n+1). \end{cases}$$

In each of these cases, we can use Lemma A.4.1 to show that M is bounded.

Case 2. Suppose that $M^{[1]}$ contains an element of the form $t_1 - s_a$ with $2 \le a \le n-1$ and is contained in the set $\{t_1 - s_a, \dots, t_1 + s_1, \dots, t_n + s_1, -t_n + s_1\}$. Let b be the number of elements of $M^{[1]}$ contained in the last column, so that $\#M^{[1]} = (n-a) + n + b$. Then $1 \le b \le n+1$, and by using the Ω-action we may assume that $M^{[1]} = \{t_1 - s_a, \dots, t_1 + s_1, \dots, t_b + s_1\}$. We have

$$\begin{aligned} w_1(M) = {} & (a-3)t_1 - t_2 - \cdots - t_b \\ & + (2n-2-b)s_1 - s_2 - \cdots - s_{a-1}. \end{aligned}$$

By assumption $t_1 - s_{a-1} \in \Phi_V \setminus M$ and $2n-a-b \geq 0$. We compute that

$$w_1(M) + (2n-a-b)(t_1 - s_{a-1}) = (2n-b-3)t_1 - t_2 - \cdots - t_b + O(\geq 0) \qquad \text{(A.4.3)}$$

All the S_G coefficients of the above expression are nonnegative unless $2n-b-2-b < 0$, in other words unless $b \geq n$. Therefore if $b < n$ the function $f^{[1]}$ mapping $t_1 - s_{a-1}$ to $2n-a-b$ and all other elements of $\Phi_V \setminus M$ to zero shows that M is bounded, since $2n-a-b < \#M^{[1]} = 2n-a+b$. If $b = n$, (A.4.3) equals $O(\geq 0) - \beta_n$. Therefore Lemma A.4.1 and the inequality $(2n-a-b)+2 < \#M^{[1]}$ show that M is bounded in this case. If $b = n+1$, (A.4.3) equals $O(\geq 0) - \beta_{n-2} - \beta_{n-1} - \beta_n$. Therefore Lemma A.4.1 and the inequality $(2n-a-b)+6 < \#M^{[1]}$ (which holds since $n \geq 3$) show that M is again bounded in this case.

Case 3. Suppose that $M^{[1]}$ is of the form $\{t_1 - s_a, \ldots, t_1 - s_n, t_1 + s_n, \ldots, t_1 + s_1, \ldots, t_n + s_1, -t_n + s_1, \ldots, -t_b + s_1\}$ for some $2 \leq a, b \leq n-1$. Using the Ω-action we may assume that $a \geq b$. A calculation using (A.1.4) shows that

$$\begin{aligned}
w_1(M) &= (a-3)t_1 - t_2 - \cdots - t_{b-1} \\
&\quad + (b-3)s_1 - s_2 - \cdots - s_{a-1} \\
&= (a-3)\beta_1 + \cdots + (a-b-1)\beta_{b-1} + \cdots + (a-b-1)\beta_{n-2} + \frac{1}{2}(a-b-1)(\beta_{n-1} + \beta_n) \\
&\quad + (b-3)\gamma_1 + \cdots + (b-a-1)\gamma_{a-1} + \cdots + (b-a-1)\gamma_{n-2} + \frac{1}{2}(b-a-1)(\gamma_{n-1} + \gamma_n).
\end{aligned}$$

By assumption $s_1 - t_{b-1} \in \Phi_V \setminus M$ and $a \geq b$, and we compute that

$$\begin{aligned}
w_1(M) + (a-b)(s_1 - t_{b-1}) &= O(\geq 0) - \beta_{b-1} - \cdots - \beta_{n-2} - \frac{1}{2}(\beta_{n-1} + \beta_n) \\
&\quad + O(\geq 0) - \gamma_{a-1} - \cdots - \gamma_{n-2} - \frac{1}{2}(\gamma_{n-1} + \gamma_n).
\end{aligned}$$

Therefore to prove that M is bounded it suffices to prove (using Lemma A.4.1) that

$$(a-b) + 2((n-b+1) + (n-a+1)) < \#M^{[1]} = 4n-a-b+1.$$

This inequality is equivalent to $2b > 3$, which is true since $b \geq 2$.

Conclusion. Since $M \in \mathscr{C}^{good}$, every M has an Ω-conjugate that falls under one of the above three cases. $\square$