

On the arithmetic of simple singularities of type E

Beth Romano and Jack A. Thorne

July 13, 2017

Abstract

An ADE Dynkin diagram gives rise to a family of algebraic curves. In this paper, we use arithmetic invariant theory to study the integral points of the curves associated to the exceptional diagrams E_6, E_7, E_8 . These curves are non-hyperelliptic of genus 3 or 4. We prove that a positive proportion of each family consists of curves with integral points everywhere locally but no integral points globally.

Contents

1	Introduction	2
2	A stable grading	5
2.1	Definition of the grading	5
2.2	Transverse slices over $V//G$	7
2.3	Reducibility conditions	11
2.4	Roots and weights	12
2.4.1	Case E_7	13
2.4.2	Case E_8	13
3	Integral structures, measures, and orbits	14
3.1	Integral structures and measures	14
3.2	Selmer elements and integral orbits	16
3.3	Subsets of $V(\mathbb{R})$ and $V(\mathbb{Q}_p)$	19
4	Counting points	22
5	Applications to 2-Selmer sets	26

5.1 Applications in Case E ₇	26
5.2 Applications in Case E ₈	29

1 Introduction

Background. Consider the following families of affine plane curves over \mathbb{Q} :

$$y^3 = x^4 + y(c_2x^2 + c_5x + c_8) + c_6x^2 + c_9x + c_{12} \quad (1.1)$$

$$y^3 = x^3y + c_{10}x^2 + x(c_2y^2 + c_8y + c_{14}) + c_6y^2 + c_{12}y + c_{18} \quad (1.2)$$

$$y^3 = x^5 + y(c_2x^3 + c_8x^2 + c_{14}x + c_{20}) + c_{12}x^3 + c_{18}x^2 + c_{24}x + c_{30}. \quad (1.3)$$

These families arise as versal deformations of the simple plane singularities of types E_6 , E_7 , and E_8 , respectively (see [Tho13]). In each family, the singularity can be recovered by setting all coefficients c_i equal to 0; yet the generic member of each family is smooth, and its smooth projective completion acquires rational points at infinity. Thus it is natural to study the arithmetic of these families of pointed smooth projective curves. The study of these families can be viewed as a variation on a classical theme: if we started instead with the singularity of type A_2 (given by the equation $y^2 = x^3$), then we would be studying the arithmetic of elliptic curves in standard Weierstrass form.

We recall that if Y is a smooth projective curve over a global field k and $P \in Y(k)$ is a rational point, then one can define the 2-Selmer set $\text{Sel}_2 Y$ of the curve Y ; it is a subset of the 2-Selmer group of the Jacobian of Y that serves as a cohomological proxy for the set $Y(k)$ of k -rational points. In the paper [Tho15], the second author studied the behaviour of the 2-Selmer sets of the curves in the family (1.1), proving the following theorem ([Tho15, Theorem 4.3]):

Theorem 1.1. *Let $\mathcal{F}_0 \subset \mathbb{Z}^6$ denote the set of tuples $(c_2, c_5, c_8, c_6, c_9, c_{12}) \in \mathbb{Z}^6$ such that the affine curve given by equation (1.1) is smooth (over \mathbb{Q}). If $b \in \mathcal{F}_0$, then call $\text{ht}(b) = \sup_i |c_i(b)|^{72/i}$ the height of b , and let Y_b denote the smooth projective completion of the fibre X_b as an algebraic curve over \mathbb{Q} . If $\mathcal{F} \subset \mathcal{F}_0$ is a subset defined by congruence conditions, then we have*

$$\limsup_{a \rightarrow \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ \text{ht}(b) < a}} \#\text{Sel}_2(Y_b)}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} < \infty.$$

Moreover, for any $\epsilon > 0$, we can find a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions such that

$$1 \leq \limsup_{a \rightarrow \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ \text{ht}(b) < a}} \#\text{Sel}_2(Y_b)}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} < 1 + \epsilon.$$

For the definition of a subset defined by congruence conditions, see (1.4) below. This theorem has the following Diophantine consequence ([Tho15, Theorem 4.8]):

Theorem 1.2. *Let $\epsilon > 0$, and let \mathcal{F}_0 be as in the statement of Theorem 1.2. If $b \in \mathcal{F}_0$, let \mathcal{X}_b denote the affine curve over \mathbb{Z} given by the equation (1.1). Then there exists a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions that satisfies the following conditions:*

1. For every $b \in \mathcal{F}$ and for every prime p , $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$.

2. We have

$$\liminf_{a \rightarrow \infty} \frac{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a, \mathcal{X}_b(\mathbb{Z}) = \emptyset\}}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} > 1 - \epsilon.$$

In other words, a positive proportion of curves in the family (1.1) have no \mathbb{Z} -points despite having \mathbb{Z}_p -points for every prime p . (The presence of marked points at infinity implies that for every $b \in \mathcal{F}_0$, the curve \mathcal{X}_b also has \mathbb{R} -points.)

The results of this paper. The goal of this paper is to generalize these results to the other two families (1.2) and (1.3) described above. The techniques we use are broadly similar to those of [Tho15], and are based around the relation, introduced in [Tho13], between the arithmetic of these families of curves and certain Vinberg representations associated to the corresponding root systems. We study this relation and then employ the orbit-counting techniques of Bhargava to prove our main theorems. We refer the reader to [Tho15, Introduction] for a more detailed discussion of these ideas.

In order to state the main theorems of this paper precisely, we must introduce some more notation. We will find it convenient to state our results in parallel for the two families (1.2) and (1.3). When it is necessary to split into cases, we will say that we are either in Case **E₇** or in Case **E₈**. We specify the following notation:

Case **E₇**: We let \mathcal{B} denote the affine scheme $\mathbb{A}_{\mathbb{Z}}^7$ with coordinates $(c_2, c_6, c_8, c_{10}, c_{12}, c_{14}, c_{18})$, and let $B = \mathcal{B}_{\mathbb{Q}}$. We let $\mathcal{X} \subset \mathbb{A}_{\mathcal{B}}^2$ denote the affine curve over \mathcal{B} given by the equation (1.2), and $X = \mathcal{X}_{\mathbb{Q}}$. We let $Y \rightarrow B$ denote the family of projective curves defined in [Tho13, Lemma 4.9] (this family is a fibre-wise compactification of X that is smooth at infinity. It can be realized as the closure of X in \mathbb{P}_B^2). We let \mathcal{F}_0 denote the set of $b \in \mathcal{B}(\mathbb{Z})$ such that X_b is smooth. If $b \in \mathcal{F}_0$, then we define $\text{ht}(b) = \sup_i |c_i(b)|^{126/i}$.

Case **E₈**: We let \mathcal{B} denote the affine scheme $\mathbb{A}_{\mathbb{Z}}^8$ with coordinates $(c_2, c_8, c_{12}, c_{14}, c_{18}, c_{20}, c_{24}, c_{30})$, and let $B = \mathcal{B}_{\mathbb{Q}}$. We let $\mathcal{X} \subset \mathbb{A}_{\mathcal{B}}^2$ denote the affine curve over \mathcal{B} given by the equation (1.3), and $X = \mathcal{X}_{\mathbb{Q}}$. We let $Y \rightarrow B$ denote the family of projective curves defined in [Tho13, Lemma 4.9] (again, this family is a fibre-wise compactification of X that is smooth at infinity. It can be realized as the closure of X in a suitable weighted projective space over B). We let \mathcal{F}_0 denote the set of $b \in \mathcal{B}(\mathbb{Z})$ such that X_b is smooth. If $b \in \mathcal{F}_0$, then we define $\text{ht}(b) = \sup_i |c_i(b)|^{240/i}$.

In either case, we say that a subset $\mathcal{F} \subset \mathcal{F}_0$ is defined by congruence conditions if there exist distinct primes p_1, \dots, p_s and a non-empty open compact subset $U_{p_i} \subset \mathcal{B}(\mathbb{Z}_{p_i})$ for each $i \in \{1, \dots, s\}$ such that

$$\mathcal{F} = \mathcal{F}_0 \cap (U_{p_1} \times \dots \times U_{p_s}), \quad (1.4)$$

where we are taking the intersection inside $\mathcal{B}(\mathbb{Z}_{p_1}) \times \dots \times \mathcal{B}(\mathbb{Z}_{p_s})$. Our first main result is then as follows.

Theorem 1.3. 1. Let $\mathcal{F}_0 \subset \mathcal{F}$ be a subset defined by congruence conditions. Then we have

$$\limsup_{a \rightarrow \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ \text{ht}(b) < a}} \#\text{Sel}_2(Y_b)}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} < \infty.$$

2. For any $\epsilon > 0$, we can find a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions such that

$$\limsup_{a \rightarrow \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ \text{ht}(b) < a}} \#\text{Sel}_2(Y_b)}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} < \begin{cases} 2 + \epsilon & \text{Case E}_7; \\ 1 + \epsilon & \text{Case E}_8. \end{cases}$$

(We note that the average in Case **E₇** is at least 2, because the family of curves (1.2) has two marked points at infinity; for a generic member of this family, these rational points define distinct elements inside the 2-Selmer set $\text{Sel}_2 Y_b$). In either case, we can apply Theorem 1.3 to deduce the following consequence.

Theorem 1.4. Let $\epsilon > 0$. Then there exists a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions satisfying the following conditions:

1. For every $b \in \mathcal{F}$ and for every prime p , $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$.

2. We have

$$\liminf_{a \rightarrow \infty} \frac{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a, \mathcal{X}_b(\mathbb{Z}) = \emptyset\}}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} > 1 - \epsilon.$$

Informally, we have shown that a positive proportion of each of the families (1.2) and (1.3) consists of curves with \mathbb{Z}_p -points for every prime p but no \mathbb{Z} -points.

Methodology. We now describe some new aspects of the proofs of Theorem 1.3 and Theorem 1.4. The main steps of our proofs are the same as those of [Tho15]: we combine the parameterization (constructed in [Tho13]) of 2-Selmer elements by rational orbits in a certain representation (G, V) arising from a graded Lie algebra with a technique of counting integral orbits (i.e. of the group $G(\mathbb{Z})$ in the set $V(\mathbb{Z})$). We thus gain information about the average size of 2-Selmer sets.

Although our proofs are similar in outline to those of [Tho15], we need to introduce several new ideas here. For example, the most challenging technical step in the argument is to eliminate the contribution of integral points which lie ‘in the cusp’. (In the notation of Section 2.3, these points correspond to vectors v such that $v_{\alpha_0} = 0$, where α_0 is the highest root in the ambient Lie algebra \mathfrak{h} .) For this step we prove an optimized criterion (Proposition 2.15) for when certain vectors are reducible (this implies that they cannot contribute to the nontrivial part of the 2-Selmer set of a smooth curve in our family). This criterion is based in large part on the Hilbert–Mumford stability criterion. Its application in this context is very natural, but seems to be new.

We then use a computer to carry out a formidable computation to bound the contribution of the parts of the cuspidal region that are not eliminated by this criterion (see Proposition 4.5). For comparison, we note that in [Tho15], the cuspidal region was broken up into 68 pieces; here the analogous procedure leads to a decomposition into 1429 (resp. 9437 pieces) in Case **E**₇ (resp. in Case **E**₈). It would be very interesting if one could discover a ‘pure thought’ way to tackle this problem that does not rely on case-by-case calculations.

The current setting also differs from that of [Tho15] in that the curves of family (1.2) have more than one marked point at infinity. (The geometric reason for this is that the projective tangent line to a flex point P of a plane quartic curve intersects the curve in exactly one other point Q . This implies that the family (1.2), essentially the universal family of plane quartics with a marked flex point, has two canonical sections.) We find that the orbits that parameterize the divisor classes arising from these points match up in a very pleasant way with a certain subgroup of the Weyl group of the ambient Lie algebra \mathfrak{h} ; see in particular Lemma 2.5.

It remains an interesting open problem to generalize the results of this paper and of [Tho15] to study the average size of the 2-Selmer group of the Jacobians of the curves in (1.1) – (1.3) (and not just the size of their 2-Selmer sets). The rational orbits necessary for this study were constructed in [Tho16], but we do not yet understand how to construct integral representatives for these orbits, in other words, how to prove the analogue of Lemma 3.5 below after replacing the set $Y_b(\mathbb{Q}_p)$ by $J_b(\mathbb{Q}_p)$. If this can be achieved, then the work we do in this paper to bound the contribution of the cuspidal region will suffice to obtain the expected upper bound on the average size of the 2-Selmer group (namely 6 in Case **E**₇ and 3 in Case **E**₈).

Notation. Given a connected reductive group H and a maximal torus $T \subset H$, we write $X^*(T) = \text{Hom}(T, \mathbb{G}_m)$ for the character group of T , $X_*(T)$ for the cocharacter group of T , and $W(H, T)$ for the (absolute) Weyl group of H with respect to T . Similarly, if \mathfrak{c} is a Cartan subalgebra of $\mathfrak{h} = \text{Lie}(H)$, then we write $\Phi(\mathfrak{h}, \mathfrak{c})$ for the roots of \mathfrak{c} and $W(H, \mathfrak{c})$ for the Weyl group of \mathfrak{c} . If $\alpha \in \Phi(\mathfrak{h}, \mathfrak{c})$, then we write $\mathfrak{h}_\alpha \subset \mathfrak{h}$ for the root space corresponding to α . We write $N_H(T)$ (resp. $N_H(\mathfrak{c})$) for the normalizer of T (resp. \mathfrak{c}) in H ,

and $Z_H(T)$ (resp. $Z_H(\mathfrak{c})$) for the associated centralizer. Similarly, if V is any subspace of \mathfrak{h} and $x \in \mathfrak{h}$, then we write $\mathfrak{z}_V(x)$ for the centralizer of x in V .

We write $\Lambda = \mathbb{R}_{>0}$ for the multiplicative group of positive reals, and $d^\times \lambda = d\lambda/\lambda$ for its Haar measure (where $d\lambda$ is the usual Lebesgue measure on the real line). If G is a group defined over a ring R , V is a representation of G , and $A \subset V$, then we write $G(R) \backslash A$ for the set of equivalence classes of A under the relation $a \sim a'$ if there exists $\gamma \in G(R)$ such that $\gamma a = a'$.

Acknowledgements. During the period in which this research was conducted, Jack Thorne served as a Clay Research Fellow. Both of the authors were supported in part by EPSRC First Grant EP/N007204/1. We thank Fabrizio Barroero for useful conversations.

2 A stable grading

In this section we establish the algebraic foundation for the proofs of our main theorems: in each of our two cases, we describe the parameterization of certain 2-coverings of Jacobians of algebraic curves by orbits in a representation arising from a $\mathbb{Z}/2\mathbb{Z}$ -graded Lie algebra. Our set-up parallels that of [Tho15]; however, we must address the complications arising from the presence of an additional point at infinity on the curves in the family (1.2). This point makes its presence known in the disconnectedness of the group H^θ defined below and in the fact that the central fibre of the family (1.2) is not irreducible.

2.1 Definition of the grading

Let k be a field of characteristic 0 with fixed separable closure k^s , and let H be a simple adjoint group over k of rank r that is equipped with a k -split maximal torus T . Let $\mathfrak{h} = \text{Lie}(\mathfrak{h})$ and $\mathfrak{t} = \text{Lie}(\mathfrak{t})$. We let $\Phi_H = \Phi(H, T)$ and choose a set of simple roots $S_H = \{\alpha_1, \alpha_2, \dots, \alpha_r\} \subset \Phi_H$. We also choose a Chevalley basis for \mathfrak{h} with root vectors $\{e_\alpha \mid \alpha \in \Phi_H\}$. Suppose that -1 is an element of the Weyl group $W(H, T)$ (this is true, e.g., if H has type E_7 or E_8 , but not if H has type E_6). Let $\check{\rho} \in X_*(T)$ be the sum of the fundamental coweights with respect to our choice of simple roots S_H . Then, up to conjugation by $H(k)$, the automorphism $\theta := \text{Ad}(\check{\rho}(-1))$ is the unique involution of H such that $\mathfrak{h}^{d\theta=-1}$ contains a regular nilpotent element of \mathfrak{h} ([Tho13, Corollary 2.15]). The grading induced by this involution is stable in the sense of [RLYG12, §5.3].

We define $G = (H^\theta)^\circ$ and $V = \mathfrak{h}^{d\theta=-1}$. Then G is a split semisimple group, and V is an irreducible representation of G , of the type studied by Kostant–Rallis in the case $k = \mathbb{C}$ [KR71]. The invariant theory of V is closely related to that of the adjoint representation of H . We now summarize some aspects of the invariant theory of the pair (G, V) , most of which may be found in [KR71], [Vin76], or [Pan05]. We refer the reader to [Tho13, §2] for detailed references.

Definition 2.1. Let $\mathfrak{c} \subset \mathfrak{h}$ be a Cartan subalgebra. If $\mathfrak{c} \subset V$, then \mathfrak{c} is called a Cartan subspace of V .

Theorem 2.2. 1. Any two Cartan subspaces $\mathfrak{c}, \mathfrak{c}' \subset V$ are conjugate by an element of $G(k^s)$.

2. Let $\mathfrak{c} \subset V$ be a Cartan subspace, and define $W(G, \mathfrak{c}) = N_G(\mathfrak{c})/Z_G(\mathfrak{c})$. Then the natural maps

$$W(G, \mathfrak{c}) \rightarrow W(H, \mathfrak{c})$$

and

$$k[\mathfrak{h}]^H \rightarrow k[V]^G \rightarrow k[\mathfrak{c}]^{W(G, \mathfrak{c})}$$

are isomorphisms. In particular, $k[V]^G$ is isomorphic to a polynomial algebra on $r = \text{rank } H$ generators.

Let us call a vector $v \in V$ semisimple (resp. nilpotent, resp. regular) if it has this property when viewed as an element of \mathfrak{h} . We have the following proposition:

Proposition 2.3. *Let $v \in V$.*

1. *The components of the Jordan decomposition $v = v_s + v_n$ in \mathfrak{h} in fact lie in V .*
2. *The vector v has a closed G -orbit in V if and only if it is semisimple.*
3. *The stabilizer of v in G is finite (and hence the G -orbit of v has maximal dimension) if and only if v is regular.*

We see in particular that a vector $v \in V$ has both a closed orbit and a finite stabilizer (i.e. v is stable in the sense of [Mum77]) if and only if it is regular semisimple. Let $\tilde{\Delta} \in k[\mathfrak{h}]^H$ be the image under the isomorphism $k[\mathfrak{t}]^{W(H,T)} \rightarrow k[\mathfrak{h}]^H$ of the product of all roots $\alpha \in \Phi_H$. Then $\tilde{\Delta}(v) \neq 0$ if and only if $v \in \mathfrak{h}$ is regular semisimple. We call $\Delta := \tilde{\Delta}|_V$ the discriminant polynomial. Then Δ is homogeneous of degree $\#\Phi_H$. If $v \in V$ is a vector such that $\Delta(v) \neq 0$, then $\mathfrak{z}_{\mathfrak{h}}(v) \subset V$, and $\mathfrak{z}_{\mathfrak{h}}(v)$ is the unique Cartan subspace of V containing v .

Before stating the next result, we review some basic definitions from geometric invariant theory. Recall that given a one-parameter subgroup $\lambda : \mathbb{G}_m \rightarrow G_{k^s}$, we may decompose $V(k^s)$ as $\bigoplus_{i \in \mathbb{Z}} V_i$, where $V_i = \{v \in V(k^s) \mid \lambda(t) \cdot v = t^i v\}$. If we decompose a vector $v \in V$ as $v = \sum v_i$ where $v_i \in V_i$ for all i , then $\{i \mid v_i \neq 0\}$ is called the set of weights for v with respect to λ .

Corollary 2.4. *Let $v \in V$. Then the following are equivalent:*

1. *v is regular semisimple.*
2. *$\Delta(v) \neq 0$.*
3. *For any nontrivial one-parameter subgroup $\lambda : \mathbb{G}_m \rightarrow G_{k^s}$, the vector v has a positive weight with respect to λ .*

Proof. What remains to be shown is that the third condition is equivalent to the vector v having a closed orbit and a finite stabilizer in G . This is the Hilbert–Mumford stability criterion (see e.g. [Mum77]). \square

We now describe G and V more explicitly. By our definition of θ , it is clear that $T \subset G$. Let $\Phi_G = \Phi(G, T)$; then $\Phi_G \subset \Phi_H$, and the complement $\Phi_V := \Phi_H - \Phi_G$ is the set of weights for the action of T on V . The Weyl group $W_G := W(G, T)$ is the subgroup of $W_H := W(H, T)$ generated by reflections corresponding to the roots of Φ_G .

Lemma 2.5. *Let $s = \check{\rho}(-1) \in T(k)$.*

1. *The stabilizer of s under the action of W_H on T is given by $\text{Stab}_{W_H}(s) = \{w \in W_H \mid w(\Phi_G) = \Phi_G\}$.*
2. *There is a split short exact sequence of groups*

$$1 \longrightarrow W_G \longrightarrow \text{Stab}_{W_H}(s) \longrightarrow H^\theta/G \longrightarrow 1.$$

More precisely, let $S_G \subset \Phi_G$ be a choice of root basis and define

$$\Omega = \{w \in W_H \mid w(S_G) = S_G\} \subset \text{Stab}_{W_H}(s).$$

Then $\text{Stab}_{W_H}(s) \simeq W_G \rtimes \Omega$, and the inclusion $N_{H^\theta}(T) \hookrightarrow H^\theta$ induces an isomorphism $\Omega \simeq H^\theta/G$.

We remark that if H is of type E_7 , then the group H^θ/G has order 2; if H is of type E_8 , then H^θ/G is trivial.

Proof. For the first item, note that since H is adjoint, $w \cdot s$ is completely determined by its action on the root spaces \mathfrak{h}_α . We have that $w \cdot s$ acts trivially on \mathfrak{h}_α if and only if $\alpha \in w^{-1}(\Phi_G)$, and otherwise $w \cdot s$ acts on \mathfrak{h}_α as multiplication by -1 . For the second item, note that by item 1, the group $\text{Stab}_{W_H}(s)$ is a subgroup of $\text{Aut}(\Phi_G) \simeq W_G \rtimes D$, where $D = \{\sigma \in \text{Aut}(\Phi_G) \mid \sigma(S_G) = S_G\}$. Clearly $W_G \subset \text{Stab}_{W_H}(s)$ and $\text{Stab}_{W_H}(s) \cap D = \Omega$, so $\text{Stab}_{W_H}(s) \simeq W_G \rtimes \Omega$. The isomorphism with H^θ/G follows from [Hum95, Section 2.2]. \square

2.2 Transverse slices over $V/\!/G$

We continue to use the notation of §2.1, and now begin our study of the categorical quotient map

$$\pi : V \rightarrow B,$$

where $B = V/\!/G = \text{Spec } k[V]^G$. If $b \in B(k)$, we write $V_b = \pi^{-1}(b)$ for the corresponding fibre. We can write down sections of the map π using the theory of \mathfrak{sl}_2 -triples. We recall that an \mathfrak{sl}_2 -triple in \mathfrak{h} is a tuple (e, h, f) of elements of $\mathfrak{h} - \{0\}$ satisfying the relations

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

We call an \mathfrak{sl}_2 -triple normal if $e, f \in V$ and $h \in \mathfrak{h}^\theta$. A graded version of the Jacobson–Morozov theorem ([Tho13, Lemma 2.17]) states that if $e \in V$ is a non-zero nilpotent element, then there exists a normal \mathfrak{sl}_2 -triple containing it. If (e, h, f) is a normal \mathfrak{sl}_2 -triple, then we define $S_{(e, h, f)} = e + \mathfrak{z}_{\mathfrak{h}}(f) \cap V \subset V$. Then $S_{(e, h, f)}$ is an affine linear subspace containing e , and one can show ([Tho13, Proposition 3.4]) that the map $\pi|_{S_{(e, h, f)}} : S_{(e, h, f)} \rightarrow B$ is faithfully flat, with smooth generic fibre. If we let $\lambda : \mathbb{G}_m \rightarrow H$ be the cocharacter such that $d\lambda(1) = h$, then we may define a contracting action of \mathbb{G}_m on $S_{(e, h, f)}$ by $t \cdot v = t^2\lambda(t^{-1})v$. With this action on $S_{(e, h, f)}$, if \mathbb{G}_m acts on B by the square of its usual action, then $\pi|_{S_{(e, h, f)}}$ is \mathbb{G}_m -equivariant (see [Tho13, §3]). If e is regular nilpotent, then we call $S_{(e, h, f)}$ a Kostant section.¹

We consider these affine subspaces for the \mathfrak{sl}_2 -triples corresponding to two conjugacy classes of nilpotent elements, namely the regular and subregular classes.

Proposition 2.6. *Let $E \in V$ be a regular nilpotent element. Then:*

1. *There exists a unique normal \mathfrak{sl}_2 -triple containing E . Let κ be the Kostant section associated to this \mathfrak{sl}_2 -triple. Then $\pi|_\kappa$ is an isomorphism.*
2. *Let $b \in B(k)$, and let $\kappa_b = (\pi|_\kappa)^{-1}(b)$. If $\Delta(b) \neq 0$, then V_b forms a single $G(k^s)$ -orbit. Consequently, there is a canonical bijection*

$$G(k) \backslash V_b(k) \cong \ker[H^1(k, Z_G(\kappa_b)) \rightarrow H^1(k, G)],$$

where the $G(k)$ -orbit of $\kappa_b \in V_b(k)$ corresponds to the neutral element of $H^1(k, Z_G(\kappa_b))$.

Proof. The first part follows from work of Kostant and Rallis as applied in [Tho13]: see especially lemmas 2.17 and 3.5. The second part follows from [BG14, Proposition 1] as applied in [Tho13, Proposition 4.13]. \square

¹We note that the definition of a Kostant section is often more general than the one stated here, but in this paper we restrict our attention to sections of this form.

For $b \in B(k)$, we continue to write κ_b for the fibre over b . We observe that if H has type E_7 , then there are two G -conjugacy classes of regular nilpotent elements in V . If H has type E_8 , then there is a single G -conjugacy class of regular nilpotent elements (see [Tho13, Corollary 2.25]). In either case, two regular nilpotent elements $E, E' \in V(k)$ are $G(k)$ -conjugate if and only if they are $G(k^s)$ -conjugate (see e.g. [Tho13, Lemma 2.14]). Combined with the first part of Proposition 2.6, this implies a strong uniqueness property for the sections $\kappa \rightarrow B$:

Corollary 2.7. *Let $\kappa, \kappa' \subset V$ be Kostant sections.*

1. *We have $\kappa = \kappa'$ if and only if $\kappa_0 = \kappa'_0$.*
2. *The sections κ and κ' are $G(k)$ -conjugate if and only if κ_0 and κ'_0 lie in the same $G(k^s)$ -orbit in V .*

Next recall that V contains a subregular nilpotent element e (by definition, this means that e is nilpotent and $\dim \text{Stab}_G(e) = 1$; the existence of subregular nilpotents in V is proved in [Tho13, Proposition 2.27]). We now discuss the sections corresponding to such an element.

Theorem 2.8. *Let (e, h, f) be a normal \mathfrak{sl}_2 -triple, and suppose that e is subregular nilpotent element of \mathfrak{h} . Let $X = S_{(e, h, f)}$.*

1. *The fibres of $X \rightarrow B$ are reduced connected affine curves. If $b \in B(k)$, then X_b is smooth if and only if $\Delta(b) \neq 0$.*
2. *Let $b \in B(k)$, and suppose that $\Delta(b) \neq 0$. Let Y_b denote the smooth projective completion of X_b , and let $J_b = \text{Pic}^0 Y_b$ be the Jacobian of Y_b . There is a canonical isomorphism $J_b[2] \cong Z_G(\kappa_b)$ of finite étale k -groups, where κ is any choice of Kostant section.*

Proof. For the first part, see [Tho13, Theorem 3.8] and [Tho13, Corollary 3.16]. For the second part, see [Tho13, Corollary 4.12]. \square

The next two theorems identify the fibres of the morphism $X \rightarrow B$ in Theorem 2.8 when H has type E_7 or E_8 . We find it convenient to split into cases.

Theorem 2.9 (Case E_7). *Suppose that H is of type E_7 . Fix a choice of regular nilpotent E , and define κ as in Proposition 2.6. Also fix a normal \mathfrak{sl}_2 -triple (e, h, f) such that e is subregular nilpotent, and define $X = S_{(e, h, f)}$ as above.*

1. *We may choose homogeneous generators $c_2, c_6, c_8, c_{10}, c_{12}, c_{14}, c_{18}$ of $k[V]^G$ and functions $x, y \in k[X]$ so that $k[X]$ is isomorphic to a polynomial ring in the elements c_2, \dots, c_{14}, x, y , and the morphism $X \rightarrow B$ is determined by the relation (1.2):*

$$y^3 = x^3y + c_{10}x^2 + x(c_2y^2 + c_8y + c_{14}) + c_6y^2 + c_{12}y + c_{18}.$$

Moreover, the elements $c_2, c_6, c_8, c_{10}, c_{12}, c_{14}, c_{18}, x, y \in k[X]$ are eigenvectors for the action of \mathbb{G}_m on X mentioned above, with weights as in the following table:

c_2	c_6	c_8	c_{10}	c_{12}	c_{14}	c_{18}	x	y
4	12	16	20	24	28	36	8	12

2. *Let $Y \rightarrow B$ denote the natural compactification of $X \rightarrow B$ as a family of plane quartic curves, given in homogeneous coordinates as*

$$y_0^3z_0 = x_0^3y_0 + c_{10}x_0^2z_0^2 + x_0(c_2y_0^2z_0 + c_8y_0z_0^2 + c_{14}z_0^3) + c_6y_0^2z_0^2 + c_{12}y_0z_0^3 + c_{18}z_0^4.$$

This compactification has two sections P_1 and P_2 at infinity, given by the equations $[x_0 : y_0 : z_0] = [0 : 1 : 0]$ and $[x_0 : y_0 : z_0] = [1 : 0 : 0]$ respectively (note that P_1 is a flex point). Assume that under the bijection of [Tho13, Lemma 4.14] the section corresponding to E is P_1 . Then for each $b \in B(k)$ such that $\Delta(b) \neq 0$, the following diagram commutes:

$$\begin{array}{ccc} X_b(k) & \xrightarrow{\iota_b} & G(k) \setminus V_b(k) \\ \eta_b \downarrow & & \downarrow \gamma_b \\ J_b(k) & \xrightarrow{\delta_b} & H^1(k, J_b[2]), \end{array}$$

where the maps in the diagram are specified as follows. The top arrow ι_b is induced by the inclusion $X \hookrightarrow V$. The left arrow η_b is the restriction of the Abel–Jacobi map $P \mapsto [(P) - (P_1)]$. To define γ_b , we use Proposition 2.6 to obtain an injective homomorphism to $G(k) \setminus V_b(k) \rightarrow H^1(k, Z_G(\kappa_b))$, and then compose with the identification $Z_G(\kappa_b) \cong J_b[2]$ of Theorem 2.8. The bottom arrow δ_b is the connecting homomorphism associated to the Kummer exact sequence

$$0 \longrightarrow J_b[2] \longrightarrow J_b \xrightarrow{\times 2} J_b \longrightarrow 0.$$

Proof. In this theorem and the next, the first part (i.e. the explicit determination of the family X) is carried out in [Tho13, Theorem 3.8], the weights for the \mathbb{G}_m action are given in [Tho13, Proposition 3.6], and the second part is the content of [Tho13, Theorem 4.15]. \square

We note that, having fixed a choice of regular nilpotent E , we can always assume, after possibly replacing e by a $H^\theta(k)$ -conjugate, that E corresponds to P_1 under the bijection of [Tho13, Lemma 4.14] referred to in the second part of Theorem 2.9.

Theorem 2.10 (Case E_8). *Suppose that H is of type E_8 . Fix a choice of regular nilpotent E , and define κ as in Proposition 2.6. Also fix a normal \mathfrak{sl}_2 -triple (e, h, f) such that e is subregular nilpotent, and define $X = S_{(e, h, f)}$ as above.*

1. *We may choose homogeneous generators $c_2, c_8, c_{12}, c_{14}, c_{18}, c_{20}, c_{24}, c_{30}$ of $k[V]^G$ and functions $x, y \in k[X]$ so that $k[X]$ is isomorphic to a polynomial ring in the elements c_2, \dots, c_{24}, x, y , and the morphism $X \rightarrow B$ is determined by the relation (1.3):*

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

Moreover, the elements $c_2, c_8, c_{12}, c_{14}, c_{18}, c_{20}, c_{24}, c_{30}, x, y \in k[X]$ are eigenvectors for the action of \mathbb{G}_m on X mentioned above, with weights as in the following table:

c_2	c_8	c_{12}	c_{14}	c_{18}	c_{20}	c_{24}	c_{30}	x	y
4	16	24	28	36	40	48	60	12	20

2. *Let $Y \rightarrow B$ denote the compactification of $X \rightarrow B$ described in [Tho13, Lemma 4.9]. Let $P : B \rightarrow Y$ denote the unique section at infinity (so that $Y = X \cup P$). Then for each $b \in B(k)$ such that $\Delta(b) \neq 0$, the following diagram commutes:*

$$\begin{array}{ccc} X_b(k) & \xrightarrow{\iota_b} & G(k) \setminus V_b(k) \\ \eta_b \downarrow & & \downarrow \gamma_b \\ J_b(k) & \xrightarrow{\delta_b} & H^1(k, J_b[2]), \end{array}$$

where the maps in the diagram are specified as follows. The top arrow ι_b is induced by the inclusion $X \hookrightarrow V$. The left arrow η_b is the restriction of the Abel–Jacobi map $Q \mapsto [(Q) - (P)]$. To define γ_b , we

use Proposition 2.6 to obtain an injective homomorphism to $G(k) \backslash V_b(k) \rightarrow H^1(k, Z_G(\kappa_b))$, and then compose with the identification $Z_G(\kappa_b) \cong J_b[2]$ of Theorem 2.8. The bottom arrow δ_b is the connecting homomorphism associated to the Kummer exact sequence

$$0 \longrightarrow J_b[2] \longrightarrow J_b \xrightarrow{\times 2} J_b \longrightarrow 0.$$

Lemma 2.11. *In Case \mathbf{E}_7 , suppose $b \in B(k)$ is such that $\Delta(b) \neq 0$. Then $\delta_b([(P_2) - (P_1)])$ is in the image of $G(k) \backslash V_b(k)$ under γ_b , and $\delta_b([(P_2) - (P_1)])$ is nontrivial if and only if $H^0(k, Z_G(\kappa_b)) = H^0(k, Z_H(\kappa_b)[2])$.*

Proof. Let $\omega \in \Omega$ be the nontrivial element, and let $E' = \sum_{\alpha \in S_H} e_{\omega(\alpha)}$. Then E' is a regular nilpotent element of V . Since $H^\theta(k)$ acts simply transitively on the set of such elements, there is a unique element $w \in H^\theta(k)$ lifting ω such that $w(E) = E'$. Let κ' denote the Kostant section corresponding to E' . Then $w\kappa = \kappa'$ and so $\kappa'_b = w\kappa_b$. We claim that $\gamma_b(\kappa'_b) = \delta_b([(P_2) - (P_1)])$. The proof is essentially the same as the proof of [Tho, Theorem 5.3], but for the convenience of the reader, we give the details here. Let \bar{X}_b be the base change of X_b to the fixed separable closure k^s/k , and define \bar{Y}_b similarly. There is a short exact sequence of étale homology groups:

$$0 \longrightarrow \mu_2 \longrightarrow H_1(\bar{X}_b, \mathbb{F}_2) \longrightarrow H_1(\bar{Y}_b, \mathbb{F}_2) \longrightarrow 0. \quad (2.1)$$

There is a natural symplectic duality on $H_1(\bar{X}_b, \mathbb{F}_2)$ which has radical μ_2 , and which descends to the usual Poincaré duality (or Weil) pairing on $H_1(\bar{Y}_b, \mathbb{F}_2) = J_b[2]$. Through an explicit calculation, one can see that $\delta_b([(P_2) - (P_1)])$ is the image of the nontrivial element of μ_2 under the connecting homomorphism associated to the dual short exact sequence

$$0 \longrightarrow J_b[2] \longrightarrow H^1(\bar{X}_b, \mathbb{F}_2) \longrightarrow \mu_2 \longrightarrow 0,$$

where we have used the Weil pairing to identify $J_b[2]$ with its dual.

Let H^{sc} denote the simply connected cover of H with centre $A_{H^{\text{sc}}}$. Note that θ lifts naturally to an automorphism of H^{sc} , which will again denote by θ , and that because H^{sc} is simply connected, the fixed-point subgroup $G' := (H^{\text{sc}})^\theta$ is connected [Ste68, Theorem 8.1]. Let $C = Z_H(\kappa_b)$ and let $C^{\text{sc}} = Z_{H^{\text{sc}}}(\kappa_b)$. Then $C \subset H$ and $C^{\text{sc}} \subset H^{\text{sc}}$ are maximal tori, and we have $Z_{G'}(\kappa_b) = C^{\text{sc}}[2]$ and $Z_G(\kappa_b) = \text{im}(C^{\text{sc}}[2] \rightarrow C[2])$. It follows from the proof of [Tho13, Theorem 4.10] that the short exact sequence (2.1) is isomorphic to

$$0 \longrightarrow A_{H^{\text{sc}}} \longrightarrow C^{\text{sc}}[2] \longrightarrow Z_G(\kappa_b) \longrightarrow 0,$$

and its dual is isomorphic to

$$0 \longrightarrow Z_G(\kappa_b) \longrightarrow C[2] \longrightarrow \pi_0(H^\theta) \longrightarrow 0, \quad (2.2)$$

where we have used the W_H -invariant duality on $X_*(C)$ and the isomorphism $C[2]/Z_G(\kappa_b) \cong \pi_0(H^\theta)$; see also [Tho13, Corollary 2.12], which states that this Weyl-invariant duality descends to a non-degenerate symplectic alternating duality on $Z_G(\kappa_b)$.

Therefore to prove the claim we must show that $\gamma_b(\kappa'_b)$ is equal to the image in $H^1(k, Z_G(\kappa_b))$ of the nontrivial element of $\pi_0(H^\theta)$ under the connecting homomorphism associated with the short exact sequence (2.2). This follows from a computation with cocycles. Indeed, the second part of Proposition 2.6 asserts that there exists $g \in G(k^s)$ such that $\kappa'_b = g\kappa_b$. Then the cohomology class $\gamma_b(\kappa'_b)$ is represented by the cocycle $\sigma \mapsto g^{-1}(\sigma g)$. But $c := g^{-1}w \in Z_{H^\theta}(\kappa_b) = C[2]$ is a lift of the nontrivial element of $\pi_0(H^\theta)$, so the claim follows from the fact that ${}^\sigma cc^{-1} = ({}^\sigma cc^{-1})^{-1} = g^{-1}(\sigma g)$ for all $\sigma \in \text{Gal}(k^s/k)$.

We have established the claim, and the first part of the lemma. To finish the proof, we note that $\delta_b([(P_2) - (P_1)])$ is nontrivial if and only if the connecting homomorphism $\pi_0(H^\theta) \rightarrow H^1(k, Z_G(\kappa_b))$ is injective. By exactness, this is equivalent to the surjectivity of the map $H^0(k, Z_G(\kappa_b)) \rightarrow H^0(k, C[2])$, which is exactly the criterion given in the statement of the lemma. \square

Corollary 2.12. *In Case E₇, let $b \in B(k)$ be such that $\Delta(b) \neq 0$, and let $C = Z_H(\kappa_b)$. Suppose that the map $\text{Gal}(k^s/k) \rightarrow W(H_{k^s}, C_{k^s})$ induced by the action of $\text{Gal}(k^s/k)$ on C_{k^s} is surjective. Then $\delta_b([(P_2) - (P_1)])$ is nontrivial in $H^1(k, J_b[2])$.*

Proof. By the lemma, it is equivalent to show that the map $H^0(k, Z_G(\kappa_b)) \rightarrow H^0(k, C[2])$ is surjective. We have $H^0(k, C[2]) = C^{W(H, C)}[2](k) = Z_H[2](k)$. Since the group H is adjoint, the centre Z_H is trivial, so the map $H^0(k, Z_G(\kappa_b)) \rightarrow H^0(k, C[2])$ is clearly surjective. \square

2.3 Reducibility conditions

We now define the notion of k -reducibility and study the properties of k -reducible elements of $V(k)$.

Definition 2.13. *Let $v \in V$. We say that v is k -reducible if $\Delta(v) = 0$ or if v is $G(k)$ -conjugate to an element of a Kostant section. Otherwise, we say that v is k -irreducible.*

The factors of the Cartan decomposition $\mathfrak{h} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi_H} \mathfrak{h}_\alpha$ are invariant under the action of θ ; this leads to a corresponding decomposition

$$V = \bigoplus_{\alpha \in \Phi_V} \mathfrak{h}_\alpha. \quad (2.3)$$

If $v \in V$, then we write $v = \sum_{\alpha \in \Phi_V} v_\alpha$ for the corresponding decomposition of v as a sum of T -eigenvectors. Now choose a set of simple roots $S_G = \{\beta_1, \dots, \beta_r\}$ of Φ_G . Since the β_i form a basis for $X^*(T) \otimes \mathbb{Q}$, each element $\gamma \in X^*(T)$ may be written uniquely as $\gamma = \sum_{i=1}^r n_i(\gamma) \beta_i$ for some $n_i(\gamma) \in \mathbb{Q}$. Our choice of simple roots $S_H \subset \Phi_H$ determines a set of positive roots Φ_H^+ . We write Φ_V^+ for $\Phi_H^+ \cap \Phi_V$.

Lemma 2.14. *Let $v \in V$ and decompose v as $\sum_{\alpha \in \Phi_V} v_\alpha$ as in (2.3). Suppose one of the following holds:*

1. *There exist rational numbers a_1, \dots, a_r not all equal to zero such that if $\alpha \in \Phi_V$ and $v_\alpha \neq 0$, then $\sum a_i n_i(\alpha) \leq 0$.*
2. *There exists $w \in \Omega$ such that $v_\alpha = 0$ if $\alpha \in w(\Phi_H^+ - S_H)$.*

Then v is k -reducible.

(We recall that the subgroup $\Omega \subset W_H$ was defined in Lemma 2.5.)

Proof. For the first part of the lemma, we will apply the criterion of Corollary 2.4. This corollary implies that if $v \in V$ and there exists a nontrivial cocharacter $\lambda \in X_*(T)$ such that v has no (strictly) positive weights with respect to λ , then $\Delta(v) = 0$. Let $\{\check{\omega}_1, \dots, \check{\omega}_r\} \subset X_*(T) \otimes \mathbb{Q}$ be the basis dual to the basis $\{\beta_1, \dots, \beta_r\}$ of $X^*(T) \otimes \mathbb{Q}$, and let $\lambda = \sum_{i=1}^r a_i \check{\omega}_i$. Then there exists a positive integer m such that $m\lambda \in X_*(T)$. The weights of v with respect to $m\lambda$ are exactly the values $\langle \alpha, m\lambda \rangle = m \sum_{i=1}^r a_i n_i(\alpha)$ for those $\alpha \in \Phi_V$ such that $n_i(\alpha) \neq 0$, so v has no positive weights with respect to $m\lambda$.

For the second item, let $E = \sum_{\alpha \in S_H} e_\alpha$, where each e_α is a root vector of our fixed Chevalley basis (see Section 2.1). Then E is a regular nilpotent element of V , and is therefore contained in a unique normal \mathfrak{sl}_2 -triple, which in turn determines a Kostant section $\kappa \subset V$ (see Proposition 2.6). Suppose that the vector $v \in V$ satisfies the condition $v_\alpha = 0$ if $\alpha \in \Phi_V^+ - S_H$. We may assume that if $\alpha \in S_H$, then $v_\alpha \neq 0$; otherwise v also satisfies the condition in the first part of the lemma. In this case, exactly the same argument as in the proof of [Tho15, Lemma 2.6] shows that v is $G(k)$ -conjugate to an element of κ , hence is k -reducible.

Now suppose that there is a nontrivial element $w \in \Omega$ such that the vector $v \in V$ satisfies the condition $v_\alpha = 0$ if $\alpha \in w(\Phi_V^+ - S_H)$. We can again assume that $v_\alpha \neq 0$ if $\alpha \in w(S_H)$. Let $E' = \sum_{\alpha \in w(S_H)} e_\alpha$, and let κ' be the Kostant section corresponding to E' . Since the group $H^\theta(k)$ acts simply transitively on the set of regular nilpotents of V ([Tho13, Lemma 2.14]), there is a unique element $x \in H^\theta(k)$ such that $x \cdot E' = E$. Then x normalizes the torus T , since $\mathfrak{t} = \text{Lie}(T)$ is the unique Cartan subalgebra of \mathfrak{h} containing the semisimple parts of the normal \mathfrak{sl}_2 -triples containing E and E' respectively. Thus x corresponds to an element of the Weyl group W_H ; since W_H acts simply transitively on the set of root bases of H , we see that x is a representative in $H^\theta(k)$ of w . As in the previous paragraph, the proof of [Tho15, Lemma 2.6] shows that $x^{-1}v$ is $G(k)$ -conjugate to an element of κ , hence that v is $G(k)$ -conjugate to an element of κ' . \square

Given a subset $M \subset \Phi_V$, we define the linear subspace

$$V(M) = \{v \in V \mid v_\alpha = 0 \text{ for all } \alpha \in M\} \subset V.$$

Proposition 2.15. *Let M be a subset of Φ_V , and suppose that one of the following three conditions is satisfied:*

1. *There exists $w \in \Omega$ such that $w(\Phi_V^+ - S_H) \subset M$.*
2. *There exist integers a_1, \dots, a_r not all equal to zero such that if $\alpha \in \Phi_V$ and $\sum_{i=1}^r a_i n_i(\alpha) > 0$, then $\alpha \in M$.*
3. *There exist $\beta \in S_G$, $\alpha \in \Phi_V - M$, and integers a_1, \dots, a_r not all equal to zero such that the following conditions hold:*
 - (a) *We have $\{\gamma \pm \beta \mid \gamma \in M\} \cap \Phi_V \subset M$.*
 - (b) *$\alpha - \beta \in \Phi_V - M$.*
 - (c) *If $\gamma \in \Phi_V$ and $\sum_{i=1}^r a_i n_i(\gamma) > 0$, then $\gamma \in M \cup \{\alpha\}$.*

Then every element of $V(M)(k)$ is k -reducible.

Proof. If either of the first two conditions is satisfied, then the desired reducibility follows from Lemma 2.14. We now show that if the third condition is satisfied, then every element of $V(M)(k)$ is k -reducible. Let $v \in V(M)(k)$. If $v_\alpha = 0$, then $v \in V(M \cup \{\alpha\})(k)$, and so v is k -reducible by the second part of the proposition. We can therefore assume that $v_\alpha \neq 0$.

Let $V_M = \{v \in V \mid v_\gamma = 0 \text{ for all } \gamma \in \Phi_V - M\}$. Then there is a T -invariant direct sum decomposition $V = V(M) \oplus V_M$. Fix a homomorphism $\text{SL}_2 \rightarrow G_\beta$ where G_β is the subgroup of G generated by the root groups corresponding to β and $-\beta$. Condition (a) implies that the decomposition $V = V(M) \oplus V_M$ is G_β -invariant. Since the ambient group H is simply laced, the β -root string through α has length two, and thus $\mathfrak{h}_\alpha \oplus \mathfrak{h}_{\alpha-\beta}$ is an irreducible G_β -submodule of V . The existence of an irreducible representation of degree two implies that $G_\beta \simeq \text{SL}_2$.

Since $\text{SL}_2(k)$ acts transitively on the non-zero vectors in the unique two-dimensional irreducible representation of SL_2 , we can find $g \in G_\beta(k) \subset G(k)$ such that $(gv)_\alpha = 0$. This shows that $gv \in V(M \cup \{\alpha\})$, hence that v is k -reducible, as required. \square

2.4 Roots and weights

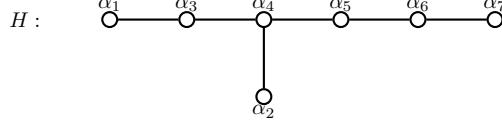
We conclude Section 2 by fixing coordinates in H and G . From now on we assume H has type E_7 or type E_8 . As above we let Φ_H^+ be the set of positive roots corresponding to our choice of root basis S_H . Similarly,

we define $\Phi_H^- \subset \Phi_H$ to be the subset of negative roots. We note that there exists a unique choice of root basis S_G of Φ_G such that the positive roots Φ_G^+ determined by S_G are given by $\Phi_G^+ = \Phi_G \cap \Phi_H^+$. Indeed, this follows from a consideration of Weyl chambers: the Weyl chambers for H (resp. G) are in bijection with the root bases of Φ_H (resp. Φ_G), and each Weyl chamber for H is contained in a unique Weyl chamber for G . If C_H is the fundamental Weyl chamber of H corresponding to S_H , and C_G is the unique Weyl chamber for G containing C_H , then defining S_G to be the root basis corresponding to C_G yields the desired property. We note that the set of negative roots Φ_G^- determined by S_G is given by $\Phi_G^- = \Phi_G \cap \Phi_H^-$.

We will later need to carry out explicit calculations, so we now define S_G in terms of the simple roots of S_H in each case **E**₇ and **E**₈. We number the simple roots of H and G as in Bourbaki [Bou68, Planches].

2.4.1 Case **E**₇

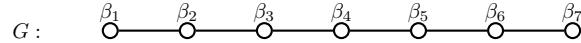
We have $S_H = \{\alpha_1, \dots, \alpha_7\}$, where the Dynkin diagram of H is as follows:



The root basis $S_G = \{\beta_1, \dots, \beta_7\}$ described above consists of the roots

$$\begin{aligned}\beta_1 &= \alpha_3 + \alpha_4 \\ \beta_2 &= \alpha_5 + \alpha_6 \\ \beta_3 &= \alpha_2 + \alpha_4 \\ \beta_4 &= \alpha_1 + \alpha_3 \\ \beta_5 &= \alpha_4 + \alpha_5 \\ \beta_6 &= \alpha_6 + \alpha_7 \\ \beta_7 &= \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5\end{aligned}$$

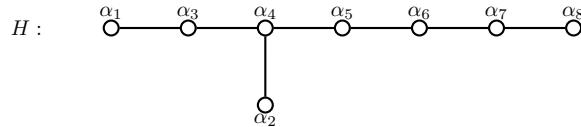
where the Dynkin diagram is as follows:



We note that the existence of a diagram automorphism for G implies that there are two possible choices of numbering of the roots in S_G consistent with the conventions of Bourbaki; we keep the above choice for the rest of this paper.

2.4.2 Case **E**₈

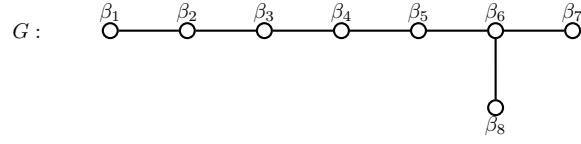
We have $S_H = \{\alpha_1, \dots, \alpha_8\}$, where the Dynkin diagram of H is as follows:



The root basis $S_G = \{\beta_1, \dots, \beta_8\}$ described above consists of the roots

$$\begin{aligned}\beta_1 &= \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 \\ \beta_2 &= \alpha_6 + \alpha_7 \\ \beta_3 &= \alpha_4 + \alpha_5 \\ \beta_4 &= \alpha_1 + \alpha_3 \\ \beta_5 &= \alpha_2 + \alpha_4 \\ \beta_6 &= \alpha_5 + \alpha_6 \\ \beta_7 &= \alpha_7 + \alpha_8 \\ \beta_8 &= \alpha_3 + \alpha_4\end{aligned}$$

where the Dynkin diagram is as follows:



Once again the existence of a diagram automorphism for G means that there are two possible choices of numbering of the roots in S_G consistent with Bourbaki; we keep the above choice for the rest of this paper.

3 Integral structures, measures, and orbits

In Section 2, we introduced the following data:

- the group H over k , together with split maximal torus $T \subset H$, root basis $S_H \subset X^*(T)$, involution $\theta = \text{Ad } \check{\rho}(-1)$, and Lie algebra $\mathfrak{h} = \text{Lie } H$;
- the group $G = (H^\theta)^\circ$ and its representation on $V = \mathfrak{h}^{d\theta=-1}$, together with a root basis $S_G \subset X^*(T)$ and Lie algebra $\mathfrak{g} = \text{Lie } G$;
- the categorical quotient $B = V//G$ and quotient map $\pi : V \rightarrow B$;
- the discriminant polynomial $\Delta \in k[B]$.

From now on, we also fix the regular nilpotent element $E = \sum_{\alpha \in S_H} e_\alpha \in V$. We now assume that $k = \mathbb{Q}$ and study integral structures on these objects.

3.1 Integral structures and measures

Our choice of Chevalley basis of \mathfrak{h} with root vectors $\{e_\alpha \mid \alpha \in \Phi_H\}$ determines a Chevalley basis of \mathfrak{g} , with root vectors $\{e_\alpha \mid \alpha \in \Phi_G\}$. It hence determines \mathbb{Z} -forms $\mathfrak{h}_\mathbb{Z} \subset \mathfrak{h}$ and $\mathfrak{g}_\mathbb{Z} \subset \mathfrak{g}$ (in the sense of [Bor70]). Moreover, $\mathcal{V} = V \cap \mathfrak{h}_\mathbb{Z}$ is an admissible \mathbb{Z} -lattice that contains E .

We extend G to a group scheme over \mathbb{Z} given by the Zariski closure of the group G in $\text{GL}(\mathcal{V})$. By abuse of notation, we also refer to this \mathbb{Z} -group scheme as G . Then the group $G(\mathbb{Z})$ acts on the lattice $\mathcal{V}(\mathbb{Z}) \subset V(\mathbb{Q})$.

The Cartan decomposition $V = \bigoplus_{\alpha \in \Phi_V} \mathfrak{h}_\alpha$ is defined over \mathbb{Z} , so extends to a decomposition $\mathcal{V} = \bigoplus_{\alpha \in \Phi_V} \mathcal{V}_\alpha$. Since there exists a subregular nilpotent element in $V = \mathcal{V}(\mathbb{Q})$, we may choose a subregular nilpotent element $e \in \mathcal{V}(\mathbb{Z})$. In Case **E₇**, we impose the additional condition that E corresponds to P_1 in the sense described in Theorem 2.9.

Fix a maximal compact subgroup $K \subset G(\mathbb{R})$. Let $P = TN \subset G$ be the Borel subgroup corresponding to the root basis S_G , and let $\bar{P} = T\bar{N} \subset G$ be the opposite Borel subgroup. Given $c \in \mathbb{R}$, we define $T_c = \{t \in T(\mathbb{R})^\circ \mid \beta(t) \leq c \text{ for all } \beta \in S_G\}$.

Proposition 3.1. *We can find a compact subset $\omega \subset \bar{N}(\mathbb{R})$ and a constant $c > 0$ such that $G(\mathbb{A}) = G(\mathbb{Q}) \cdot (G(\bar{\mathbb{Z}}) \times \mathfrak{S})$, where $\mathfrak{S} = \omega T_c K$.*

Proof. It suffices to show that $G(\mathbb{A}^\infty) = G(\mathbb{Q}) \cdot G(\bar{\mathbb{Z}})$ and that we can choose \mathfrak{S} so that $G(\mathbb{Z}) \cdot \mathfrak{S} = G(\mathbb{R})$. This is true: see [Bor66, §6], [PR94, Theorem 4.15], and [PR94, Theorem 8.11, Corollary 2]. \square

Henceforth we fix a choice of $\mathfrak{S} = \omega T_c K$ as in Proposition 3.1.

After rescaling the polynomials $c_i \in \mathbb{Q}[V]^G$ and $x, y \in \mathbb{Q}[X]$ appearing in Theorem 2.9 (resp. Theorem 2.10), we can assume that each polynomial c_i lies in $\mathbb{Z}[\mathcal{V}]^G$. We define $\mathcal{B} = \text{Spec } \mathbb{Z}[c_2, c_6, \dots, c_{18}]$ in Case **E₇** (resp. $\text{Spec } \mathbb{Z}[c_2, c_8, \dots, c_{30}]$ in Case **E₈**), and write $\pi : \mathcal{V} \rightarrow \mathcal{B}$ for the natural morphism, which recovers our existing map $\pi : V \rightarrow B$ after extension of scalars to \mathbb{Q} . If $b \in \mathcal{B}(\mathbb{R}) = B(\mathbb{R})$, then we define the height of b to be

$$\text{ht}(b) = \sup_i |c_i(b)|^{\deg \Delta / i}. \quad (3.1)$$

If $v \in V(\mathbb{R})$, then we define $\text{ht}(v) = \text{ht}(\pi(v))$. Since $\deg c_i = i$, the height function is homogeneous: for all $\lambda \in \mathbb{R}^\times$, we have $\text{ht}(\lambda v) = |\lambda|^{\deg \Delta} \text{ht}(v)$.

We define $\mathcal{X} = \text{Spec } \mathbb{Z}[x, y, c_2, c_6, \dots, c_{18}]$ in Case **E₇** (resp. $\text{Spec } \mathbb{Z}[x, y, c_2, c_8, \dots, c_{30}]$ in Case **E₈**). Thus \mathcal{X} is isomorphic to affine space $\mathbb{A}_{\mathbb{Z}}^{r+2}$, and the morphism $X \rightarrow B$ naturally extends to a morphism $\mathcal{X} \rightarrow \mathcal{B}$, still given in coordinates by the equation (1.2) in Case **E₇** (resp. (1.3) in Case **E₈**). For any ring R and any subset $A \subset \mathcal{V}(R)$, we write $A^{\text{reg,ss.}}$ for $\{a \in A \mid \Delta(a) \neq 0\}$. Similarly if $A' \subset \mathcal{B}(R)$ then we write $(A')^{\text{reg,ss.}}$ for the set $\{a \in A' \mid \Delta(a) \neq 0\}$.

Fix a left-invariant top form ω_G on G ; it is determined uniquely up to multiplication by $\mathbb{Z}^\times = \{\pm 1\}$. For any place v of \mathbb{Q} , we define a Haar integral on $G(\mathbb{Q}_v)$ using the volume element $dg = |\omega_G|_v$.

If $\mathbb{Q}_v = \mathbb{R}$, then we can use the Iwasawa decomposition on $G(\mathbb{R}) = T(\mathbb{R})^\circ \bar{N}(\mathbb{R})K = \bar{N}(\mathbb{R})T(\mathbb{R})^\circ K$ to decompose $dg = dt \, dn \, dk$ on $G(\mathbb{R})$ as follows (cf. [Tho15, Section 2.7]). We give $T(\mathbb{R})^\circ$ the measure pulled back from the isomorphism $\prod_{\alpha \in S_G} \alpha : T(\mathbb{R})^\circ \simeq \mathbb{R}_{>0}^r$. We give K its normalized (probability) Haar measure. We then choose the unique Haar measure dn on $\bar{N}(\mathbb{R})$ such that $dg = dt \, dn \, dk$. For $t \in T(\mathbb{R})$, we define $\delta_G(t) = \prod_{\alpha \in \Phi_G^-} \alpha(t)$. Then for any continuous compactly supported function $f : G(\mathbb{R}) \rightarrow \mathbb{C}$, we have the equalities

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

We also define measures on V and B as in [Tho15, Section 2.8] by fixing an invariant differential top form ω_V on \mathcal{V} and by defining $\omega_B = dc_2 \wedge dc_6 \wedge \dots \wedge dc_{18}$ in Case **E₇** (resp. $\omega_B = dc_2 \wedge dc_8 \wedge \dots \wedge dc_{30}$ in Case **E₈**). If v is a place of \mathbb{Q} , then the formulae $db = |\omega_B|_v$ and $dv = |\omega_V|_v$ define measures on $B(\mathbb{Q}_v)$ and $V(\mathbb{Q}_v)$ respectively. Fixing these choices, we have the following useful result.

Lemma 3.2. *There exists a rational number $W_0 \in \mathbb{Q}^\times$ with the following property: let k'/\mathbb{Q} be any field extension, and let $\mathfrak{c} \subset V(k')$ be a Cartan subspace. Let $\mu_{\mathfrak{c}} : G_{k'} \times \mathfrak{c} \rightarrow V_{k'}$ be the natural 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 [Tho15, Proposition 2.13]. \square

Proposition 3.3. *Let p be a prime.*

1. *Let $\phi : \mathcal{V}(\mathbb{Z}_p)^{\text{reg.ss.}} \rightarrow \mathbb{R}$ be a function of compact support that is locally constant (resp. continuous) and invariant under the action of $G(\mathbb{Z}_p)$. Then the function $F_\phi : B(\mathbb{Q}_p)^{\text{reg.ss.}} \rightarrow \mathbb{R}$ defined by the formula*

$$F_\phi(b) = \sum_{v \in G(\mathbb{Z}_p) \setminus \mathcal{V}_b(\mathbb{Z}_p)} \frac{\phi(v)}{\# \text{Stab}_{G(\mathbb{Z}_p)}(v)}$$

is of compact support and locally constant (resp. continuous), and we have the formula

$$\int_{v \in \mathcal{V}(\mathbb{Z}_p)} \phi(v) dv = |W_0|_p \text{vol}(G(\mathbb{Z}_p)) \int_{b \in \mathcal{B}(\mathbb{Z}_p)} F_\phi(b) db.$$

2. *Define a function $m_p : \mathcal{V}(\mathbb{Z}_p)^{\text{reg.ss.}} \rightarrow \mathbb{R}$ by the formula*

$$m_p(v) = \sum_{v' \in G(\mathbb{Z}_p) \setminus (G(\mathbb{Q}_p) \cdot v \cap \mathcal{V}(\mathbb{Z}_p))} \frac{\# \text{Stab}_{G(\mathbb{Q}_p)}(v)}{\# \text{Stab}_{G(\mathbb{Z}_p)}(v')}.$$

Then m_p is locally constant.

3. *Let $\psi : \mathcal{V}(\mathbb{Z}_p)^{\text{reg.ss.}} \rightarrow \mathbb{R}$ be a continuous function of compact support that is $G(\mathbb{Q}_p)$ -invariant, in the sense that if $v, v' \in \mathcal{V}(\mathbb{Z}_p)$, $g \in G(\mathbb{Q}_p)$, and $gv = v'$, then $\psi(v) = \psi(v')$. Then we have the formula*

$$\int_{v \in \mathcal{V}(\mathbb{Z}_p)} \psi(v) dv = |W_0|_p \text{vol}(G(\mathbb{Z}_p)) \int_{b \in \mathcal{B}(\mathbb{Z}_p)} \sum_{v \in G(\mathbb{Q}_p) \setminus \mathcal{V}_b(\mathbb{Z}_p)} \frac{m_p(v)\psi(v)}{\# \text{Stab}_{G(\mathbb{Q}_p)}(v)} db.$$

Proof. The first part follows from Lemma 3.2 and the p -adic formula for integration in fibres; see [Igu00, §7.6]. To prove the second part, we note that the function $v \mapsto \# \text{Stab}_{G(\mathbb{Q}_p)}(v)$ is locally constant, because the universal stabilizer $Z \rightarrow V^{\text{reg.ss.}}$ is finite étale. It therefore suffices to show that the function

$$n_p(v) := \sum_{v' \in G(\mathbb{Z}_p) \setminus (G(\mathbb{Q}_p) \cdot v \cap \mathcal{V}(\mathbb{Z}_p))} \frac{1}{\# \text{Stab}_{G(\mathbb{Z}_p)}(v')}$$

is locally constant. Suppose $v \in V(\mathbb{Q}_p)^{\text{reg.ss.}}$. Let $\mathfrak{c} \subset V(\mathbb{Q}_p)$ be the unique Cartan subspace containing v . Since $\pi|_{\mathfrak{c}}$ is étale above $B(\mathbb{Q}_p)^{\text{reg.ss.}}$, we can find an open compact neighbourhood B_v of $\pi(v)$ in $B(\mathbb{Q}_p)^{\text{reg.ss.}}$ such that $\pi^{-1}(B_v) \cap \mathfrak{c} = \sqcup_{i=1}^s U_i$ is a disjoint union of open subsets of \mathfrak{c} and each $\pi|_{U_i} : U_i \rightarrow B_v$ is a homeomorphism. Let $U = U_j$ be the open subset containing v . Let $\mu : G(\mathbb{Q}_p) \times U \rightarrow V(\mathbb{Q}_p) \cap \pi^{-1}(B_v)$ be the restriction of the natural action map. Then μ is proper, and so $\mu^{-1}(\mathcal{V}(\mathbb{Z}_p) \cap \pi^{-1}(B_v))$ is compact. It follows that the characteristic function χ of the set $\mu(\mu^{-1}(\mathcal{V}(\mathbb{Z}_p) \cap \pi^{-1}(B_v))) \subset \mathcal{V}(\mathbb{Z}_p)^{\text{reg.ss.}}$ is locally constant and of compact support. For $v' \in U$, we have $n_p(v') = F_\chi(\pi(v'))$, where F_χ is as defined in the statement of the first part of the proposition. Thus by the first part of the proposition n_p is locally constant. The third part of the proposition follows from the first two. \square

3.2 Selmer elements and integral orbits

We now discuss the construction of elements of $\mathcal{V}(\mathbb{Z}_p)$ and $\mathcal{V}(\mathbb{Z})$ from rational points of algebraic curves. We first show that certain geometric orbits have integral representatives.

Lemma 3.4. *There exists an integer $N_0 \geq 1$ with the following properties:*

1. For any prime p and any $b \in \mathcal{B}(\mathbb{Z}_p)$, we have $N_0 \cdot \kappa_b \in \mathcal{V}(\mathbb{Z}_p)$.
2. In Case **E₇**, let $w \in \Omega$ be the non-trivial element and let κ' denote the Kostant section corresponding to the regular nilpotent element $E' = \sum_{\alpha \in S_H} e_{w\alpha}$. Then for any prime p and for any $b \in \mathcal{B}(\mathbb{Z}_p)$, we have $N_0 \cdot \kappa'_b \in \mathcal{V}(\mathbb{Z}_p)$.
3. For any prime p and any $x \in \mathcal{X}(\mathbb{Z}_p)$, we have $N_0 \cdot x \in \mathcal{V}(\mathbb{Z}_p)$.
4. If $b \in N_0^2 \cdot \mathcal{B}(\mathbb{Z})$, then $b \in \pi(\mathcal{V}(\mathbb{Z}))$.

In the first three items N_0 is acting via the \mathbb{G}_m -action discussed in Section 2.2. In the third item N_0 is acting via the natural \mathbb{G}_m -action on B .

Proof. This follows from the existence of the contracting \mathbb{G}_m -actions on κ , κ' , and \mathcal{X} , cf. [Tho15, Lemma 2.8]. \square

Lemma 3.5. *There exists an integer $N_1 \geq 1$ with the following property: for any prime p and any $b \in N_1 \cdot \mathcal{B}(\mathbb{Z}_p)$ such that $\Delta(b) \neq 0$, the canonical image of $Y_b(\mathbb{Q}_p)$ in $H^1(\mathbb{Q}_p, J_b[2])$ is contained in the image of the composite map:*

$$\mathcal{V}_b(\mathbb{Z}_p) \rightarrow G(\mathbb{Q}_p) \setminus V_b(\mathbb{Q}_p) \xrightarrow{\gamma_b} H^1(\mathbb{Q}_p, J_b[2])$$

(where γ_b is as in Theorems 2.9 and 2.10 for the case when $k = \mathbb{Q}_p$).

Proof. We just treat the case when H is of type E_7 ; the E_8 case is more straightforward, since there is only one point at infinity. We will show that we can take $N_1 = 2^4 N_0^2$, where N_0 is as in Lemma 3.4. We recall that the curve Y_b is given by the equation

$$y_0^3 z_0 = x_0^3 y_0 + c_{10} x_0^2 z_0^2 + x_0 (c_2 y_0^2 z_0 + c_8 y_0 z_0^2 + c_{14} z_0^3) + c_6 y_0^2 z_0^2 + c_{12} y_0 z_0^3 + c_{18} z_0^4,$$

and has two sections $P_1 = [0 : 1 : 0]$ and $P_2 = [1 : 0 : 0]$ at infinity; the map $Y_b(\mathbb{Q}_p) \rightarrow J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)$ sends a point P to the class of the divisor $(P) - (P_1)$. We define \mathcal{Y} to be the closed subscheme of $\mathbb{P}_{\mathcal{B}}^2$ defined by the same equation; then the complement in \mathcal{Y} of its sections at infinity is naturally identified with \mathcal{X} by Theorem 2.9. For $b \in \mathcal{B}(\mathbb{Q}_p)$, \mathcal{Y}_b is smooth in an open neighbourhood of these sections at infinity. If $t \in \mathbb{Q}_p^{\times}$, then the isomorphism $X_b \rightarrow X_{t^2 b}$ induced by the action of \mathbb{G}_m on X extends to an isomorphism $Y_b \rightarrow Y_{t^2 b}$ that maps $[x_0 : y_0 : z_0]$ to $[t^8 x_0 : t^{12} y_0 : z_0]$.

We first claim that if $b \in 2^4 \mathcal{B}(\mathbb{Z}_p)$, then every divisor class in the image of the map $Y_b(\mathbb{Q}_p) \rightarrow J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)$ is represented by either the zero divisor, the divisor $P_2 - P_1$, or a divisor of the form $P - P_1$ for some $P \in \mathcal{X}_b(\mathbb{Z}_p)$.

If $P \in Y_b(\mathbb{Q}_p)$, then we write \bar{P} for the image of P in $\mathcal{Y}_b(\mathbb{F}_p)$. The special fibre $\mathcal{Y}_{b, \mathbb{F}_p}$ is reduced, and has at most two irreducible components, which are geometrically irreducible. Moreover, if there are two irreducible components, then \bar{P}_1 and \bar{P}_2 lie on distinct irreducible components. Indeed, due to the presence of the contracting \mathbb{G}_m -action, any property of the morphism $\mathcal{Y} \rightarrow \mathcal{B}$ which is open on the base can be checked in the central fibre. Thus [Sta17, Tag 0C0E] implies that all of the fibres of \mathcal{Y} are geometrically reduced; and then [Sta17, Tag 055R] implies that the two sections P_1, P_2 together meet all irreducible components in every geometric fibre. In particular, every irreducible component of $\mathcal{Y}_{b, \mathbb{F}_p}$ is geometrically irreducible.

Let $\mathcal{J}_b = \text{Pic}_{\mathcal{Y}_b/\mathbb{Z}_p}^0$ be the open subscheme of $\text{Pic}_{\mathcal{Y}_b/\mathbb{Z}_p}$ corresponding to those invertible sheaves that are fibrewise of degree 0 on each irreducible component (see [BLR90, §8.4]). Then \mathcal{J}_b is a smooth and separated scheme over \mathbb{Z}_p (see [BLR90, §9.4, Theorem 2]). We note that if $Q \in \mathcal{J}_b(\mathbb{Z}_p)$ has trivial image in $\mathcal{J}_b(\mathbb{Z}_p/2^3 p \mathbb{Z}_p)$, then Q is divisible by 2 in $\mathcal{J}_b(\mathbb{Z}_p)$ (this follows from [Sil09, Theorem 6.1] and its generalization [CX08, Proposition 3.1]).

Let $P = (x, y) \in Y_b(\mathbb{Q}_p)$. To prove the claim, it suffices to show that if $P \notin \mathcal{X}_b(\mathbb{Z}_p)$, then one of the divisor classes $[(P) - (P_1)]$ or $[(P) - (P_2)]$ is divisible by 2 in $J_b(\mathbb{Q}_p)$. We can assume that $xy \neq 0$. We note that if $P \notin \mathcal{X}_b(\mathbb{Z}_p)$, then (at least) one of x, y must be non-integral. If x is integral then the defining equation of Y_b shows that y is integral too. We can therefore write $x = p^m u$, $y = p^n v$, with $u, v \in \mathbb{Z}_p^\times$ and $m < 0$. We note that if $n < 0$, then we must have $2n = 3m$, hence we can write $n = 3k$, $m = 2k$ for some $k < 0$.

We first treat the case where p is odd. If $n < 0$, then we have

$$P = [p^{2k}u : p^{3k}v : 1] = [p^{-k}u : v : p^{-3k}] \equiv P_1 \pmod{p},$$

and we see that $[(P) - (P_1)]$ is divisible by 2 in $J_b(\mathbb{Q}_p)$. If $n \geq 0$, then $P \equiv P_2 \pmod{p}$, and $[(P) - (P_2)]$ is divisible by 2 in $J_b(\mathbb{Q}_p)$. This establishes the claim in the case when p is odd.

Now suppose that $p = 2$. Our assumption $b \in 2^4 \mathcal{B}(\mathbb{Z}_2)$ means that $c_i(b)$ is divisible by 2^{4i} for each $i \in \{2, \dots, 18\}$. We write $\iota : Y_b \rightarrow Y_{\frac{1}{4}b}$ for the map $[x_0 : y_0 : z_0] \mapsto [2^{-8}x_0 : 2^{-12}y_0 : z_0] = [2^4x_0 : y_0 : 2^{12}z_0]$. If $n < 0$, then we get

$$\iota(P) = [2^{4-k}u : v : 2^{12-3k}] \equiv P_1 \pmod{2^4}.$$

This shows that $[(\iota(P)) - (P_1)]$ is divisible by 2 in $J_{\frac{1}{4}b}(\mathbb{Q}_2)$, hence $[(P) - (P_1)]$ is divisible by 2 in $J_b(\mathbb{Q}_2)$. If $n \geq 0$, then we have $P = [1 : 2^{n-m}v/u : 2^{-m}/u] = [1 : w : z]$, say, and we have an equation

$$w(1 - w^2z) = O(2^8z)$$

in \mathbb{Z}_2 . It follows that $n - m > 8$. Then we get

$$\iota(P) = [2^4 : 2^{n-m}v/u : 2^{12-m}/u] = [1 : 2^{n-m-4}v/u : 2^{8-m}/u] \equiv P_2 \pmod{2^4},$$

hence $[(P) - (P_2)]$ is divisible by 2 in $J_b(\mathbb{Q}_2)$. This completes the proof of the claim.

We now show how the claim implies the lemma. We drop our assumption on the parity of p , and take $b = N_0^2 c$, where $c \in 2^4 \mathcal{B}(\mathbb{Z}_p)$. Given a class ϕ in $H^1(\mathbb{Q}_p, J_c[2])$, if ϕ is in the image of $Y_c(\mathbb{Q}_p)$, then ϕ is represented by either P_1 , P_2 , or an element of $\mathcal{X}_c(\mathbb{Z}_p)$. Let ϕ' denote the corresponding class in $H^1(\mathbb{Q}_p, J_b[2])$. If P_1 is a representative, then $\kappa_b \in V_b(\mathbb{Q}_p)$ represents the corresponding rational orbit. By Lemma 3.4, we have $\kappa_b = N_0 \cdot \kappa_c \in \mathcal{V}(\mathbb{Z}_p)$, so κ_b is even an integral representative for this rational orbit. If P_2 is a representative, then $\kappa'_b \in \mathcal{V}(\mathbb{Z}_p)$ is an integral representative, by the same argument.

Suppose instead that ϕ is represented by a divisor $(P) - (P_1)$, where $P \in \mathcal{X}_c(\mathbb{Z}_p)$. Then ϕ' is represented by the divisor $(N_0 \cdot P) - (P_1)$, where now $N_0 \cdot P \in N_0 \cdot \mathcal{X}(\mathbb{Z}_p)$. By Lemma 3.4, we have $N_0 \cdot \mathcal{X}(\mathbb{Z}_p) \subset \mathcal{V}(\mathbb{Z}_p)$, showing that $N_0 \cdot P \in V_b(\mathbb{Z}_p)$ is an integral representative for the rational orbit corresponding to the class ϕ . This completes the proof. \square

Proposition 3.6. *Let $N_1 \in \mathbb{Z}_{\geq 1}$ be as in Lemma 3.5. Then for any $b \in N_1 \cdot \mathcal{B}(\mathbb{Z})$ such that $\Delta(b) \neq 0$, the 2-Selmer set $\text{Sel}_2(Y_b) \subset H^1(\mathbb{Q}_p, J_b[2])$ is contained in the image of the composite map*

$$\mathcal{V}_b(\mathbb{Z}) \rightarrow G(\mathbb{Q}) \setminus V_b(\mathbb{Q}) \xrightarrow{\gamma_b} H^1(\mathbb{Q}, J_b[2]).$$

Consequently, for any $b \in \mathcal{B}(\mathbb{Z})$ such that $\Delta(b) \neq 0$, we have $\#\text{Sel}_2(Y_b) \leq \#G(\mathbb{Q}) \setminus \mathcal{V}_{N_1 \cdot b}(\mathbb{Z})$.

Proof. Suppose $c \in \text{Sel}_2(Y_b)$. We first show that $c \in \gamma_b(G(\mathbb{Q}) \setminus V(\mathbb{Q}))$; by Proposition 2.6 this is the case exactly when the image c' of c under the map

$$H^1(\mathbb{Q}, J_b[2]) \rightarrow H^1(\mathbb{Q}, G)$$

is trivial. By commutativity of the diagram in Theorem 2.9 in Case **E₇** (resp. Theorem 2.10 in Case **E₈**) and the definition of the 2-Selmer set, we see that c' is locally trivial, in the sense that its image in $H^1(\mathbb{Q}_v, G)$

is trivial for every place v of \mathbb{Q} . We claim that this implies that c' is itself trivial. Indeed, write G^{sc} for the simply connected cover of G . The centre of G has order 2 in both cases (see, e.g., [Tho16, Proof of Proposition A.1]). Thus we see that there is a short exact sequence of groups over \mathbb{Q} :

$$1 \longrightarrow \mu \longrightarrow G^{\text{sc}} \longrightarrow G \longrightarrow 1,$$

where $\mu = \mu_4$ (in Case **E**₇) or μ_2 (in Case **E**₈). This leads to the following commutative diagram of pointed Galois cohomology sets, in which the rows are exact:

$$\begin{array}{ccccccc} H^1(\mathbb{Q}, \mu) & \longrightarrow & H^1(\mathbb{Q}, G^{\text{sc}}) & \longrightarrow & H^1(\mathbb{Q}, G) & \longrightarrow & H^2(\mathbb{Q}, \mu) \\ \downarrow \text{loc}_1 & & \downarrow \text{loc}_2 & & \downarrow \text{loc}_3 & & \downarrow \text{loc}_4 \\ \prod_v H^1(\mathbb{Q}_v, \mu) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, G^{\text{sc}}) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, G) & \longrightarrow & \prod_v H^2(\mathbb{Q}_v, \mu). \end{array}$$

Since G^{sc} is simply connected, the map loc_2 is bijective, and $H^1(\mathbb{Q}_p, G^{\text{sc}})$ is trivial for every prime p . By class field theory, the map loc_4 is injective. Using these facts, a diagram chase shows that the triviality of $\text{loc}_3(c')$ forces c' itself to be trivial.

We can therefore choose a vector $v \in V_b(\mathbb{Q})$ representing our class c . By Lemma 3.5, for each prime p there exists an element $g_p \in G(\mathbb{Q}_p)$ such that $g_p \cdot v \in V_b(\mathbb{Z}_p)$. By Proposition 3.1, there is an element $g \in G(\mathbb{Q})$ such that $g_p \in G(\mathbb{Z}_p)g$ for every prime p . It follows that $g \cdot v \in V_b(\mathbb{Z})$, as required. \square

3.3 Subsets of $V(\mathbb{R})$ and $V(\mathbb{Q}_p)$

We conclude this section by constructing some useful subsets of $V(\mathbb{R})$ and $V(\mathbb{Q}_p)$. We first consider $V(\mathbb{R})$. Let $\mathfrak{c}_1, \dots, \mathfrak{c}_n$ denote representatives of the distinct $G(\mathbb{R})$ -conjugacy classes of Cartan subspaces of $V(\mathbb{R})$. For each $i \in \{1, \dots, n\}$, let \mathfrak{c}'_i denote the closed subset of $\mathfrak{c}_i^{\text{reg.ss.}}$ given by $\mathfrak{c}'_i = \{v \in \mathfrak{c}_i^{\text{reg.ss.}} \mid \text{ht}(v) = 1\}$. Arguing as in [Tho15, §2.9], we can find a cover of \mathfrak{c}'_i by finitely many connected semialgebraic open subsets U_{ij} such that each map $\pi|_{U_{ij}} : U_{ij} \rightarrow \{b \in B(\mathbb{R})^{\text{reg.ss.}} \mid \text{ht}(b) = 1\}$ is a homeomorphism onto its image. We write L_1, \dots, L_m for the sets $\pi(U_{ij})$ for all i, j in any order, and for $L_k = \pi(U_{i,j})$ we set $s_k := (\pi|_{U_{i,j}})^{-1} : L_k \rightarrow V(\mathbb{R})^{\text{reg.ss.}}$. We can extend s_k to a map $s_k : \Lambda \cdot L_k \rightarrow V(\mathbb{R})^{\text{reg.ss.}}$ by the formula $s_k(\lambda b) = \lambda s_k(b)$ for any $\lambda \in \Lambda$, $b \in L_k$.

Lemma 3.7. *With notation as above, each map $s_k : \Lambda \cdot L_k \rightarrow V(\mathbb{R})^{\text{reg.ss.}}$ is a semialgebraic map, and $s_k(L_k)$ has compact closure in $V(\mathbb{R})$. The quantity $r_k := \#\text{Stab}_{G(\mathbb{R})}(s_k(b))$ is independent of the choice of $b \in L_k$. We have $\cup_{k=1}^m G(\mathbb{R}) \cdot \Lambda \cdot s_k(L_k) = V(\mathbb{R})^{\text{reg.ss.}}$. For any continuous function $f : V(\mathbb{R})^{\text{reg.ss.}} \rightarrow \mathbb{R}$ of compact support, we have*

$$\int_{v \in G(\mathbb{R}) \cdot \Lambda \cdot L_k} f(v) dv = \frac{|W_0|_\infty}{r_k} \int_{b \in \Lambda \cdot L_k} \int_{g \in G(\mathbb{R})} f(g \cdot s_k(b)) dg db.$$

Consequently for any $x \geq 1$ we have:

$$\text{vol}(\mathfrak{S} \cdot [1, x^{1/\deg \Delta}] \cdot s_k(L_k)) \leq |W_0|_\infty \text{vol}(\mathfrak{S}) \text{vol}([1, x^{1/\deg \Delta}] \cdot L_k).$$

Proof. Let $\mu_k : G(\mathbb{R}) \times (\Lambda \cdot L_k) \rightarrow V(\mathbb{R})^{\text{reg.ss.}}$ be given by $(g, b) \mapsto g \cdot s_k(b)$. Then μ_k is a local diffeomorphism onto its image, with fibres of cardinality r_k . By Lemma 3.2 we have $\mu_k^* \omega_V = W_0 \omega_G \wedge \omega_B$. The displayed formulae follow from this identity. \square

We now consider $V(\mathbb{Q}_p)$.

Lemma 3.8. *There exists a constant $\varepsilon \in (0, 1)$ with the following property: let p be a prime congruent to 1 mod 6. Then there exists a non-empty open compact subset $U_p \subset \mathcal{B}(\mathbb{Z}_p)$ such that for all $b \in U_p$, we have $\Delta(b) \neq 0$, $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$, and*

$$\frac{\#\text{im}(Y_b(\mathbb{Q}_p) \rightarrow J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)))}{\#J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)} \leq \varepsilon.$$

Proof. Let p be a prime with $p \equiv 1 \pmod{6}$. It suffices to show that we can find a single $b \in \mathcal{B}(\mathbb{Z}_p)$ with $\Delta(b) \neq 0$, $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$, and

$$\frac{\#\text{im}(Y_b(\mathbb{Q}_p) \rightarrow J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p))}{\#J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)} < 1.$$

By continuity considerations of the type in [PS14, §8], we can then take U_p to be any sufficiently small open compact neighbourhood of b in $\mathcal{B}(\mathbb{Z}_p)$. We will in fact exhibit $b \in U_p$ such that $\Delta(b) \neq 0$, $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$, the component group Φ of the Néron model of J_b is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$, and the image of $Y_b(\mathbb{Q}_p)$ in Φ is the identity. This will imply that the lemma holds with $\varepsilon = \frac{1}{4}$.

We first return to the E_6 family of curves (1.1):

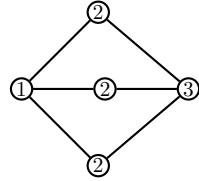
$$y^3 = x^4 + y(c_2x^2 + c_5x + c_8) + c_6x^2 + c_9x + c_{12}$$

described in the introduction to this paper. In this case the existence of such a point b is asserted in [Tho15, Proposition 2.15]. The proof given there is incorrect; more precisely, the description of the special fibre of a regular model of the curve $y^3 = x^4 - p^2$ is incorrect. We will first remedy this error. The calculation in this case will also play a role in the proof of the lemma in Cases **E₇** and **E₈**.

We consider instead the curve given by the equation $y^3 = (x - 1)(x^3 - p^2)$. (This curve can be put into the canonical form (1.1) by a linear change of variable in x .) Let \mathcal{Y} be the curve inside $\mathbb{P}_{\mathbb{Z}_p}^2$ given by the projective closure of this equation, and let $\mathcal{Z} \subset \mathbb{A}_{\mathbb{Z}_p}^2$ denote the complement of the unique point at infinity. It is clear that $\mathcal{Z}(\mathbb{Z}_p) \neq \emptyset$. Moreover, \mathcal{Y} has a unique point that is not regular, namely the point corresponding to $(x, y) = (0, 0)$ in the special fibre $\mathcal{Z}_{\mathbb{F}_p}$.

This singularity can be resolved by blowing up. Let $\mathcal{Y}' \rightarrow \mathcal{Y}$ denote the blow-up at the unique non-regular point of \mathcal{Y} . Then \mathcal{Y}' has exactly 3 non-regular points. The special fibre of \mathcal{Y}' has two irreducible components, namely the strict transform of $\mathcal{Y}_{\mathbb{F}_p}$, and a smooth exceptional divisor. Let $\mathcal{Y}'' \rightarrow \mathcal{Y}'$ denote the blow-up of the 3 non-regular points. Then \mathcal{Y}'' is regular, and the special fibre $\mathcal{Y}_{\mathbb{F}_p}''$ has 5 irreducible components: the strict transform C_1 of $\mathcal{Y}_{\mathbb{F}_p}$, the strict transform C_5 of the exceptional divisor in $\mathcal{Y}_{\mathbb{F}_p}'$, and the smooth exceptional divisors C_2, C_3, C_4 of the blow-up $\mathcal{Y}'' \rightarrow \mathcal{Y}$.

We note that blow-up commutes with flat base change, so to verify our claims about the component group Φ it suffices to perform these blow-ups in the completed local ring of \mathcal{Y} at the maximal ideal (p, x, y) , which is in turn isomorphic to $\mathbb{Z}_p[[x, y]]/(y^3 - x^4 + p^2)$. Here we find that all the irreducible components in the special fibre of $\mathcal{Y}_{\mathbb{F}_p}''$ are smooth and geometrically irreducible, and their intersection graph is given as follows:



All intersections are transverse, and the multiplicities of C_1, C_2, C_3, C_4 and C_5 are respectively 1, 2, 2, 2, and 3. The intersection matrix of the special fibre of \mathcal{Y}'' is therefore

$$M = \begin{pmatrix} -6 & 1 & 1 & 1 & 0 \\ 1 & -2 & 0 & 0 & 1 \\ 1 & 0 & -2 & 0 & 1 \\ 1 & 0 & 0 & -2 & 1 \\ 0 & 1 & 1 & 1 & -2 \end{pmatrix}.$$

Let $v = (1, 2, 2, 2, 3)$. Then $Mv = 0$ and there is an isomorphism $\Phi \cong v^\perp / \text{im } M$, where we consider v as an element of \mathbb{Z}^5 and M as a \mathbb{Z} -module homomorphism (see [BLR90, §9.6]). A calculation shows that $\Phi \cong (\mathbb{Z}/2\mathbb{Z})^2$, as claimed. Each point of $\mathcal{Y}(\mathbb{Z}_p) = \mathcal{Y}''(\mathbb{Z}_p)$ reduces modulo p to a smooth point of the special fibre $\mathcal{Y}_{\mathbb{F}_p}''$. Since there is exactly one component of $\mathcal{Y}_{\mathbb{F}_p}''$ of multiplicity one, we see that all points of $\mathcal{Y}(\mathbb{Z}_p)$ reduce to this component; consequently, their image in the Néron component group Φ is trivial (to see this, use the recipe in [Lor00, §5]).

We now turn to Case **E₇**. Consider a perturbation

$$y^3 = (x-1)(x^3-p^2) + \lambda x^3 y,$$

where $\lambda \in \mathbb{Z}_p - \{0\}$. Using the procedure of Proposition 5.1, we can make a change of variable to put this curve in the form (1.2): the perturbation causes the point $[0 : 1 : 0]$ at infinity to be a flex point, but no longer a hyperflex point. One may check that the curve obtained in this way has nontrivial integral points. For λ close enough to 0, this curve will also satisfy the condition

$$\frac{\#\text{im}(Y_b(\mathbb{Q}_p) \rightarrow J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p))}{\#J_b(\mathbb{Q}_p)/2J_b(\mathbb{Q}_p)} \leq \frac{1}{4}.$$

Finally, we turn to Case **E₈**. We now let \mathcal{Z} be the curve given by the equation $y^3 = (x^2-1)(x^3-p^2)$, and let \mathcal{Y} denote the projective curve over \mathbb{Z}_p containing \mathcal{Z} and given by the multihomogeneous equation $y^3 = z(x^2-z^2)(x^3-p^2z^3)$. Then \mathcal{Y} is smooth along the unique section at infinity. We see that \mathcal{Y} has a unique non-regular point, namely the point inside \mathcal{Z} corresponding to the maximal ideal (p, x, y) . The completed local ring of \mathcal{Z} at this point is isomorphic to $\mathbb{Z}_p[[x, w]]/(w^3 - x^3 + p^2)$. It follows that the singularities of \mathcal{Y} can be resolved by two blow-ups, exactly as in the E_6 case described above. Moreover, the intersection matrix is equal to M as defined above, and the isomorphism class of the component group of the Néron model of the Jacobian of $\mathcal{Y}_{\mathbb{Q}_p}$ is also $(\mathbb{Z}/2\mathbb{Z})^2$. This concludes the proof. \square

Lemma 3.9. *There exists an open subset $U_2 \subset \mathcal{B}(\mathbb{Z}_2)$ such that for all $b \in U_2$, we have $\Delta(b) \neq 0$, $\mathcal{X}_b(\mathbb{Z}_2) \neq \emptyset$, and the image of the map $\mathcal{X}_b(\mathbb{Z}_2) \rightarrow J_b(\mathbb{Q}_2)/2J_b(\mathbb{Q}_2)$ does not intersect the subgroup generated by the divisor class $[(P_1) - (P_2)]$ in Case **E₇** (resp. does not contain the identity in Case **E₈**).*

Proof. If $c \in \mathcal{B}(\mathbb{F}_2)$ is such that \mathcal{X}_c is smooth, let us write \mathcal{Y}_c for the smooth projective completion of \mathcal{X}_c and \mathcal{J}_c for $\text{Pic}^0_{\mathcal{Y}_c}$. In order to prove the lemma, it suffices to exhibit a single point $c \in \mathcal{B}(\mathbb{F}_2)$ such that \mathcal{X}_c is smooth, and such that the image of the map $\mathcal{X}_c(\mathbb{F}_2) \rightarrow \mathcal{J}_c(\mathbb{F}_2)/2\mathcal{J}_c(\mathbb{F}_2)$ is nontrivial and does not intersect the given subgroup. Indeed, suppose c is such a point, and define U_2 to be the preimage of c under the natural map $\mathcal{B}(\mathbb{Z}_2) \rightarrow \mathcal{B}(\mathbb{F}_2)$. If $b \in U_2$, then there is a commutative diagram

$$\begin{array}{ccc} \mathcal{X}_b(\mathbb{Z}_2) & \longrightarrow & J_b(\mathbb{Q}_2)/2J_b(\mathbb{Q}_2) \\ \downarrow & & \downarrow \\ \mathcal{X}_c(\mathbb{F}_2) & \longrightarrow & \mathcal{J}_c(\mathbb{F}_2)/2\mathcal{J}_c(\mathbb{F}_2). \end{array}$$

By Hensel's Lemma, the existence of a point in $\mathcal{X}_c(\mathbb{F}_2)$ implies that $\mathcal{X}_b(\mathbb{Z}_2)$ is non-empty. Since the diagram is commutative, the image of $\mathcal{X}_b(\mathbb{Z}_2)$ does not intersect the subgroup generated by the divisor class $[(P_1) - (P_2)]$ in Case **E₇** (resp. does not contain the identity in Case **E₈**).

It remains to exhibit such a point $c \in \mathcal{B}(\mathbb{F}_2)$ in each case. In Case **E₇**, we consider the curve

$$\mathcal{X}_c : y^3 = x^3 y + y + 1.$$

We have that \mathcal{X}_c is smooth over \mathbb{F}_2 , and $\mathcal{X}_c(\mathbb{F}_2)$ consists of exactly one point $(x, y) = (1, 1)$. There is an isomorphism $\mathcal{J}_c(\mathbb{F}_2) \cong \mathbb{Z}/18\mathbb{Z}$, hence an isomorphism $\mathcal{J}_c(\mathbb{F}_2)/2\mathcal{J}_c(\mathbb{F}_2) \cong \mathbb{Z}/2\mathbb{Z}$. The subgroup of

$\mathcal{J}_c(\mathbb{F}_2)/2\mathcal{J}_c(\mathbb{F}_2)$ generated by the divisor class $[(P_1) - (P_2)]$ is the trivial subgroup, while the point $(1, 1)$ has nontrivial image in $\mathcal{J}_c(\mathbb{F}_2)/2\mathcal{J}_c(\mathbb{F}_2)$ (in fact, its image in $\mathcal{J}_c(\mathbb{F}_2)$ is a generator).

In Case **E₈**, we consider the curve

$$\mathcal{X}_c : y^3 = x^5 + y(x^3 + x^2) + x^3 + 1.$$

We have that \mathcal{X}_c is smooth over \mathbb{F}_2 , and $\mathcal{X}_c(\mathbb{F}_2)$ consists of the two points $(x, y) = (0, 1)$ and $(x, y) = (1, 1)$. There is an isomorphism $\mathcal{J}_c(\mathbb{F}_2) \cong \mathbb{Z}/30\mathbb{Z}$, hence an isomorphism $\mathcal{J}_c(\mathbb{F}_2)/2\mathcal{J}_c(\mathbb{F}_2) \cong \mathbb{Z}/2\mathbb{Z}$. Both of the rational points of $\mathcal{X}_c(\mathbb{F}_2)$ have nontrivial image in $\mathcal{J}_c(\mathbb{F}_2)/2\mathcal{J}_c(\mathbb{F}_2)$.

We verified all these properties of the given curves \mathcal{X}_c using the `ClassGroup` functionality in `magma` [BCP97]. \square

Lemma 3.10. *1. For every prime p , there exists an open compact subset $U_p \subset \mathcal{B}(\mathbb{Z}_p)$ such that for every $b \in U_p$, $\Delta(b) \neq 0$ and $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$.*
2. There exists an integer $N_3 \geq 1$ such that for every prime $p > N_3$ and for every $b \in \mathcal{B}(\mathbb{Z}_p)$ such that $\Delta(b) \neq 0$, we have $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$.

Proof. For each prime p , it is not difficult to find a point $c \in \mathcal{B}(\mathbb{F}_p)$ such that \mathcal{X}_c is smooth and $\mathcal{X}_c(\mathbb{F}_p)$ is non-empty. Taking U_p to be the preimage of c in $\mathcal{B}(\mathbb{Z}_p)$ establishes the first part of the lemma. The second part follows from Hensel's Lemma and the Weil bounds; here we are implicitly using the fact, already established in the proof of Lemma 3.5, that for any $c \in \mathcal{B}(\mathbb{F}_p)$, the irreducible components of \mathcal{X}_c are geometrically irreducible. \square

4 Counting points

In Section 3 we have defined an algebraic group over \mathbb{Z} and a representation \mathcal{V} , as well as various associated structures. In Section 4, we continue with the same notation and now show how to estimate the number of points in $G(\mathbb{Z}) \setminus \mathcal{V}(\mathbb{Z})$ of bounded height.

We first prove a simplified result, Theorem 4.1. The more refined version (Theorem 4.7), which is needed for applications, will be given at the end of this section. Let $L \subset B(\mathbb{R})$ be one of the subsets L_k described in Lemma 3.7, and let $s : L \rightarrow V(\mathbb{R})$ be the corresponding section. Then L is a connected semialgebraic subset of $B(\mathbb{R})$; s is a semialgebraic map; and $s(L)$ has compact closure in $V(\mathbb{R})$. The map $\Lambda \times L \rightarrow B(\mathbb{R})$, $(\lambda, \ell) \mapsto \lambda \cdot \ell$ given by the \mathbb{G}_m -action on B is an open immersion, and $\text{ht}(\lambda \cdot \ell) = \lambda^{\deg \Delta}$.

For any subset $A \subset \mathcal{V}(\mathbb{Z})$, we write A^{irr} for the subset of points $a \in A$ that are \mathbb{Q} -irreducible, in the sense of §2.3. We recall that r is the rank of H . Our first result is as follows.

Theorem 4.1. *There exist constants $C, \delta > 0$, not dependent on choice of L , such that*

$$\#G(\mathbb{Z}) \setminus \{v \in [G(\mathbb{R}) \cdot \Lambda \cdot s(L)] \cap \mathcal{V}(\mathbb{Z})^{\text{irr}} \mid \text{ht}(v) < a\} \leq C \cdot \text{vol}([1, a^{1/\deg \Delta}] \cdot L) + O(a^{\frac{1}{2} + r/\deg \Delta - \delta}).$$

Our proof is very similar to that of [Tho15, Theorem 3.1], except that a significant amount of case-by-case computation is required in order to control the contribution of elements that are ‘in the cusp’ (i.e. elements that lie in the codimension-one subspace of V where the coordinate corresponding to the highest root of H vanishes; see Proposition 4.5 below). To avoid repetition, we omit the details of proofs that are essentially the same as proofs appearing in [Tho15, §3].

First we introduce some notation. Recall that we have fixed a choice of $\mathfrak{S} = \omega T_c K \subset G(\mathbb{R})$ as in Proposition 3.1, where $\omega \subset \overline{N}(\mathbb{R})$ is a compact subset and $T_c \subset T(\mathbb{R})^\circ$ is open. As in [Tho15, Section 3.1], we fix a

compact semialgebraic set $G_0 \subset G(\mathbb{R}) \times \Lambda$ of non-empty interior with the property that $K \cdot G_0 = G_0$. We assume that the projection of G_0 to Λ is contained in $[1, C_0]$ for some constant C_0 and that $\text{vol}(G_0) = 1$. Given a subset $A \subset \mathcal{V}(\mathbb{Z})$ we let

$$\begin{aligned} N(A, a) &= \int_{h \in G_0} \#(\mathfrak{S}h \cdot \Lambda \cdot s(L) \cap \{v \in A^{\text{irr}} \mid \text{ht}(v) < a\}) dh \\ N^*(A, a) &= \int_{h \in G_0} \#(\mathfrak{S}h \cdot \Lambda \cdot s(L) \cap \{v \in A \mid \text{ht}(v) < a\}) dh. \end{aligned}$$

The following two lemmas are the analogues in our situation of [Tho15, Lemma 3.3] and [Tho15, Lemma 3.4]; the proofs are the same.

Lemma 4.2. *Let $A \subset V(\mathbb{Z})$ be a G -invariant subset. Then*

$$\#G(\mathbb{Z}) \setminus \{v \in [G(\mathbb{R}) \cdot \Lambda \cdot s(L)] \cap A^{\text{irr}} \mid \text{ht}(v) < a\} \leq N(A, a)$$

and

$$\#G(\mathbb{Z}) \setminus \{v \in [G(\mathbb{R}) \cdot \Lambda \cdot s(L)] \cap A \mid \text{ht}(v) < a\} \leq N^*(A, a).$$

Lemma 4.3. *Given $a \geq 1, n \in \overline{N}(\mathbb{R}), t \in T(\mathbb{R}),$ and $\lambda \in \Lambda,$ define $E(n, t, \lambda, a) = nt\lambda G_0 s(L) \cap \{v \in V(\mathbb{R}) \mid \text{ht}(v) < a\}.$ For any subset $A \subset V(\mathbb{Z}),$ we have*

$$N(A, a) \leq 2^r \int_{\lambda \in \Lambda} \int_{t \in T_c} \int_{n \in \omega} \#[E(n, t, \lambda, a) \cap A^{\text{irr}}] \delta_G(t)^{-1} dn dt d^\times \lambda$$

and

$$N^*(A, a) \leq 2^r \int_{\lambda \in \Lambda} \int_{t \in T_c} \int_{n \in \omega} \#[E(n, t, \lambda, a) \cap A] \delta_G(t)^{-1} dn dt d^\times \lambda,$$

where δ_G is as defined in Section 3.1.

In order to actually count points, we will use the following result, which follows from [BW14, Theorem 1.3]. This replaces the use of [Tho15, Proposition 3.5], itself based on a result of Davenport [Dav51]. We prefer to cite [BW14] since the possibility of applying [Dav51] to a general semialgebraic set rests implicitly on the Tarski–Seidenberg principle (see [Dav64]).

Theorem 4.4. *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 $u \in \text{GL}_n(\mathbb{R}),$ we have*

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

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 $Z.$

To state the next proposition, we recall that for any subset $M \subset \Phi_V,$ $V(M) \subset V$ is the linear subspace consisting of vectors $v = \sum_{\alpha \in \Phi_V} v_\alpha$ with $v_\alpha = 0$ for all $\alpha \in M.$ Given disjoint subsets $M_0, M_1 \subset \Phi_V,$ we define an open subscheme $V(M_0, M_1) \subset V(M_0)$ by

$$V(M_0, M_1) = \{v \in V(M_0) \mid v_\alpha \neq 0 \text{ for all } \alpha \in M_1\}.$$

We also define $S(M_0) = V(M_0)(\mathbb{Q}) \cap \mathcal{V}(\mathbb{Z})$ and $S(M_0, M_1) = V(M_0, M_1)(\mathbb{Q}) \cap \mathcal{V}(\mathbb{Z}).$ For ease of notation, if $M = \{\alpha\}$ is a single root, we write $S(M)$ as $S(\alpha).$

Proposition 4.5. *Let $\alpha_0 \in \Phi_V$ denote the highest root of H with respect to the root basis $S_H.$ Then there exists $\delta > 0$ such that $N(S(\alpha_0), a) = O(a^{\frac{1}{2}+r/\deg \Delta-\delta}).$*

Proof. We call a pair (M_0, M_1) of disjoint subsets of Φ_V a cusp datum. To prove the proposition, it suffices to find a set \mathcal{C} of cusp data such that

1. $S(\alpha_0)^{\text{irr}} \subset \bigcup_{(M_0, M_1) \in \mathcal{C}} S(M_0, M_1)$
2. If $(M_0, M_1) \in \mathcal{C}$, then $N^*(S(M_0, M_1), a) = O(a^{\frac{1}{2}+r/\deg \Delta-\delta})$.

Consider the partial order on Φ_V given by $\beta \geq \alpha$ if and only if $n_i(\beta - \alpha) \geq 0$ for all i , where n_i is as defined in Section 2.3. Let \mathcal{M} be the collection of subsets $M \subset \Phi_V$ such that if $\alpha \in M$ and $\beta \geq \alpha$ then $\beta \in M$. Given a subset $M \in \mathcal{M}$, we let $\lambda(M) = \{\alpha \in \Phi_V \mid M \cup \{\alpha\} \in \mathcal{M}\}$. We let \mathcal{C} be the collection of cusp data defined inductively as follows: in step 1, we form the cusp datum $(\{\alpha_0\}, \lambda(\{\alpha_0\}))$. In each successive step we create the set of cusp data $\{(M_0 \cup \{\alpha\}, \lambda(M_0 \cup \{\alpha\})) \mid \alpha \in M_1\}$ for each cusp datum (M_0, M_1) formed in the previous step, and then remove any cusp data such that M_0 satisfies any of the conditions of Proposition 2.15. By construction the collection \mathcal{C} satisfies condition 1 above. For each cusp datum $(M_0, M_1) \in \mathcal{C}$, we check that $N^*(S(M_0, M_1), a) = O(a^{\frac{1}{2}+r/\deg \Delta-\delta})$. To do so, by the same logic as in [Tho15, §5], it suffices to find a function $f : M_1 \rightarrow \mathbb{R}_{\geq 0}$ satisfying the following two conditions:

- $\sum_{\alpha \in M_1} f(\alpha) < \#M_0$
- For each $1 \leq i \leq r$, we have $\sum_{\alpha \in \Phi_G^+} n_i(\alpha) - \sum_{\alpha \in M_0} n_i(\alpha) + \sum_{\alpha \in M_1} f(\alpha) n_i(\alpha) > 0$.

One can program a computer to generate the list of cusp data in \mathcal{C} , after inputting the root datum of \mathfrak{h} and the description of its 2-grading, and then to verify that there exists such a function f for each $(M_0, M_1) \in \mathcal{C}$. We have carried out this verification process. Our code is available in the Mathematica notebooks `E7CuspData.nb` and `E8CuspData.nb`.² (In the name of efficiency, we actually follow a slightly different procedure, since it is time-consuming to check the condition in part 3 of Proposition 2.15. Namely, we generate a list of cusp data by eliminating only those pairs (M_0, M_1) such that M_0 satisfies the condition in part 2 of Proposition 2.15. For the cusp data on this list, we check that either a function f as above exists, or that one of the remaining conditions, i.e. part 1 or part 3 of Proposition 2.15, holds. When verifying the condition in part 3, we restrict our search to $\alpha \in M_1$. The end result is a collection of cusp data satisfying items 1 and 2 above, which suffices to prove the proposition.) \square

Proposition 4.6. *Let $N \geq 1$ be an integer, and let $v \in \mathcal{V}(\mathbb{Z})$. Let $A_{v,N} = v + N \cdot \mathcal{V}(\mathbb{Z})$. Then there exists $\delta > 0$ such that*

$$N^*(A_{v,N} - S(\alpha_0), a) \leq \frac{2^r |W_0|_\infty \text{vol}(\mathfrak{S})}{N^{\dim V}} \text{vol}([1, a^{1/\deg \Delta}] \cdot L) + O(a^{\frac{1}{2}+r/\deg \Delta-\delta}).$$

Proof. Let $\|\cdot\| : V(\mathbb{R}) \rightarrow \mathbb{R}_{\geq 0}$ denote the supremum norm with respect to the decomposition $\mathcal{V} = \bigoplus_{\alpha \in \Phi_V} \mathcal{V}_\alpha$ as a direct sum of free \mathbb{Z} -modules of rank 1. Let $J > 0$ be a constant such that $\|v\| \leq J$ for all $v \in \omega \cdot G_0 \cdot s(L)$. Let $F(n, t, \lambda, a) = \{v \in E(n, t, \lambda, a) \mid |v_{\alpha_0}| \geq 1\}$. If $F(n, t, \lambda, a) \neq \emptyset$, then $\lambda \alpha_0(t) \geq 1/J$. By Theorem 4.4, we have

$$\#((\mathcal{V}(\mathbb{Z}) - S(\alpha_0)) \cap E(n, t, \lambda, a)) = \#(\mathcal{V}(\mathbb{Z}) \cap F(n, t, \lambda, a)) = \text{vol}(F(n, t, \lambda, a)) + O(\lambda^{\dim V-1} \alpha_0(t)^{-1}).$$

Similarly we have

$$\#((A_{v,N} - S(\alpha_0)) \cap E(n, t, \lambda, a)) = N^{-\dim V} \text{vol}(F(n, t, \lambda, a)) + O(\lambda^{\dim V-1} \alpha_0(t)^{-1}). \quad (4.1)$$

²These Mathematica notebooks may be found at <https://www.dpmms.cam.ac.uk/~jat58/E7CuspData.nb> and <https://www.dpmms.cam.ac.uk/~jat58/E8CuspData.nb> respectively.

By Lemma 4.3, $N^*(A_{v,N} - S(\alpha_0), a)$ is bounded above by

$$\begin{aligned} & 2^r \int_{\lambda \in \Lambda} \int_{t \in T_c} \int_{n \in \omega} N^{-\dim V} \operatorname{vol}(F(n, t, \lambda, a)) \delta_G(t)^{-1} dn dt d^\times \lambda \\ & + 2^r \int_{\lambda=C_0^{-1}}^{a^{1/\deg \Delta}} \int_{t \in T_c} \int_{n \in \omega} O(\lambda^{\dim V-1} \alpha_0(t)^{-1}) \delta_G(t)^{-1} dn dt d^\times \lambda. \end{aligned} \quad (4.2)$$

The second term in (4.2) is $O(a^{\frac{1}{2}+(r-1)/\deg \Delta})$. Lemma 3.7 shows that the first term is bounded above by

$$\begin{aligned} & 2^r \int_{\lambda \in \Lambda} \int_{t \in T_c} \int_{n \in \omega} N^{-\dim V} \operatorname{vol}(E(n, t, \lambda, a)) \delta_G(t)^{-1} dn dt d^\times \lambda \\ & = \frac{2^r}{N^{\dim V}} \int_{\lambda \in \Lambda} \int_{g \in \mathfrak{S}} \int_{v \in V(\mathbb{R})} \int_{h \in G_0} \mathbf{1}_{v \in gh\lambda s(L), \operatorname{ht}(v) < a} dh dv dg d^\times \lambda \\ & \leq \frac{2^r |W_0|_\infty}{N^{\dim V}} \int_{h \in G_0} \operatorname{vol}(\mathfrak{S}) \operatorname{vol}([1, a^{1/\deg \Delta}] \cdot L) dh. \\ & = \frac{2^r |W_0|_\infty}{N^{\dim V}} \operatorname{vol}(\mathfrak{S}) \operatorname{vol}([1, a^{1/\deg \Delta}] \cdot L). \end{aligned}$$

This completes the proof. \square

We can now finish the proof of Theorem 4.1. By Lemma 4.2, we have

$$G(\mathbb{Z}) \setminus \{v \in [G(\mathbb{R}) \cdot \Lambda \cdot s(L)] \cap \mathcal{V}(\mathbb{Z})^{\operatorname{irr}} \mid \operatorname{ht}(v) < a\} \leq N(\mathcal{V}(\mathbb{Z}), a) \leq N(\mathcal{V}(\mathbb{Z}) - S(\alpha_0), a) + N^*(S(\alpha_0), a).$$

The result now follows on combining Proposition 4.5 and Proposition 4.6.

We now state the more refined version of Theorem 4.1 mentioned at the beginning of this section.

Theorem 4.7. *Let p_1, \dots, p_s be distinct primes, and for each $i \in \{1, \dots, s\}$, let $V_{p_i} \subset \mathcal{V}(\mathbb{Z}_{p_i}) \cap V(\mathbb{Q}_{p_i})^{\operatorname{reg.ss.}}$ be an open compact subset that is $G(\mathbb{Q}_{p_i})$ -invariant, in the sense that if $v \in V_{p_i}$, $g \in G(\mathbb{Q}_{p_i})$ and $gv \in \mathcal{V}(\mathbb{Z}_{p_i})$, then $gv \in V_{p_i}$. Let $A = \mathcal{V}(\mathbb{Z}) \cap (V_{p_1} \times \dots \times V_{p_s})$ (where we are identifying $\mathcal{V}(\mathbb{Z})$ with its image in $\mathcal{V}(\mathbb{Z}_{p_1}) \times \dots \times \mathcal{V}(\mathbb{Z}_{p_s})$ under the diagonal embedding). Then there exist constants $C, \delta > 0$ not depending on s or the sets V_{p_1}, \dots, V_{p_s} such that*

$$\#G(\mathbb{Q}) \setminus \{v \in A^{\operatorname{irr}} \mid \operatorname{ht}(v) < a\} \leq C \left(\prod_{i=1}^s \int_{b \in \mathcal{B}(\mathbb{Z}_{p_i})} \frac{\#(G(\mathbb{Q}_{p_i}) \setminus (V_{p_i} \cap V_b(\mathbb{Q}_{p_i})))}{\# \operatorname{Stab}_{G(\mathbb{Q}_{p_i})}(\kappa_b)} db \right) a^{\frac{1}{2}+r/\deg \Delta} + O(a^{\frac{1}{2}+r/\deg \Delta-\delta}).$$

Proof. We recall that for each prime p we have defined in the statement of Proposition 3.3 a locally constant function $m_p : V(\mathbb{Q}_p)^{\operatorname{reg.ss.}} \rightarrow \mathbb{R}$ by the formula

$$m_p(v) = \sum_{v' \in G(\mathbb{Z}_p) \setminus (G(\mathbb{Q}_p) \cdot v \cap \mathcal{V}(\mathbb{Z}_p))} \frac{\# \operatorname{Stab}_{G(\mathbb{Q}_p)}(v)}{\# \operatorname{Stab}_{G(\mathbb{Z}_p)}(v')}.$$

The same argument as in the proof of [Tho15, Corollary 3.9] leads to an estimate

$$\#G(\mathbb{Q}) \setminus \{v \in A^{\operatorname{irr}} \mid \operatorname{ht}(v) < a\} \leq 2^r \sum_{\substack{v \in G(\mathbb{Z}) \setminus A \\ \operatorname{ht}(v) < a}} \frac{1}{m_{p_i}(v)}.$$

Combining Lemma 4.2, Proposition 4.6, and Proposition 4.5, and summing over all choices of L as in Lemma 3.7, yields absolute constants $C, \delta > 0$ such that

$$\sum_{\substack{v \in G(\mathbb{Z}) \setminus A \\ \operatorname{ht}(v) < a}} \frac{1}{m_{p_i}(v)} \leq C \left(\prod_{i=1}^s \int_{v \in V_{p_i}} \frac{1}{m_{p_i}(v)} dv \right) a^{\frac{1}{2}+r/\deg \Delta} + O(a^{\frac{1}{2}+r/\deg \Delta-\delta}).$$

By the third part of Proposition 3.3, this expression is equal to

$$C \left(\prod_{i=1}^s |W_0|_{p_i} \operatorname{vol}(G(\mathbb{Z}_{p_i})) \right) \left(\prod_{i=1}^s \int_{b \in \mathcal{B}(\mathbb{Z}_{p_i})} \frac{\#(G(\mathbb{Q}_{p_i}) \setminus (V_{p_i} \cap V_b(\mathbb{Q}_{p_i})))}{\# \operatorname{Stab}_{G(\mathbb{Q}_{p_i})}(\kappa_b)} db \right) a^{\frac{1}{2} + r/\deg \Delta} + O(a^{\frac{1}{2} + r/\deg \Delta - \delta}).$$

The products $\prod_{i=1}^s |W_0|_{p_i} \operatorname{vol}(G(\mathbb{Z}_{p_i}))$ can be bounded independently of s and the primes p_1, \dots, p_s . They can therefore be absorbed into the constant, giving the estimate in the statement of the theorem. \square

5 Applications to 2-Selmer sets

In this final section, we prove our main theorems, including the results stated in the introduction, by combining all the theory developed so far. In order to avoid confusion, we treat each of the two families of curves (corresponding to Case **E**₇ and Case **E**₈) in turn.

5.1 Applications in Case **E**₇

As above, we write $\mathcal{B} = \operatorname{Spec} \mathbb{Z}[c_2, c_6, c_8, c_{10}, c_{12}, c_{14}, c_{18}]$ for affine space over \mathbb{Z} in 7 variables, and write $\mathcal{X} \rightarrow \mathcal{B}$ for the family of affine plane curves given by equation (1.2):

$$y^3 = x^3y + c_{10}x^2 + x(c_2y^2 + c_8y + c_{14}) + c_6y^2 + c_{12}y + c_{18}.$$

This family has the following interpretation:

Proposition 5.1. *Let k/\mathbb{Q} be a field. Then:*

1. *The locus inside \mathcal{B}_k above which the morphism $\mathcal{X}_k \rightarrow \mathcal{B}_k$ is smooth is the complement of an irreducible closed subset of \mathcal{B}_k of codimension 1.*
2. *The set of points $b \in \mathcal{B}(k)$ for which \mathcal{X}_b is smooth is in bijection with the set of equivalence classes of triples (C, P_1, t) , where:*
 - (a) *C is a smooth, non-hyperelliptic curve of genus 3 over k .*
 - (b) *$P_1 \in C(k)$ is a flex point in the canonical embedding, i.e. the projective tangent line to C at P_1 intersects C with multiplicity 3 at the point P_1 .*
 - (c) *$t \in T_{P_1}C$ is a non-zero Zariski tangent vector at the point P_1 .*

If b corresponds to (C, P_1, t) , then \mathcal{X}_b is isomorphic to $C - \{P_1, P_2\}$, where $P_2 \in C(k)$ is the unique point such that $3P_1 + P_2$ is a canonical divisor. For $\lambda \in k^\times$, the coefficients c_i satisfy the equality

$$c_i(C, P_1, \lambda t) = \lambda^{i/2} c_i(C, P_1, t).$$

Proof. Part 1 follows from the fact that \mathcal{X}_b is smooth if and only if $\Delta(b) \neq 0$. The proof of the second part is very similar to the proof of [Tho15, Lemma 4.1], although here we cannot appeal to Pinkham's Theorem. Let (C, P_1, t) be a tuple of the type described in the proposition, and let $P_2 \in C(k)$ be the point such that $3P_1 + P_2$ is a canonical divisor. The Riemann–Roch Theorem shows that $h^0(C, \mathcal{O}_C(3P_1)) = 2$ and $h^0(C, \mathcal{O}_C(2P_1 + P_2)) = 2$. We can therefore find functions $y, x \in k(C)^\times$, uniquely determined up to addition of constants, such that the polar divisor of y is $3P_1$ and the polar divisor of x is $2P_1 + P_2$, and such that $y = z^{-3} + \dots$, $x = z^{-2} + \dots$ locally at the point P_1 , where z is a local parameter at P_1 such that $dz(t) = 1$. We can also assume that y vanishes at the point P_2 .

The 10 monomials

$$1, x, x^2, y, yx, yx^2, yx^3, y^2, y^2x, y^3$$

all lie in the 9-dimensional space $H^0(C, \mathcal{O}_C(9P_1 + 2P_2))$ and are linearly independent, as can be seen by considering their polar divisors. It follows that they satisfy a unique linear relation of the form

$$y^3 = x^3y + x^2(c_4y + c_{10}) + x(c_2y^2 + c_8y + c_{14}) + c_6y^2 + c_{12}y + c_{18}. \quad (5.1)$$

The function y is uniquely determined by the above data. We also see that there is a unique translate $x + a$ ($a \in k$) such that, after replacing x by $x + a$, we have $c_4 = 0$ in equation (5.1). The homogenization of the equation (5.1) then describes the canonical embedding of the curve C . \square

If k/\mathbb{Q} is a field extension and $b \in \mathcal{B}(k)$ is such that \mathcal{X}_b is smooth, then we write Y_b for the unique smooth projective completion of \mathcal{X}_b .

As in the introduction, we define $\mathcal{F}_0 = \{b \in \mathcal{B}(\mathbb{Z}) \mid \mathcal{X}_{b,\mathbb{Q}} \text{ is smooth}\}$. We say that a subset $\mathcal{F} \subset \mathcal{F}_0$ is defined by congruence conditions if there exist distinct primes p_1, \dots, p_s and a non-empty open compact subset $U_{p_i} \subset \mathcal{B}(\mathbb{Z}_{p_i})$ for each $i \in \{1, \dots, s\}$ such that

$$\mathcal{F} = \mathcal{F}_0 \cap (U_{p_1} \times \dots \times U_{p_s}),$$

where we are taking the intersection inside $\mathcal{B}(\mathbb{Z}_{p_1}) \times \dots \times \mathcal{B}(\mathbb{Z}_{p_s})$.

We recall that for $b \in \mathcal{B}(\mathbb{R})$ we have defined $\text{ht}(b) = \sup_i |c_i(b)|^{126/i}$. This function is homogeneous of degree 126, in the sense that for $\lambda \in \mathbb{R}^\times$, we have $\text{ht}(\lambda \cdot b) = |\lambda|^{126} \text{ht}(b)$. (We note that 126 is the number of roots in the root system of type E_7 , and so also the degree of the discriminant polynomial Δ considered in §2.1.)

Lemma 5.2. *There exists a constant $\delta > 0$ such that if $\mathcal{F} \subset \mathcal{F}_0$ is a subset defined by congruence conditions as above, then*

$$\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\} = \left(\prod_{i=1}^r \text{vol}(U_{p_i}) \right) a^{\frac{1}{2} + \frac{7}{126}} + O(a^{\frac{1}{2} + \frac{7}{126} - \delta})$$

as $a \rightarrow \infty$.

Proof. This is an easy consequence of Theorem 4.4. \square

Our main theorems are now as follows.

Theorem 5.3. *Let $\mathcal{F} \subset \mathcal{F}_0$ be a subset defined by congruence conditions. Then*

$$\limsup_{a \rightarrow \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ \text{ht}(b) < a}} \#\text{Sel}_2(Y_b)}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} < \infty.$$

In order to state the next theorem, we observe that if $b \in \mathcal{B}(\mathbb{Q})$ is such that \mathcal{X}_b is smooth, then the 2-Selmer set $\text{Sel}_2(Y_b)$ always contains the ‘trivial’ classes arising from divisors supported on the points P_1, P_2 at infinity (as in the statement of Proposition 5.1). We write $\text{Sel}_2(Y_b)^{\text{triv}}$ for the subset of $\text{Sel}_2(Y_b)$ consisting of these classes, and note that $\#\text{Sel}_2(Y_b)^{\text{triv}} \leq 2$, with equality if and only if the divisor class $[(P_2) - (P_1)]$ is not divisible by 2 in $J_b(\mathbb{Q})$.

Theorem 5.4. *For any $\epsilon > 0$, there exists a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions such that*

$$\limsup_{a \rightarrow \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ \text{ht}(b) < a}} \#\text{Sel}_2(Y_b)}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} < 2 + \epsilon.$$

Consequently, for any such choice of \mathcal{F} we have

$$\liminf_{a \rightarrow \infty} \frac{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a \text{ and } \text{Sel}_2(Y_b) = \text{Sel}_2(Y_b)^{\text{triv}}\}}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} > 1 - \epsilon.$$

The proof of Theorem 5.4 is essentially a refined version of the proof of Theorem 5.3, so we just give the proof of Theorem 5.4.

Proof of Theorem 5.4. Let p_1, \dots, p_s be primes congruent to 1 modulo 6. Let $\varepsilon \in (0, 1)$ be as in Lemma 3.8, and for each $i \in \{1, \dots, s\}$, let $U_{p_i} \subset \mathcal{B}(\mathbb{Z}_{p_i})$ be the set described in the statement of Lemma 3.8. These sets have the following property: define

$$V_{p_i} = \pi^{-1}(U_{p_i}) \cap \mathcal{V}(\mathbb{Z}_{p_i}) \cap ([G(\mathbb{Q}_{p_i}) \cdot X(\mathbb{Q}_{p_i})] \cup [G(\mathbb{Q}_{p_i}) \cdot \kappa(\mathbb{Q}_p)] \cup [G(\mathbb{Q}_{p_i}) \cdot \kappa'(\mathbb{Q}_p)]),$$

where κ' is any Kostant section that is not G -conjugate to κ . Then V_{p_i} is an open compact subset of $\mathcal{V}(\mathbb{Z}_{p_i})^{\text{reg,ss.}}$, and for any $b \in U_{p_i}$ we have $\Delta(b) \neq 0$ and

$$\frac{\#(G(\mathbb{Q}_{p_i}) \setminus (V_{p_i} \cap V_b(\mathbb{Q}_{p_i})))}{\#\text{Stab}_{G(\mathbb{Q}_{p_i})}(\kappa_b)} \leq \varepsilon. \quad (5.2)$$

We let $\mathcal{F} = \mathcal{F}_0 \cap (U_{p_1} \times \dots \times U_{p_s})$. For any $b \in \mathcal{F}$, let $\text{Sel}_2(Y_b)^{\text{irr}} \subset \text{Sel}_2(Y_b)$ denote the subset of ‘nontrivial’ elements, i.e. the complement of $\text{Sel}_2(Y_b)^{\text{triv}}$ in $\text{Sel}_2(Y_b)$. Let $A = \mathcal{V}(\mathbb{Z}) \cap (V_{p_1} \times \dots \times V_{p_s})$. Then by Proposition 3.6, for any $a > 0$ we have

$$\sum_{\substack{b \in \mathcal{F} \\ \text{ht}(b) < a}} \# \text{Sel}_2(Y_b)^{\text{irr}} \leq G(\mathbb{Q}) \setminus \{v \in A^{\text{irr}} \mid \text{ht}(v) < N_1^{\deg \Delta} a\}.$$

By combining Theorem 4.7, Lemma 5.2, and the inequality (5.2), we see that there exist constants $C, \delta > 0$, not depending on s or the choice of primes p_1, \dots, p_s , such that

$$\frac{\sum_{\substack{b \in \mathcal{F} \\ \text{ht}(b) < a}} \# \text{Sel}_2(Y_b)^{\text{irr}}}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} \leq \frac{\varepsilon^s C + O(a^{-\delta})}{1 + O(a^{-\delta})}.$$

Since $\# \text{Sel}_2(Y_b) \leq 2 + \# \text{Sel}_2(Y_b)^{\text{irr}}$, the first sentence in the statement of the theorem now follows on choosing s sufficiently large and letting $a \rightarrow \infty$. The second sentence follows from the first on combining it with the following lemma. \square

Lemma 5.5. *Let $\mathcal{F} \subset \mathcal{F}_0$ be a family defined by congruence conditions. Then the limit*

$$\lim_{a \rightarrow \infty} \frac{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a, \# \text{Sel}_2(Y_b)^{\text{triv}} = 2\}}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}}$$

exists and equals 1.

Proof. Let $b \in \mathcal{F}$, and let $C_b = Z_H(\kappa_b)$, a maximal torus of H . The Galois action on C_b induces an associated homomorphism $\text{Gal}(\mathbb{Q}^s/\mathbb{Q}) \rightarrow W(H, C_b)$. Corollary 2.12 shows that if this homomorphism is surjective, then $\# \text{Sel}_2(Y_b)^{\text{triv}} = 2$. It therefore suffices to show that the limit

$$\lim_{a \rightarrow \infty} \frac{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a, \text{Gal}(\mathbb{Q}^s/\mathbb{Q}) \rightarrow W(H, C_b) \text{ surjective}\}}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}}$$

exists and equals 1. This is a variant of the Hilbert Irreducibility Theorem and can be proved along similar lines to the arguments in [Ser97, §13.2]. \square

Theorem 5.6. *For any $\epsilon > 0$, there exists a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions such that the following conditions are satisfied:*

1. *For every $b \in \mathcal{F}$ and every prime p , we have $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$.*

2. *We have*

$$\liminf_{a \rightarrow \infty} \frac{\#\{b \in \mathcal{F} \mid \mathcal{X}_b(\mathbb{Z}_{(2)}) = \emptyset\}}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} > 1 - \epsilon.$$

For the sets \mathcal{F} constructed in Theorem 5.6, we may say that a positive proportion of the curves \mathcal{X}_b ($b \in \mathcal{F}$) have integral points everywhere locally, but no integral points globally.

Proof. By Lemma 3.9 and Lemma 3.10, we can choose for every prime p an open compact subset $U_p \subset \mathcal{B}(\mathbb{Z}_p)$ such that the following conditions are satisfied:

1. For each $b \in U_2$, $\Delta(b) \neq 0$ and the image of the map $\mathcal{X}_b(\mathbb{Z}_2) \rightarrow J_b(\mathbb{Q}_2)/2J_b(\mathbb{Q}_2)$ does not intersect the subgroup generated by $[(P_1) - (P_2)]$.
2. For every prime p and for every $b \in U_p$ such that $\Delta(b) \neq 0$, the set $\mathcal{X}_b(\mathbb{Z}_p)$ is non-empty.
3. For every sufficiently large prime p , $U_p = \mathcal{B}(\mathbb{Z}_p)$.

Let $\mathcal{F} \subset \mathcal{F}_0$ be the corresponding subset defined by congruence conditions. Fix $\epsilon > 0$. By modifying U_p at sufficiently many primes congruent to 1 modulo 6, as in the proof of Theorem 5.4, we can assume moreover that the following condition is satisfied:

4. *We have*

$$\liminf_{X \rightarrow \infty} \frac{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a \text{ and } \text{Sel}_2(Y_b) = \text{Sel}_2(Y_b)^{\text{triv}}\}}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} > 1 - \epsilon.$$

To complete the proof of the theorem, we just need to show that if $b \in \mathcal{F}$ is such that $\text{Sel}_2(Y_b) = \text{Sel}_2(Y_b)^{\text{triv}}$, then $\mathcal{X}(\mathbb{Z}_{(2)}) = \emptyset$. To this end, we consider the commutative diagram

$$\begin{array}{ccc} \mathcal{X}_b(\mathbb{Z}_{(2)}) & \longrightarrow & \mathcal{X}_b(\mathbb{Z}_2) \\ \downarrow & & \downarrow \\ \text{Sel}_2(Y_b) & \longrightarrow & J_b(\mathbb{Q}_2)/2J_b(\mathbb{Q}_2), \end{array}$$

where the maps are the natural ones. By construction of U_2 , the image of the right-hand vertical map is contained in the complement of the subgroup generated by the divisor class $[(P_1) - (P_2)]$. By assumption, the image of the bottom horizontal map is contained in the subgroup generated by the divisor class $[(P_1) - (P_2)]$. This forces $\mathcal{X}_b(\mathbb{Z}_{(2)})$ to be empty, as desired. \square

5.2 Applications in Case E_8

We now forget the notation of §5.1, and write $\mathcal{B} = \text{Spec } \mathbb{Z}[c_2, c_8, c_{12}, c_{14}, c_{18}, c_{20}, c_{24}, c_{30}]$ for affine space over \mathbb{Z} in 8 variables, and write $\mathcal{X} \rightarrow \mathcal{B}$ for the family of affine plane curves given by equation (1.3):

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

This family has the following interpretation:

Proposition 5.7. *Let k/\mathbb{Q} be a field. Then:*

1. *The locus inside \mathcal{B}_k above which the morphism $\mathcal{X}_k \rightarrow \mathcal{B}_k$ is smooth is the complement of an irreducible closed subset of \mathcal{B}_k of codimension 1.*
2. *The set of points $b \in \mathcal{B}(k)$ for which \mathcal{X}_b is smooth is in bijection with the set of equivalence classes of triples (C, P, t) , where:*
 - (a) *C is a smooth, non-hyperelliptic curve of genus 4 over k .*
 - (b) *$P \in C(k)$ is a point such that $6P$ is a canonical divisor and $h^0(C, \mathcal{O}_C(3P)) = 2$.*
 - (c) *$t \in T_{PC}$ is a non-zero Zariski tangent vector at the point P .*

If b corresponds to (C, P_1, t) , then \mathcal{X}_b is isomorphic to $C - \{P\}$. For $\lambda \in k^\times$, the coefficients c_i satisfy the equality

$$c_i(C, P, \lambda t) = \lambda^i c_i(C, P, t).$$

The proof is very similar to the proof of [Tho15, Lemma 4.1] and to the proof of Proposition 5.1, so we omit it.

If k/\mathbb{Q} is a field extension and $b \in \mathcal{B}(k)$ is such that \mathcal{X}_b is smooth, then we write Y_b for the unique smooth projective completion of \mathcal{X}_b . As in Case **E₇**, we define $\mathcal{F}_0 = \{b \in \mathcal{B}(\mathbb{Z}) \mid \mathcal{X}_{b,\mathbb{Q}} \text{ is smooth}\}$, and we say that a subset $\mathcal{F} \subset \mathcal{F}_0$ is defined by congruence conditions if there exist distinct primes p_1, \dots, p_s and a non-empty open compact subset $U_{p_i} \subset \mathcal{B}(\mathbb{Z}_{p_i})$ for each $i \in \{1, \dots, s\}$ such that

$$\mathcal{F} = \mathcal{F}_0 \cap (U_{p_1} \times \dots \times U_{p_s}).$$

If $b \in \mathcal{B}(\mathbb{R})$, then we have $\text{ht}(b) = \sup_i |c_i(b)|^{240/i}$. This function is homogeneous of degree 240, in the sense that for $\lambda \in \mathbb{R}^\times$, we have $\text{ht}(\lambda b) = |\lambda|^{240} \text{ht}(b)$. As in Case **E₇**, an application of Theorem 4.4 shows that there exists a constant $\delta > 0$ such that if $\mathcal{F} \subset \mathcal{F}_0$ is a subset defined by congruence conditions as above, then

$$\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\} = \left(\prod_{i=1}^s \text{vol}(U_{p_i}) \right) a^{\frac{1}{2} + \frac{1}{30}} + O(a^{\frac{1}{2} + \frac{1}{30} - \delta})$$

as $a \rightarrow \infty$.

Our main theorems in Case **E₈** are as follows. We omit the proofs since they are similar, and simpler, than those in Case **E₇** in the previous section.

Theorem 5.8. *Let $\mathcal{F} \subset \mathcal{F}_0$ be a subset defined by congruence conditions. Then*

$$\limsup_{a \rightarrow \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ \text{ht}(b) < a}} \#\text{Sel}_2(Y_b)}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} < \infty.$$

Theorem 5.9. *For any $\epsilon > 0$, there exists a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions such that*

$$\limsup_{a \rightarrow \infty} \frac{\sum_{\substack{b \in \mathcal{F} \\ \text{ht}(b) < a}} \#\text{Sel}_2(Y_b)}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} < 1 + \epsilon.$$

Consequently, we have

$$\liminf_{a \rightarrow \infty} \frac{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a \text{ and } \#\text{Sel}_2(Y_b) = 1\}}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} > 1 - \epsilon.$$

Theorem 5.10. *For any $\epsilon > 0$, there exists a subset $\mathcal{F} \subset \mathcal{F}_0$ defined by congruence conditions such that the following conditions are satisfied:*

1. *For every $b \in \mathcal{F}$ and every prime p , we have $\mathcal{X}_b(\mathbb{Z}_p) \neq \emptyset$.*

2. *We have*

$$\liminf_{a \rightarrow \infty} \frac{\#\{b \in \mathcal{F} \mid \mathcal{X}_b(\mathbb{Z}_{(2)}) = \emptyset\}}{\#\{b \in \mathcal{F} \mid \text{ht}(b) < a\}} > 1 - \epsilon.$$

References

- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).
- [BG14] Manjul Bhargava and Benedict H. Gross. Arithmetic invariant theory. In *Symmetry: representation theory and its applications*, volume 257 of *Progr. Math.*, pages 33–54. Birkhäuser/Springer, New York, 2014.
- [BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1990.
- [Bor66] Armand Borel. Density and maximality of arithmetic subgroups. *J. Reine Angew. Math.*, 224:78–89, 1966.
- [Bor70] Armand Borel. 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, 1970.
- [Bou68] N. Bourbaki. *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines*. Actualités Scientifiques et Industrielles, No. 1337. Hermann, Paris, 1968.
- [BW14] Fabrizio Barroero and Martin Widmer. Counting lattice points and O-minimal structures. *Int. Math. Res. Not. IMRN*, (18):4932–4957, 2014.
- [CX08] Pete L. Clark and Xavier Xarles. Local bounds for torsion points on abelian varieties. *Canad. J. Math.*, 60(3):532–555, 2008.
- [Dav51] H. Davenport. On a principle of Lipschitz. *J. London Math. Soc.*, 26:179–183, 1951.
- [Dav64] H. Davenport. Corrigendum: “On a principle of Lipschitz”. *J. London Math. Soc.*, 39:580, 1964.
- [Hum95] James E. Humphreys. *Conjugacy classes in semisimple algebraic groups*, volume 43 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1995.
- [Igu00] Jun-ichi Igusa. *An introduction to the theory of local zeta functions*, volume 14 of *AMS/IP Studies in Advanced Mathematics*. American Mathematical Society, Providence, RI; International Press, Cambridge, MA, 2000.
- [KR71] B. Kostant and S. Rallis. Orbits and representations associated with symmetric spaces. *Amer. J. Math.*, 93:753–809, 1971.

- [Lor00] Dino Lorenzini. Reduction of points in the group of components of the Néron model of a Jacobian. *J. Reine Angew. Math.*, 527:117–150, 2000.
- [Mum77] David Mumford. Stability of projective varieties. *Enseignement Math. (2)*, 23(1-2):39–110, 1977.
- [Pan05] Dmitri I. Panyushev. On invariant theory of θ -groups. *J. Algebra*, 283(2):655–670, 2005.
- [PR94] Vladimir Platonov and Andrei Rapinchuk. *Algebraic groups and number theory*, volume 139 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.
- [PS14] Bjorn Poonen and Michael Stoll. Most odd degree hyperelliptic curves have only one rational point. *Ann. of Math. (2)*, 180(3):1137–1166, 2014.
- [RLYG12] Mark Reeder, Paul Levy, Jiu-Kang Yu, and Benedict H. Gross. Gradings of positive rank on simple Lie algebras. *Transform. Groups*, 17(4):1123–1190, 2012.
- [Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.
- [Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
- [Sta17] The Stacks Project Authors. Stacks project. <http://stacks.math.columbia.edu>, 2017.
- [Ste68] Robert Steinberg. *Endomorphisms of linear algebraic groups*. Memoirs of the American Mathematical Society, No. 80. American Mathematical Society, Providence, R.I., 1968.
- [Tho] Jack A. Thorne. On the average number of 2-Selmer elements of elliptic curves over $\mathbb{F}_q(X)$ with two marked points. Preprint.
- [Tho13] Jack A. Thorne. Vinberg’s representations and arithmetic invariant theory. *Algebra Number Theory*, 7(9):2331–2368, 2013.
- [Tho15] Jack A. Thorne. E_6 and the arithmetic of a family of non-hyperelliptic curves of genus 3. *Forum Math. Pi*, 3:e1, 41, 2015.
- [Tho16] Jack A. Thorne. Arithmetic invariant theory and 2-descent for plane quartic curves. *Algebra Number Theory*, 10(7):1373–1413, 2016. With an appendix by Tasho Kaletha.
- [Vin76] È. B. Vinberg. The Weyl group of a graded Lie algebra. *Izv. Akad. Nauk SSSR Ser. Mat.*, 40(3):488–526, 709, 1976.

BETH ROMANO blr24@dpmms.cam.ac.uk

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL PHYSICS, WILBERFORCE ROAD, CAMBRIDGE, CB3 0WB, UK

JACK A. THORNE thorne@dpmms.cam.ac.uk

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL PHYSICS, WILBERFORCE ROAD, CAMBRIDGE, CB3 0WB, UK