E_8 and the average size of the 3-Selmer group of the Jacobian of a pointed genus-2 curve

Beth Romano Jack A. Thorne

April 20, 2018

Abstract

We prove that the average size of the 3-Selmer group of a genus-2 curve with a marked Weierstrass point is 4.

Contents

1 Introduction

In this paper we prove new theorems about the arithmetic statistics of odd genus-2 curves. If $f(x) = x^5 + c_{12}x^3 + c_{18}x^2 + c_{24}x + c_{30} \in \mathbb{Q}[x]$ is a polynomial of non-zero discriminant, then the smooth projective completion of the affine curve

$$\mathscr{C}_f^0 : y^2 = f(x)$$

is a genus-2 curve with a marked Weierstrass point (the unique point at infinity). Conversely, any pair $(\mathscr{C}, \mathscr{P})$, where $\mathscr{C}$ is a (smooth, projective, connected) curve of genus 2 and $\mathscr{P} \in \mathscr{C}(\mathbb{Q})$ is a marked Weierstrass point, arises from a unique such polynomial $f(x)$ satisfying the following conditions:

1. The coefficients of $f(x)$ are integers and the discriminant of $f(x)$ is non-zero.
2. No polynomial of the form $n^{-10}f(n^2x)$ has integer coefficients, where $n \geq 2$ is an integer.

We write $\mathscr{E}$ for the set of all polynomials $f(x) = x^5+c_{12}x^3+c_{18}x^2+c_{24}x+c_{30} \in \mathbb{Z}[x]$ of non-zero discriminant, and $\mathscr{E}_{\text{min}} \subset \mathscr{E}$ for the subset satisfying condition 2. above. For $f(x) \in \mathscr{E}$, we write $\mathscr{C}_f$ for the corresponding pointed genus-2 curve and $\mathscr{J}_f$ for the Jacobian of $\mathscr{C}_f$, a principally polarized abelian surface over $\mathbb{Q}$. We define the height $\text{ht}(f)$ of a polynomial $f(x) \in \mathscr{E}$ by the formula

$$\text{ht}(f) = \sup_i |c_i(f)|^{120/i}.$$

Note that for any $a > 0$, the set $\{f \in \mathscr{E} | \text{ht}(f) < a\}$ is finite. We can now state our first main theorem.

Theorem 1.1 (Theorem 7.1)**.** *The average size of the 3-Selmer group* $\text{Sel}_3(\mathscr{J}_f)$ *for* $f \in \mathscr{E}_{min}$ *is 4. More precisely, we have*

$$\lim_{a \to \infty} \frac{\sum_{f \in \mathscr{E}_{min}, \text{ht}(f) < a} |\text{Sel}_3(\mathscr{J}_f)|}{|\{f \in \mathscr{E}_{min} \mid \text{ht}(f) < a\}|} = 4.$$

(A similar result can be proved for subsets of $\mathscr{E}_{\min}$ defined by congruence conditions. See Remark 7.3.)

Here is one consequence of Theorem 1.1 for rational points, which follows from work of Poonen and Stoll [PS14]:

Theorem 1.2. *A positive proportion of curves $(\mathscr{C}, \mathscr{P}) \in \mathscr{F}$ satisfy $\mathscr{C}(\mathbb{Q}) = \{\mathscr{P}\}$. More precisely, we have*

$$\liminf_{a \to \infty} \frac{|\{f \in \mathscr{E}_{min} \mid \mathrm{ht}(f) < a, |\mathscr{C}_f(\mathbb{Q})| = 1\}|}{|\{f \in \mathscr{E}_{min} \mid \mathrm{ht}(f) < a\}|} > 0.$$

1.1 Method of proof

In the paper [BG13], Bhargava and Gross calculated the average size of the the 2-Selmer group of the Jacobian of an odd hyperelliptic curve of fixed genus $g \geq 2$ using a connection with the arithmetic invariant theory of a graded Lie algebra; more precisely, the $\mathbb{Z}/2\mathbb{Z}$-graded Lie algebra arising from the element -1 of the automorphism group of a type A_{2g} root lattice. This amounts to studying the orbits of the group SO_{2g+1} on the space of traceless, self-adjoint $(2g+1) \times (2g+1)$ matrices.

In this paper, we exploit the stable $\mathbb{Z}/3\mathbb{Z}$-grading of the Lie algebra of type E_8 in order to study the 3-Selmer groups of odd genus-2 curves. Note that we are firmly in the territory of exceptional groups! In particular, there seems to be no hope of generalizing anything in this paper to study e.g. the 3-Selmer groups of hyperelliptic curves of higher genus. Nevertheless, we expect the methods developed in this paper to have applications elsewhere, for reasons we will soon explain.

Let H be a split reductive group over $\mathbb{Q}$ of type E_8, with split maximal torus T, and let $\check{\rho} : \mathbb{G}_m \to T$ be the sum of the fundamental coweights with respect to some choice root basis. The restriction θ of $\check{\rho}$ to μ_3 determines a stable $\mathbb{Z}/3\mathbb{Z}$-grading

$$\mathfrak{h} = \oplus_{i \in \mathbb{Z}/3\mathbb{Z}} \mathfrak{h}(i)$$

of the Lie algebra $\mathfrak{h} = \mathrm{Lie}\, H$, and hence a coregular representation of $G = H(0) = H^\theta$ on $V = \mathfrak{h}(1)$ (see e.g. [RLYG12] – the word 'stable' refers to the presence of stable G-orbits in V, i.e. orbits that are are closed and have finite stabilizers).

One can identify G with SL_9/μ_3 and V with the 3rd exterior power of the standard representation of SL_9. The relation between this representation and 3-descent on odd genus-2 curves has been studied previously by Rains and Sam [RS]. We do not use their work. Instead, we follow a different approach which we find more suited to studying integrality problems (of which more in a moment).

Using results of Vinberg, one can identify the geometric quotient $B = V /\!\!/ G = \mathrm{Spec}\, \mathbb{Q}[V]^G$ with the spectrum of the polynomial algebra $\mathbb{Q}[c_{12}, c_{18}, c_{24}, c_{30}]$ in 4 indeterminates (thus $c_{12}, \dots, c_{30}$ are algebraically independent G-invariant polynomials on V). We can therefore think of B as parameterizing polynomials $f(x) = x^5 + c_{12}x^3 + c_{20}x^2 + c_{24}x + c_{30}$. We write $V_f \subset V$ for the G-invariant closed subscheme given by the fibre of the quotient map $\pi : V \to B$ above a point f of the base.

The first step in the proof of Theorem 1.1 is to construct for any field $k/\mathbb{Q}$ and any $f \in B(k)$ of non-zero discriminant an injection

$$\eta_f : \mathscr{J}_f(k)/3\mathscr{J}_f(k) \to G(k)\backslash V_f(k), \tag{1.1}$$

where $\mathscr{J}_f$ is the Jacobian of the curve given by the equation $y^2 = f(x)$.

In fact, we go further than this, giving a version of this construction which works over any $\mathbb{Q}$-algebra R (and for any $f \in B(R)$ with discriminant that is a unit on R). If R is a ring over which every locally free module is free, then we obtain an injection

$$\eta_f : \mathscr{J}_f(R)/3\mathscr{J}_f(R) \to G(R)\backslash V_f(R), \tag{1.2}$$

recovering the previous map in the case that $R = k$ is a field.

This construction is based on changing our point of view from G-orbits in V to isomorphism classes of triples (H', θ', γ'), where H' is a reductive group of type E_8, θ' is a stable $\mathbb{Z}/3\mathbb{Z}$-grading, and $\gamma' \in \mathfrak{h}'(1)$. We give a construction that begins with a Heisenberg group (such as the μ_3-extension of $\mathscr{J}_f[3]$ arising from the Mumford theta group of thrice the canonical principal polarization of $\mathscr{J}_f$) and a representation W of this Heisenberg group, and returns a Lie algebra $\mathfrak{h}'$ of type E_8 with a stable $\mathbb{Z}/3\mathbb{Z}$-grading θ', together with a representation of $\mathfrak{g}' = (\mathfrak{h}')^{\theta'}$ on the same space W. The existence of this construction, which seems to be related to twisted vertex operator realizations of affine Kac–Moody algebras [Lep85], still seems remarkable to us! The general version of this construction will be described in a future work of the first author [Rom].

The next step in the proof of Theorem 1.1 is to introduce integral structures. All of the objects H, θ, G, V can be defined naturally over $\mathbb{Z}$, and we can require that our polynomials $c_{12}, \ldots, c_{30}$ lie in $\mathbb{Z}[V]^G$. If p is a prime and $f(x) = x^5 + c_{12}x^3 + c_{18}x^2 + c_{24}x + c_{30} \in \mathbb{Z}_p[x]$ is a polynomial of non-zero discriminant, then our constructions so far yield a map $\mathscr{J}_f(\mathbb{Q}_p)/3\mathscr{J}_f(\mathbb{Q}_p) \to G(\mathbb{Q}_p)\backslash V_f(\mathbb{Q}_p)$. However, it is essential to be able to show that each $G(\mathbb{Q}_p)$-orbit in $V_f(\mathbb{Q}_p)$ which is in the image of this map admits an integral representative, i.e. intersects $V_f(\mathbb{Z}_p)$ non-trivially. This has been a sticking point for some time. In our earlier papers [Tho15, RTa], our failure to construct integral representatives in full generality meant we could provide upper bounds only for the average sizes of the Selmer sets, and not full Selmer groups, of the families of curves studied there.

In this paper we introduce a new general technique to construct integral orbit representatives. We describe it briefly here. If $f(x) \in \mathbb{Z}_p[x]$ is a polynomial of non-zero discriminant, we choose a lifting to $\widetilde{f}(x) \in \mathbb{Z}_p[u][x]$ with favourable properties. In particular, the discriminant of $\widetilde{f}(x)$ should be non-zero in $\mathbb{F}_p[u]$ and square-free in $\mathbb{Q}_p[u]$. The construction giving rise to the map (1.2) determines a triple (H', θ', γ') over the complement in $\operatorname{Spec} \mathbb{Z}_p[u]$ of the locus where the discriminant of $\widetilde{f}$ vanishes.

Using an explicit construction of integral representatives in the square-free discriminant case, we extend this triple to the complement in $\operatorname{Spec} \mathbb{Z}_p[u]$ of finitely many closed points. Finally, we use the fact that a reductive group on the punctured spectrum of a 2-dimensional regular local ring extends uniquely to the whole spectrum (see [CTS79, Theorem 6.13]) to extend our triple further to the whole of $\operatorname{Spec} \mathbb{Z}_p[u]$. Specializing to $u = 0$, we find the desired integral representative.

This argument is inspired by the proof of the fundamental lemma for Lie algebras [Ngô 10]. The problem of constructing integral representatives can be viewed as the problem of showing that a graded analogue of an affine Springer fibre is non-empty. From this point of view, attempting to deform the problem to a case where it can be solved directly is a natural strategy. Although we develop this technique here just in the case of the stable $\mathbb{Z}/3\mathbb{Z}$-grading of E_8 and its relation to odd genus-2 curves, it is completely general. In a future work [RTb], we will return to the families of curves studied in our earlier papers [Tho15, RTa] and obtain complete information about the average sizes of the 2-Selmer groups of their Jacobians.

Once integral representatives have been constructed, we can reduce the problem of studying the average size of the 3-Selmer groups of the curves $\mathscr{C}_f$ to the problem of studying the number of orbits of $G(\mathbb{Z})$ in $V(\mathbb{Z})$ of bounded height (with congruence conditions and local weights imposed). In the final step in the proof of Theorem 1.1, we use Bhargava's techniques and their interpretation in the framework of graded Lie algebras (as in e.g. [BG13], [Tho15]) to carry out this orbit count and finally prove Theorem 1.1.

Remark 1.3. In the second author's thesis [Tho13], simple curve singularities and their deformations played an important role. The same is true here. The family of affine curves given by the equation $y^2 = x^5 + c_{12}x^3 + c_{18}x + c_{24}x + c_{30}$ is a versal deformation of a type A_4 singularity. Here, we think of this family instead as being embedded in the family of affine surfaces

$$y^2 = z^3 + x^5 + c_{12}x^3 + c_{18}x + c_{24}x + c_{30}.$$

This is a versal deformation of the E_8 surface singularity $y^2 = z^3 + x^5$, together with its action of μ_3 by the formula $\zeta \cdot (x, y, z) = (x, y, \zeta^{-1} z)$. This fact plays an important role in §4.4.

1.2 Organization of this paper

We now describe the organization of this paper. In §2 we review relevant properties of the E_8 root lattice and its associated Weyl group. In §3, fundamental for the construction of orbits, we give our "Heisenberg group to graded Lie algebra" functor. In §4, we describe the invariant theory of our graded Lie algebra, and use the construction of §3 to parameterize and construct orbits. An important role is played by two special transverse slices to nilpotent elements, namely the Kostant section and the subregular Slodowy slice: we use the first of these to normalize the set of orbits, and the second to normalize our generators for the ring of G-invariant polynomials on V.

In §5 we give our construction of integral orbit representatives. We treat the local case using the ideas described above, and then deduce the existence of integral orbit representations for Selmer elements in the global case as a consequence. In §6, we give the point-counting results we need in order to prove Theorem 1.1. The power of Bhargava's techniques is such that little more than formal verification is required in order to check that they give the desired result here. We have therefore given a compressed treatment, describing only what is new in this particular case; we trust that the interested reader will be able to easily fill in the details, interpolating from e.g. the proof of [BG13, Theorem 25].

Finally, in §7 we combine all of this to prove our main theorems.

1.3 Acknowledgments

Both authors received support from EPSRC First Grant EP/N007204/1. This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 714405).

1.4 Notation

If H is a group scheme, then we will use a gothic letter $\mathfrak{h} = \operatorname{Lie} H$ for its Lie algebra. If $\theta : \mu_n \to \operatorname{Aut}(H)$ is homomorphism, then we write $\mathfrak{h} = \oplus_{i \in \mathbb{Z}/n\mathbb{Z}} \mathfrak{h}(i)$ for the corresponding grading; thus $\mathfrak{h}(i)$ is the isotypic subspace in $\mathfrak{h}$ corresponding to the character $\zeta \mapsto \zeta^i$ of μ_n.

If G is a group scheme over a base S, X an S-scheme on which G acts, T an S-scheme, and $x \in X(T)$, then we write $Z_G(x)$ for the scheme-theoretic stabilizer of x, which is a T-scheme. By a Lie algebra over S, we mean a coherent sheaf of $\mathcal{O}_S$-modules $\mathfrak{g}$ together with an alternating bilinear form $[\cdot, \cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ that satisfies the Jacobi identity. Similarly, if $\mathfrak{g}$ is a Lie algebra that is equipped with a Lie algebra homomorphism $\mathfrak{g} \to \operatorname{End}_{\mathcal{O}_S}(W)$, for some locally free sheaf W of $\mathcal{O}_S$-modules, and $x \in W \otimes_{\mathcal{O}_S} \mathcal{O}_T$, then we define $\mathfrak{z}_{\mathfrak{g}}(x)$ to be the Lie centralizer of x, which is a Lie algebra over T.

If G is reductive and $A \subset G$ is a maximal torus, we write $X^*(A) = \operatorname{Hom}(A, \mathbb{G}_m)$ for its character group, $\Phi(G, A) \subset X^*(A)$ for its set of roots, and $X_*(A)$ for its cocharacter group. We write $N_G(A)$ for the normalizer of A and $W(G, A) = N_G(A)/A$ for the Weyl group of A in G.

If G is a smooth group scheme over a scheme S, then we write $H^1(S, G)$ for the set of isomorphism classes of G-torsors over S, which we think of as a non-abelian étale cohomology set. If $S = \operatorname{Spec} R$ is affine then we will write $H^1(R, G)$ for the same object.

If G is a smooth linear algebraic group over a field k which acts on an integral affine variety X, and G^0 is reductive, then we write $X/\!\!/G = \operatorname{Spec} k[X]^G$ for the categorical quotient, which is again an integral affine variety.

2 The E_8 root lattice

Throughout this paper, we will constantly make use of the properties of a certain conjugacy class of automorphisms of the E_8 root lattice. We therefore record some of these properties here. For us, an E_8 root lattice Λ is a finite free $\mathbb{Z}$-module, equipped with a symmetric bilinear pairing $(\cdot,\cdot) : \Lambda \times \Lambda \to \mathbb{Z}$ with the following property: let $\Phi \subset \Lambda$ be the set of elements $\alpha \in \Lambda$ with $(\alpha, \alpha) = 2$. Then Φ forms a root system in $\Lambda_{\mathbb{R}}$ of Dynkin type E_8 (elements of Φ are called roots). Any two E_8 root lattices are isomorphic.

Let Λ be an E_8 root lattice with $\Phi \subset \Lambda$ its set of roots. Note that because E_8 is simply laced, if $\alpha, \beta \in \Phi$, then $\alpha + \beta \in \Phi$ if and only if $(\alpha, \beta) = -1$. We will make frequent use of this fact throughout the proofs in §3. Given $\gamma \in \Lambda$, we define $\check{\gamma}$ to be the element of the dual lattice $\Lambda^\vee = \operatorname{Hom}(\Lambda, \mathbb{Z})$ given by $\check{\gamma}(\mu) = (\gamma, \mu)$ for all $\mu \in \Lambda$. We note that the map $\Lambda \to \Lambda^\vee$ defined by $\gamma \mapsto \check{\gamma}$ is an isomorphism of lattices. If $\alpha \in \Phi$ is a root, then $\check{\alpha}$ is called a coroot.

We write $\operatorname{Aut}(\Lambda)$ for the group of automorphisms of Λ that preserve the pairing $(\cdot,\cdot)$. Since E_8 has no diagram automorphisms, $\operatorname{Aut}(\Lambda)$ equals the Weyl group $W(\Lambda)$, which is generated by the reflections in the root hyperplanes $\alpha^\perp$ (for $\alpha \in \Phi$). We recall that an element $w \in W(\Lambda)$ is said to be elliptic if $\Lambda^w = 0$.

Lemma 2.1. *$W(\Lambda)$ contains a unique conjugacy class of elliptic elements of order 3. Let w be such an element, and let $\Lambda_w = \Lambda/(w-1)\Lambda$ be the group of w-coinvariants in Λ. Then:*

1. *There is an isomorphism $\Lambda_w \cong \mathbb{F}_3^4$.*
2. *Any choice of orbit representatives for the action of $\langle w \rangle$ on Φ gives a complete set of coset representatives for the non-zero elements of Λ_w. The centralizer of w in $W(\Lambda)$ acts transitively on $\Lambda_w - \{0\}$.*

Proof. See [Ree11, Table 1] and [Ree11, Lemma 4.4]. □

We also note for later use that if $w \in W(\Lambda)$ is elliptic of order 3, then $w^2\gamma + w\gamma + \gamma = 0$ for all $\gamma \in \Lambda$. In [Ree11], for any elliptic element $w \in W(\Lambda)$, Reeder defines a symplectic pairing on Λ_w that is invariant under the action of the centralizer of w in $W(\Lambda)$. We now describe a slight variant of this pairing.

Let S be a $\mathbb{Z}[1/3]$-scheme. We now let Λ be an étale sheaf of E_8 root lattices on S. By this we mean that Λ is a locally constant étale sheaf of finite free $\mathbb{Z}$-modules, which is equipped with a pairing $\Lambda \times \Lambda \to \mathbb{Z}$ making each stalk $\Lambda_{\overline{s}}$ above a geometric point $\overline{s} \to S$ into an E_8 root lattice. Then $\operatorname{Aut}(\Lambda)$ is a finite étale S-group.

In this setting we define an elliptic μ_3-action on Λ to be a homomorphism $\theta : \mu_3 \to \operatorname{Aut}(\Lambda)$ such that for any geometric point $\overline{s} \to S$ and any primitive 3rd root of unity $\zeta \in \mu_3(\overline{s})$, $\theta(\zeta) \in \operatorname{Aut}(\Lambda_{\overline{s}})$ is an elliptic element of order 3.

If θ is an elliptic μ_3-action on Λ, then we write Λ_θ for the sheaf of θ-coinvariants; by Lemma 2.1, it is a locally constant étale sheaf of $\mathbb{F}_3$-vector spaces of rank 4. We define a pairing $\langle\cdot,\cdot\rangle : \Lambda_\theta \times \Lambda_\theta \to \mu_3$ by the formula

$$\langle \lambda, \mu \rangle = \zeta^{((1-\theta(\zeta))\lambda, \mu)}, \tag{2.1}$$

for any primitive 3rd root of unity ζ. (Despite appearances, the pairing does not depend on a choice of root of unity.)

Lemma 2.2. *The pairing (2.1) is symplectic and non-degenerate, and it induces an isomorphism $\Lambda_\theta \cong \mathrm{Hom}(\Lambda_\theta, \mu_3)$.*

Proof. This can be checked on geometric points, in which case it reduces to [Ree11, Lemma 2.2, Lemma 2.3]. □

Let H be a reductive group over S with geometric fibres of type E_8. We define a stable $\mathbb{Z}/3\mathbb{Z}$-grading of H to be a homomorphism $\theta : \mu_3 \to H$ such that for each geometric point $\overline{s} \to S$, there exists a maximal torus $A \subset H_{\overline{s}}$ that is normalized by the image of θ and such that the induced map $\mu_3 \to \mathrm{Aut}(X^*(A))$ is an elliptic μ_3-action (this definition makes sense since $X^*(A)$ is an E_8 root lattice). Note that any such θ is then automatically a closed immersion, cf. [Con14, Lemma B.1.3].

The next lemma shows that any two stable $\mathbb{Z}/3\mathbb{Z}$-gradings are conjugate étale locally on the base.

Lemma 2.3. *Let S be a $\mathbb{Z}[1/3]$-scheme. Let (H, θ) and (H', θ') be two pairs consisting of a reductive group over S with geometric fibres of type E_8 and a stable $\mathbb{Z}/3\mathbb{Z}$-grading. Then for any $s \in S$ there exists an étale morphism $S' \to S$ with image containing s and an isomorphism $H_{S'} \to H'_{S'}$ intertwining $\theta_{S'}$ and $\theta'_{S'}$.*

Proof. The question is étale local on S, so we can assume that $H = H'$ are both split reductive groups. Let T denote the scheme of elements $h \in H$ such that $\mathrm{Ad}(h) \circ \theta = \theta'$; this is a closed subscheme of H which is smooth over S, by [Con14, Proposition 2.1.2]. Since surjective smooth morphisms have sections étale locally, we just need to show that $T \to S$ is surjective. Since the formation of T commutes with base change, we are therefore free to assume that $S = \mathrm{Spec}\, k$ is the spectrum of an algebraically closed field.

In this case, there exist (by assumption) maximal tori A, $A' \subset H$ on which θ, θ' act through elliptic automorphisms of order 3. Using the conjugacy of maximal tori, we can therefore assume that $A = A'$. Using Lemma 2.1, we can assume that θ, θ' define the same element of the Weyl group of A.

We have therefore reduced the problem to the statement that if $w \in W(H, A)$ is an elliptic element of order 3, then any two lifts n, n' to the normalizer $N_H(A)(k)$ are $H(k)$-conjugate. In fact, they are even $A(k)$-conjugate, as follows from the fact that the morphism $1 - w : A \to A$ is étale (and surjective). This completes the proof. □

3 A functor

Let R be a $\mathbb{Z}[1/3]$-algebra. In this section we describe a functorial construction of a graded Lie algebra over R from a Heisenberg group. We will later observe that the input data can be constructed from a genus-2 curve with a Weierstrass point (see §4.3).

3.1 Two groupoids

We first need to introduce some notation.

We write Heis_R for the groupoid of triples $(\Lambda, \theta, \mathscr{H})$, where:

1. Λ is an étale sheaf of E_8 root lattices on $\mathrm{Spec}\, R$ in the sense described in §2 with symmetric pairing $(\cdot, \cdot) : \Lambda \times \Lambda \to \mathbb{Z}$.

2. $\theta : \mu_3 \to \mathrm{Aut}(\Lambda)$ is an elliptic μ_3-action on Λ.

3. $\mathscr{H}$ is a central extension
$$1 \to \mu_3 \to \mathscr{H} \to \Lambda_\theta \to 1$$
of étale R-groups, with the property that the induced commutator pairing $\Lambda_\theta \times \Lambda_\theta \to \mu_3$ is the same as the pairing $\langle \cdot, \cdot \rangle : \Lambda_\theta \times \Lambda_\theta \to \mu_3$ given by (2.1).

Morphisms $(\Lambda, \theta, \mathscr{H}) \to (\Lambda', \theta', \mathscr{H}')$ in Heis_R are pairs of isomorphisms $\alpha : \Lambda \to \Lambda'$, $\beta : \mathscr{H} \to \mathscr{H}'$ intertwining θ and θ' and making the induced diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_3 \arrow[r] \arrow[d, "="] & \mathscr{H} \arrow[r] \arrow[d, "\beta"] & \Lambda_\theta \arrow[r] \arrow[d, "\alpha_\theta"] & 1 \\
1 \arrow[r] & \mu_3 \arrow[r] & \mathscr{H}' \arrow[r] & \Lambda'_{\theta'} \arrow[r] & 1
\end{tikzcd}$$

commute. (Here α_θ is the map naturally induced by α.)

We write GrLieT_R for the groupoid of triples (H, θ, A), where:

1. H is a reductive group over R with geometric fibres all of Dynkin type E_8.

2. $A \subset H$ is a maximal torus.

3. $\theta : \mu_3 \to H$ is a homomorphism whose image normalizes A, and such that the induced map $\theta : \mu_3 \to \mathrm{Aut}(X^*(A))$ is an elliptic μ_3-action.

Morphisms $(H, \theta, A) \to (H', \theta', A')$ in this category are given by isomorphisms $\gamma : H \to H'$ sending A to A' and intertwining θ and θ'. If $S = \operatorname{Spec} R$ is an affine scheme over $\mathbb{Z}[1/3]$, then we will also occasionally write Heis_S and GrLieT_S for the categories Heis_R and GrLieT_R.

Note that if $R \to R'$ is a homomorphism of $\mathbb{Z}[1/3]$-algebras, then pullback determines functors $\mathrm{Heis}_R \to \mathrm{Heis}_{R'}$ and $\mathrm{GrLieT}_R \to \mathrm{GrLieT}_{R'}$. We could define stacks Heis and GrLieT over $\mathbb{Z}[1/3]$, and even try to represent them as quotient stacks using the objects introduced in §4 (as in [HLHN14]). We have chosen not to do this here in order to avoid obscuring the main point of our constructions, which are based on relatively explicit calculations.

We will introduce variants of these categories in §4.3. In particular, we will introduce the category GrLie_R of pairs (H, θ) (we forget the torus).

3.2 Definition of the functor

The main goal of §3 is to prove the following theorem.

Theorem-Construction 3.1. *Let $N = 2 \times 3 \times 5 \times 7$, and $S = \mathbb{Z}[1/N]$. Then for each S-algebra R, there is a functor* $\mathrm{Heis}_R \to \mathrm{GrLieT}_R$*, compatible with arbitrary base change $R \to R'$.*

We now define the functor $\mathrm{Heis}_R \to \mathrm{GrLieT}_R$. Let $(\Lambda, \theta, \mathscr{H}) \in \mathrm{Heis}_R$. We can assume $\operatorname{Spec} R$ is connected. Let $R \to R'$ be a Galois finite étale extension[1] over which Λ and $\mathscr{H}$ become constant. Let $\Gamma = \mathrm{Aut}_R(R')$. We will first define a Lie algebra over R' and then recover a Lie algebra over R by étale descent. (For this

[1] i.e. a ring map such that $\operatorname{Spec} R' \to \operatorname{Spec} R$ is a surjective, finite étale morphism which is a Galois covering

naive form of étale descent, see [Sta18, Tag 0D1V].) For the remainder of the section we fix a choice of primitive 3rd root of unity $\zeta \in \mu_3(R')$. For ease of notation, we write $w = \theta(\zeta)$.

Let $\Phi \subset \Lambda$ be the set of roots, let $\widetilde{\Lambda} = \Lambda \times_{\Lambda_\theta} \mathscr{H}$, and let $\widetilde{\Phi}$ denote the pre-image of Φ in $\widetilde{\Lambda}$. Thus $\widetilde{\Lambda}$ is a central extension

$$1 \to \mu_3 \to \widetilde{\Lambda} \to \Lambda \to 1$$

that also has commutator pairing given by $\langle \cdot, \cdot \rangle$, and $\widetilde{\Phi} \to \Phi$ is a 3-fold cover. For an element $\widetilde{\alpha} \in \widetilde{\Phi}$, we write α for the image of $\widetilde{\alpha}$ in Φ.

To construct an element of $\mathrm{GrLieT}_{R'}$, we first let A be the torus over R with $X^*(A) = \Lambda$. We next construct a Lie algebra over R' of type E_8. Let $\mathfrak{a} = \operatorname{Lie} A$. Note that $\mathfrak{a}_{R'} \cong \operatorname{Hom}(\Lambda, R')$, and so for any $\alpha \in \Phi$, the coroot $\check{\alpha}$ corresponds to an element of $\mathfrak{a}_{R'}$. In fact $\mathfrak{a}_{R'}$ is generated by $\{\check{\alpha} \mid \alpha \in \Phi\}$. Let $\mathfrak{h}'$ be the quotient of the free R'-module with basis elements $X_{\widetilde{\alpha}}$, $\widetilde{\alpha} \in \widetilde{\Phi}$, by the relations $X_{\zeta\widetilde{\alpha}} = \zeta X_{\widetilde{\alpha}}$ (for any $\widetilde{\alpha} \in \widetilde{\Phi}$). Finally, let $\mathfrak{h}_{R'} = \mathfrak{a}_{R'} \oplus \mathfrak{h}'$. Thus $\mathfrak{h}_{R'}$ is a free R'-module of rank 248 generated by $\{\check{\alpha}, X_{\widetilde{\beta}} \mid \alpha \in \Phi, \widetilde{\beta} \in \widetilde{\Phi}\}$ (by abuse of notation we also write $X_{\widetilde{\beta}}$ for the image of this vector in $\mathfrak{h}'$).

We define a bilinear map $[\cdot, \cdot] : \mathfrak{h}_{R'} \times \mathfrak{h}_{R'} \to \mathfrak{h}_{R'}$ as follows. We set $[x, y] = 0$ for any $x, y \in \mathfrak{a}$. We let

$$[\check{\alpha}, X_{\widetilde{\beta}}] = -[X_{\widetilde{\beta}}, \check{\alpha}] = (\alpha, \beta) X_{\widetilde{\beta}}$$

for any $\alpha \in \Phi, \widetilde{\beta} \in \widetilde{\Lambda}$. Finally, the bracket of vectors $X_{\widetilde{\alpha}}$, $X_{\widetilde{\beta}}$ is defined by the formula

$$[X_{\widetilde{\alpha}}, X_{\widetilde{\beta}}] = \begin{cases} -\widetilde{\alpha}\widetilde{\beta}\check{\alpha} & \text{if } \alpha + \beta = 0. \\ (-1)^{(\alpha, w\beta)} \langle \alpha, \beta \rangle X_{\widetilde{\alpha}\widetilde{\beta}} & \text{if } \alpha + \beta \in \Phi. \\ 0 & \text{otherwise.} \end{cases}$$

We observe that the map is well-defined, i.e. it respects the defining relation $X_{\zeta\widetilde{\alpha}} = \zeta X_{\widetilde{\alpha}}$.

Proposition 3.2. *With the above definition, $\mathfrak{h}_{R'}$ is a Lie algebra (i.e. the bracket $[\cdot, \cdot]$ is antisymmetric and satisfies the Jacobi identity).*

In order to prove the proposition, we first make the following observation.

Lemma 3.3. *If $\alpha, \beta, \alpha + \beta \in \Phi$, then $(-1)^{(\alpha, w\beta)} + (-1)^{(w\alpha, \beta)} = 0$.*

Proof. We have $(-1)^{(\alpha, w\beta)} = (-1)^{(w^2\alpha, \beta)} = (-1)^{(-\alpha - w\alpha, \beta)} = (-1)^{(w\alpha, \beta)+1}$ since $(\alpha, \beta) = -1$. □

We also point out the useful fact that because the pairing $\langle \cdot, \cdot \rangle$ is alternating, we have $\widetilde{\alpha}\widetilde{\beta} = \widetilde{\beta}\widetilde{\alpha}$ whenever $\alpha + \beta = 0$.

Proof of Proposition 3.2. Using Lemma 3.3 and the fact that the pairing $\langle \cdot, \cdot \rangle$ is alternating, it is not hard to check that the bracket $[\cdot, \cdot]$ is antisymmetric. Thus it suffices to check the Jacobi identity. Consider

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] \tag{3.1}$$

for generators x, y, z. If any of x, y, z are in $\mathfrak{a}_{R'}$, then it follows easily from the definition of the bracket that (3.1) is zero.

Thus we restrict our attention to the case when $x = X_{\widetilde{\alpha}}, y = X_{\widetilde{\beta}}$ and $z = X_{\widetilde{\gamma}}$ for some $\widetilde{\alpha}, \widetilde{\beta}, \widetilde{\gamma} \in \widetilde{\Lambda}$.

First suppose $\alpha+\beta+\gamma=0$. Then $\beta+\gamma=-\alpha\in\Phi$, and similarly $\beta+\gamma, \alpha+\beta\in\Phi$. So we have

$$\begin{aligned}
[x,[y,z]]+[y,[z,x]]+[z,[x,y]] &= (-1)^{(\beta,w\gamma)}\langle\beta,\gamma\rangle[X_{\widetilde{\alpha}}, X_{\widetilde{\beta}\widetilde{\gamma}}]+(-1)^{(\gamma,w\alpha)}\langle\gamma,\alpha\rangle[X_{\widetilde{\beta}}, X_{\widetilde{\gamma}\widetilde{\alpha}}] \\
&\quad +(-1)^{(\alpha,\beta)}\langle\alpha,\beta\rangle[X_{\widetilde{\gamma}}, X_{\widetilde{\alpha}\widetilde{\beta}}] \\
&= -\widetilde{\alpha}\widetilde{\beta}\widetilde{\gamma}\left[(-1)^{(\beta,w\gamma)}\langle\beta,\gamma\rangle\check{\alpha}+(-1)^{(\gamma,w\alpha)}\langle\gamma,\alpha\rangle\check{\beta}+(-1)^{(\alpha,w\beta)}\langle\alpha,\beta\rangle\check{\gamma}\right].
\end{aligned}$$

Replacing γ by $-\alpha-\beta$ and $\check{\gamma}$ by $-\check{\alpha}-\check{\beta}$ and using the fact that $(\beta,w\beta)=(\alpha,w\alpha)=-1$, we may simplify this equation to

$$[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=\widetilde{\alpha}\widetilde{\beta}\widetilde{\gamma}\left[(-1)^{(\beta,w\alpha)}\langle\beta,-\alpha\rangle+(-1)^{(\alpha,w\beta)}\langle\alpha,\beta\rangle\right](\check{\alpha}+\check{\beta}),$$

which is zero by Lemma 3.3.

For the rest of the proof we assume $\alpha+\beta+\gamma\neq 0$. For (3.1) to be nonzero, at least one term in (3.1) must be nonzero. Without loss of generality, we may assume the first term is nonzero, and so either $\beta+\gamma=0$ or $\beta+\gamma\in\Phi$. We deal with each of these cases separately.

Case 1: $\beta+\gamma=0$.

In this case the first term of (3.1) is $(\alpha,\beta)\widetilde{\beta}\widetilde{\gamma}X_{\widetilde{\alpha}}$. By assumption $(\alpha,\beta)\neq 0$. Suppose $(\alpha,\beta)=-1$. Then $(\alpha,\gamma)=1$ and $(\gamma,\alpha+\beta)=-1$, so

$$\begin{aligned}
[x,[y,z]]+[y,[z,x]]+[z,[x,y]] &= -\widetilde{\beta}\widetilde{\gamma}X_{\widetilde{\alpha}}+(-1)^{(\alpha,w\beta)+(\gamma,w\alpha+w\beta)}\langle\alpha,\beta\rangle\langle\gamma,\alpha+\beta\rangle X_{\widetilde{\gamma}\widetilde{\alpha}\widetilde{\beta}} \\
&= -\widetilde{\beta}\widetilde{\gamma}X_{\widetilde{\alpha}}+\langle\alpha,\beta\rangle^{-1}X_{\widetilde{\gamma}\widetilde{\alpha}\widetilde{\beta}}.
\end{aligned}$$

Note that

$$X_{\widetilde{\gamma}\widetilde{\alpha}\widetilde{\beta}}=\langle\alpha,\beta\rangle X_{\widetilde{\gamma}\widetilde{\beta}\widetilde{\alpha}}=\langle\alpha,\beta\rangle\widetilde{\gamma}\widetilde{\beta}X_{\widetilde{\alpha}},$$

where we are using the fact that $\widetilde{\beta}\widetilde{\gamma}\in\mu_3$. Thus (3.1) is zero in the case when $(\alpha,\beta)=-1$. The case when $(\alpha,\beta)=1$ is similar.

If $(\alpha,\beta)=-2$ then $\alpha=\gamma=-\beta$, so

$$\begin{aligned}
[x,[y,z]]+[y,[z,x]]+[z,[x,y]] &= -2\widetilde{\beta}\widetilde{\gamma}X_{\widetilde{\alpha}}+2\widetilde{\alpha}\widetilde{\beta}X_{\widetilde{\gamma}} \\
&= -2\widetilde{\beta}\widetilde{\gamma}X_{\widetilde{\alpha}}+2\widetilde{\alpha}\widetilde{\beta}\widetilde{\gamma}(\widetilde{\alpha})^{-1}X_{\widetilde{\alpha}}.
\end{aligned}$$

Since $\widetilde{\alpha}$ commutes with $\widetilde{\beta}$ and $\widetilde{\gamma}$ commutes with $(\widetilde{\alpha})^{-1}$, we see that this is zero. The case when $(\alpha,\beta)=2$ is similar.

Case 2: $\beta+\gamma\in\Phi$.

Since we are assuming that the first term in (3.1) is nonzero, we have that $\alpha+\beta+\gamma\in\Phi$, and so $(\beta,\gamma)=(\alpha,\beta+\gamma)=-1$. Thus $(\alpha,\beta)+(\alpha,\gamma)=-1$, and at least one of (α,β) or (α,γ) is less than 0. If (α,β) or (α,γ) is -2, then the proof reduces to that of Case 1.

Suppose $(\alpha,\beta)=-1$. Then

$$\begin{aligned}
[x,[y,z]]+[y,[z,x]]+[z,[x,y]] &= (-1)^{(\alpha,w\beta+w\gamma)+(\beta,w\alpha)}\langle\alpha,\beta+\gamma\rangle\langle\beta,\gamma\rangle X_{\widetilde{\alpha}\widetilde{\beta}\widetilde{\gamma}} \\
&\quad +(-1)^{(\alpha,w\beta)+(\gamma,w\alpha+w\beta)}\langle\alpha,\beta\rangle\langle\gamma,\alpha+\beta\rangle X_{\widetilde{\gamma}\widetilde{\alpha}\widetilde{\beta}} \\
&= (-1)^{(\alpha,w\beta)}\langle\alpha,\beta\rangle\left[(-1)^{(\alpha+\beta,w\gamma)}\langle\alpha+\beta,\gamma\rangle+(-1)^{(\gamma,w\alpha+w\beta)}\langle\gamma,\alpha+\beta\rangle^2\right]X_{\widetilde{\alpha}\widetilde{\beta}\widetilde{\gamma}},
\end{aligned}$$

which is zero by Lemma 3.3 since $\langle\alpha+\beta,\gamma\rangle=\langle\gamma,\alpha+\beta\rangle^2$. If $(\alpha,\gamma)=-1$, the proof is similar. □

Recall that $\Gamma = \mathrm{Aut}_R(R')$. The étale sheaves Λ and $\mathscr{H}$ become constant over R', and the group Γ acts on their sections over $\mathrm{Spec}\, R'$. This group therefore also acts on the sections over $\mathrm{Spec}\, R'$ of $\widetilde{\Lambda}$. We define a semi-linear action of Γ on $\mathfrak{h}_{R'}$ by giving it its canonical action on $\mathfrak{a}_{R'}$ and by defining

$$\sigma(X_{\widetilde{\alpha}}) = \begin{cases} X_{\sigma(\widetilde{\alpha})} & \text{if } \sigma(\zeta) = \zeta; \\ -X_{\sigma(\widetilde{\alpha})} & \text{if } \sigma(\zeta) = \zeta^{-1} \end{cases}$$

for all $\sigma \in \Gamma$.

Lemma 3.4. *The action of Γ on $\mathfrak{h}_{R'}$ just defined leaves the Lie bracket invariant.*

Proof. We check the relation

$$\sigma([X_{\widetilde{\alpha}}, X_{\widetilde{\beta}}]) = [\sigma(X_{\widetilde{\alpha}}), \sigma(X_{\widetilde{\beta}})] \tag{3.2}$$

If $\sigma(\zeta) = \zeta$, then (3.2) is clear. Suppose instead that $\sigma(\zeta) = \zeta^{-1}$. We split into cases. If $\alpha + \beta = 0$, the both sides of (3.2) are equal to $-(\widetilde{\alpha}\widetilde{\beta})^{-1}\sigma(\check{\alpha})$.

If $\alpha + \beta$ is a root, then the left-hand side of (3.2) equals $(-1)^{(\alpha, w\beta)+1}\langle \alpha, \beta \rangle^{-1} X_{\sigma(\widetilde{\alpha}\widetilde{\beta})}$, while the right-hand side equals $(-1)^{(\sigma(\alpha), w\sigma(\beta))}\langle \sigma(\alpha), \sigma(\beta) \rangle X_{\sigma(\widetilde{\alpha}\widetilde{\beta})}$. Since $\sigma^{-1} w \sigma = w^{-1}$ as elements of $\mathrm{Aut}(\Lambda)$, we have

$$(-1)^{(\sigma\alpha, w\sigma\beta)} = (-1)^{(w\alpha, \beta)} = (-1)^{(\alpha, w\beta)+1}$$

and

$$\langle \sigma\alpha, \sigma\beta \rangle = \zeta^{(\sigma\alpha, \sigma\beta) - (w\sigma\alpha, \sigma\beta)} = \zeta^{(\alpha, \beta) - (\alpha, w\beta)} = \langle \beta, \alpha \rangle,$$

and thus both sides of (3.2) are equal.

□

We let $\mathfrak{h} = \mathfrak{h}_{R'}^{\Gamma}$, $H = \mathrm{Aut}_R(\mathfrak{h})$. Our assumption that $N = 2 \times 3 \times 5 \times 7$ is a unit in R says exactly that the Killing form of $\mathfrak{h}$ is non-degenerate, and therefore (by the main theorem of [Vas16]) that H is a reductive group over R with geometric fibres of Dynkin type E_8. Moreover, we have $\mathrm{Lie}\, H = \mathfrak{h}$ and we can identify $Z_H(\mathfrak{a}) = A$.

To complete the description of the functor $\mathrm{Heis}_R \to \mathrm{GrLieT}_R$, it remains to describe the homomorphism $\theta : \mu_3 \to H$. We make μ_3 act on $\widetilde{\Lambda} = \Lambda \times_{\Lambda_\theta} \mathscr{H}$ by putting the trivial μ_3-action on $\mathscr{H}$. We define a map $\theta : \mu_3 \to \mathrm{Aut}(\mathfrak{h}_{R'})$ using the existing action on $\mathfrak{a}$, together with the formula

$$\theta(\zeta)(X_{\widetilde{\alpha}}) = X_{\theta(\zeta)(\widetilde{\alpha})}.$$

Lemma 3.5. *With the above definition, $\theta : \mu_3(R') \to \mathrm{Aut}(\mathfrak{h}_{R'})$ preserves the Lie bracket and is equivariant for the action of $\Gamma = \mathrm{Aut}_R(R')$.*

Proof. Recall that we have defined $w = \theta(\zeta)$. In order to prove the lemma, it suffices to show that

$$[w(x), w(y)] = w([x, y]) \tag{3.3}$$

for any generators x, y of $\mathfrak{h}_{R'}$. If $x, y \in \mathfrak{a}_{R'}$, then both sides of (3.3) are zero. If $x = \check{\alpha}$ and $y = X_{\widetilde{\beta}}$ for some $\alpha \in \Phi, \widetilde{\beta} \in \widetilde{\Lambda}$, then equality in (3.3) follows from the fact that $(w\alpha, w\beta) = (\alpha, \beta)$. Suppose $x = X_{\widetilde{\alpha}}$ and $y = X_{\widetilde{\beta}}$ for some $\widetilde{\alpha}, \widetilde{\beta} \in \widetilde{\Lambda}$. If $(\alpha, \beta) \geq 0$, then both sides of (3.3) are zero, and if $\alpha + \beta \in \Phi$, then equality in (3.3) follows from the fact that $\langle w\alpha, w\beta \rangle = \langle \alpha, \beta \rangle$. If $\alpha + \beta = 0$, then

$$\begin{aligned} [w(X_{\widetilde{\alpha}}), w(X_{\widetilde{\beta}})] &= -(w\widetilde{\alpha})(w\widetilde{\beta})w(\check{\alpha}) \\ &= -w(\widetilde{\alpha}\widetilde{\beta})w(\check{\alpha}) \\ &= -\widetilde{\alpha}\widetilde{\beta}w(\check{\alpha}), \end{aligned}$$

where we are using that $\widetilde{\alpha}\widetilde{\beta} \in \mu_3$. Thus we again have equality in (3.3). It is immediate from the definition that θ as defined above is equivariant for the action of Γ. □

We write again $\theta : \mu_3 \to \operatorname{Aut}(\mathfrak{h}) = H$ for the induced homomorphism. This completes the construction of the triple (H, θ, A). It is (up to canonical isomorphism) independent of the choice of primitive 3rd root of unity $\zeta \in \mu_3(R')$; indeed, this choice entered only in the definition of the Lie bracket via the formula $[X_{\widetilde{\alpha}}, X_{\widetilde{\beta}}] = (-1)^{(\alpha, \theta(\zeta)(\beta))} \langle \alpha, \beta \rangle X_{\widetilde{\alpha}\widetilde{\beta}}$ (when $\widetilde{\alpha}, \widetilde{\beta} \in \widetilde{\Phi}$ and $\alpha + \beta$ is a root). The other choice would give $[X_{\widetilde{\alpha}}, X_{\widetilde{\beta}}] = (-1)^{(\alpha, \theta(\zeta^{-1})(\beta))} \langle \alpha, \beta \rangle X_{\widetilde{\alpha}\widetilde{\beta}}$. If $\mathfrak{h}'_{R'}$ denotes the Lie algebra over R' defined using the other primitive 3rd root of unity ζ^{-1}, then the map $\mathfrak{h}_{R'} \to \mathfrak{h}'_{R'}$ which is the identity on the summand $\mathfrak{a}_{R'}$ and which sends $X_{\widetilde{\alpha}} \in \mathfrak{h}_{R'}$ to $-X_{\widetilde{\alpha}} \in \mathfrak{h}'_{R'}$ is an isomorphism which intertwines the two actions of $\operatorname{Aut}_R(R')$, and therefore defines an isomorphism between the Lie algebras over R corresponding to the two possible choices of root of unity.

This completes the definition of the functor $\mathrm{Heis}_R \to \mathrm{GrLieT}_R$, and therefore the proof of Theorem 3.1.

We observe that if $(\Lambda, \theta, \mathscr{H}) \in \mathrm{Heis}_R$, then there is a morphism $f_R : H^0(R, \Lambda_\theta) \to \operatorname{Aut}_{\mathrm{Heis}_R}(\Lambda, \theta, \mathscr{H})$ defined as follows: if $\lambda \in H^0(R, \Lambda_\theta)$, then $f_R(\lambda)$ acts as the identity on Λ and as $\mu \mapsto \langle \lambda, \mu \rangle \mu$ on $\mathscr{H}$. Let $(H, \theta, A) \in \mathrm{GrLieT}_R$ be the tuple corresponding to $(\Lambda, \theta, \mathscr{H})$ under the construction of Theorem 3.1. Varying R and taking into the account the functorial nature of our construction, we obtain a morphism of group schemes over R:

$$\Lambda_\theta \to \operatorname{Aut}(H, \theta, A) = N_H(A)^\theta. \tag{3.4}$$

We can describe this explicitly:

Lemma 3.6. *Let notation be as in the above discussion. Then there is a canonical isomorphism $\Lambda_\theta \cong A^\theta$, under which the morphism (3.4) corresponds to the adjoint action of $A^\theta = Z_H(A)^\theta \subset \operatorname{Aut}(H, \theta, A) = N_H(A)^\theta$.*

Proof. By definition, we have $X^*(A) = \Lambda$, hence $X_*(A) \cong \Lambda^\vee = \operatorname{Hom}(\Lambda, \mathbb{Z})$. There is a canonical isomorphism $A^\theta \cong (\Lambda^\vee \otimes \mu_3)^\theta$.

There is an isomorphism $\Lambda_\theta \cong (\Lambda^\vee \otimes \mu_3)^\theta$, given by the formula $\lambda \mapsto (1 - \theta(\zeta))\check{\lambda} \otimes \zeta$ for $\lambda \in \Lambda$; this does not depend on the choice of ζ and also depends only on the image of λ in Λ_θ.

Composing the above two isomorphisms gives the desired isomorphism $\Lambda_\theta \cong A^\theta$. Now fix $\lambda \in \Lambda_\theta$, and let $R \to R'$ be a Galois finite étale cover over which Λ and $\mathscr{H}$ become constant.

We will give an explicit description of λ as an automorphism of $\mathfrak{h}_{R'} = \mathfrak{a}_{R'} \oplus \mathfrak{h}'$. By definition, it acts as the identity on $\mathfrak{a}_{R'}$ and sends the vector $X_{\widetilde{\alpha}}$ to $X_{\langle \lambda, \alpha \rangle \widetilde{\alpha}}$. In other words, it leaves invariant the α-root space and acts by the scalar $\langle \lambda, \alpha \rangle$ there.

On the other hand, the element $(1 - w)\check{\lambda}(\zeta)$ in A^θ also acts as the identity on A and leaves invariant each root space, acting on the α-root space by the scalar

$$\zeta^{((1-w)\lambda, \alpha)} = \langle \lambda, \alpha \rangle.$$

This completes the proof. □

3.3 Identifying $\mathfrak{h}(0)$

Theorem 3.1 associates to any triple $(\Lambda, \theta, \mathscr{H}) \in \mathrm{Heis}_R$ a triple $(H, \theta, A) \in \mathrm{GrLieT}_R$. In the proof of our next result, we show that if W is an irreducible representation of $\mathscr{H}$ on which the central μ_3 acts by its tautological (scalar) character, then we can identify $\mathfrak{h}(0)$ with $\mathfrak{sl}(W)$ and $\mathscr{H}$ with a certain subgroup of $\mathrm{SL}(W)$. This result will play an essential role in the construction of orbits in §4.3.

Theorem 3.7. *Let $(\Lambda, \theta, \mathscr{H}) \in \mathrm{Heis}_R$. Let W be a locally free R-module of rank 9, and suppose $\rho : \mathscr{H} \to \mathrm{Aut}_R(W)$ is a homomorphism such that the central μ_3 acts on W through its tautological character. Let (H, θ, A) denote the image of $(\Lambda, \theta, \mathscr{H})$ under the functor of Theorem 3.1 and let $G = H^\theta$. Then:*

1. *G is a semisimple reductive group. Let G^{sc} denote its simply connected cover.*
2. *There is a commutative diagram of R-groups with exact rows:*

$$\begin{tikzcd}
1 \arrow[r] & \mu_3 \arrow[r] & G^{sc} \arrow[r] & G \arrow[r] & 1 \\
1 \arrow[r] & \mu_3 \arrow[r] \arrow[u, "="'] & \mathscr{H} \arrow[r] \arrow[u] & \Lambda_\theta \arrow[r] \arrow[u] & 1,
\end{tikzcd}$$

where the map $\Lambda_\theta \to G$ is induced by a canonical isomorphism $\Lambda_\theta \cong A^\theta$.

To prove the theorem, we can again assume that $\operatorname{Spec} R$ is connected, and choose a Galois finite étale extension $R \to R'$ over which Λ and $\mathscr{H}$ become constant. The group G is reductive with geometric fibres of type SL_9/μ_3, so its simply connected cover $G^{\mathrm{sc}} \to G$ exists, and has a kernel which is a group of multiplicative type over R of order 3. Let $\mathfrak{g} = \operatorname{Lie} G$. Then $\mathfrak{g} = \mathfrak{h}^\theta$ (see e.g. [Con14, Lemma 2.2.4]).

The first step in the proof of Theorem 3.7 is to define an action of the Lie algebra $\mathfrak{g}$ on W; equivalently, to define a Γ-equivariant map $\mathfrak{g}_{R'} \to \mathrm{End}_{R'}(W_{R'})$.

If $\widetilde{\alpha} \in \widetilde{\Phi}$, define $Z_{\widetilde{\alpha}} = X_{\widetilde{\alpha}} + X_{\theta(\zeta)(\widetilde{\alpha})} + X_{\theta(\zeta^2)(\widetilde{\alpha})} \in \mathfrak{g}_{R'}$. These elements span $\mathfrak{g}_{R'}$.

Let $\pi : \widetilde{\Lambda} \to \mathscr{H}$ denote the canonical projection. We define a map $\rho' : \mathfrak{g}_{R'} \to \mathrm{End}_{R'}(W_{R'})$ by the formula

$$\rho'(Z_{\widetilde{\alpha}}) = \zeta(1 - \zeta^{-1})^{-1}\rho(\pi(\widetilde{\alpha})).$$

Proposition 3.8. *With the above definition, ρ' is a well-defined Lie algebra homomorphism that commutes with the action of $\Gamma = \mathrm{Aut}_R(R')$.*

Proof. We see that ρ' is well defined exactly because $\rho(\zeta) = \zeta \cdot 1_W$. The key point is to check that the Lie bracket is preserved, or in other words that the relation

$$\rho'([Z_{\widetilde{\alpha}}, Z_{\widetilde{\beta}}]) = [\rho'(Z_{\widetilde{\alpha}}), \rho'(Z_{\widetilde{\beta}})] \tag{3.5}$$

holds for all $\widetilde{\alpha}, \widetilde{\beta} \in \widetilde{\Phi}$. We give a case-by-case-proof depending on the value of (α, β). Before beginning, we note again the useful fact that if $\alpha \in \Phi$, then $\alpha + w(\alpha) + w^2(\alpha) = 0$. In particular, $\alpha + w(\alpha)$ and $\alpha + w^2(\alpha)$ are roots.

Case 1. If $(\alpha, \beta) = \pm 2$, then $\alpha = \pm\beta$. If $\alpha = \beta$ then both sides of (3.5) vanish. If $\alpha = -\beta$, then the right-hand side vanishes because $\pi(\widetilde{\alpha})$ and $\pi(\widetilde{\beta})$ commute in $\mathscr{H}$. On the other hand, $[Z_{\widetilde{\alpha}}, Z_{\widetilde{\beta}}]$ equals

$$\begin{aligned}
&[X_{\widetilde{\alpha}}, X_{\widetilde{\beta}}] + [X_{w\widetilde{\alpha}}, X_{w\widetilde{\beta}}] + [X_{w^2\widetilde{\alpha}}, X_{w^2\widetilde{\beta}}] \\
&+[X_{\widetilde{\alpha}}, X_{w\widetilde{\beta}}] + [X_{w\widetilde{\alpha}}, X_{w^2\widetilde{\beta}}] + [X_{w^2\widetilde{\alpha}}, X_{\widetilde{\beta}}] \\
&+[X_{\widetilde{\alpha}}, X_{w^2\widetilde{\beta}}] + [X_{w\widetilde{\alpha}}, X_{\widetilde{\beta}}] + [X_{w^2\widetilde{\alpha}}, X_{w\widetilde{\beta}}].
\end{aligned} \tag{3.6}$$

The first line of (3.6) is zero because it is an element of $\mathfrak{g}_{R'} \cap \mathfrak{a}_{R'} = 0$. The second line vanishes because $\alpha - w\alpha$ is not a root. The third line vanishes because $\alpha - w^2\alpha$ is not a root. Therefore both sides of (3.5) are zero in this case.

We note that if any of $(\alpha, w\beta) = \pm 2, (\alpha, w^2\beta) = \pm 2, (w\alpha, \beta) = \pm 2$, or $(w^2\alpha, \beta) = \pm 2$, then because $Z_{\widetilde{\alpha}} = Z_{w\widetilde{\alpha}} = Z_{w^2\widetilde{\alpha}}$ and similarly for $Z_{\widetilde{\beta}}$, we still have that both sides of (3.5) are zero, so for the rest of the proof we can, and do, assume that this is not the case.

Case 2. If $(\alpha, \beta) = -1$, then $\alpha + \beta$ is a root. Note that the equation $(\alpha, \beta) + (w\alpha, \beta) + (w^2\alpha, \beta) = 0$ implies that $(w\alpha, \beta)$ and $(w^2\alpha, \beta)$ are nonnegative, and similarly for $(\alpha, w\beta)$ and $(\alpha, w^2\beta)$. This implies that $[Z_{\widetilde{\alpha}}, Z_{\widetilde{\beta}}] = (-1)^{(\alpha, w\beta)}\langle\alpha, \beta\rangle Z_{\widetilde{\alpha}\widetilde{\beta}}$ and that $\langle\alpha, \beta\rangle = \zeta^{-(w\alpha,\beta)-1} \neq 1$. Thus

$$\begin{aligned}
[\rho'(Z_{\widetilde{\alpha}}), \rho'(Z_{\widetilde{\beta}})] &= \zeta^{-1}(1-\zeta^{-1})^{-2}\left[\rho(\pi(\widetilde{\alpha})), \rho(\pi(\widetilde{\beta}))\right] \\
&= \zeta^{-1}(1-\zeta^{-1})^{-2}(1-\rho(\pi(\widetilde{\beta}\widetilde{\alpha}\widetilde{\beta}^{-1}\widetilde{\alpha}^{-1})))\rho(\pi(\widetilde{\alpha}\widetilde{\beta})) \\
&= \zeta^{-1}(1-\zeta^{-1})^{-2}(1-\langle\beta, \alpha\rangle)\rho(\pi(\widetilde{\alpha}\widetilde{\beta})).
\end{aligned}$$

If $\langle\alpha, \beta\rangle = \zeta$, then $(w\alpha, \beta) = 1$ and $(\alpha, w\beta) = 0$, so

$$\zeta^{-1}(1-\zeta^{-1})^{-2}(1-\langle\beta, \alpha\rangle)\rho(\pi(\widetilde{\alpha}\widetilde{\beta})) = \zeta^{-1}(1-\zeta^{-1})^{-1} = \rho'(\left[Z_{\widetilde{\alpha}}, Z_{\widetilde{\beta}}\right]).$$

If $\langle\alpha, \beta\rangle = \zeta^{-1}$, then $(w\alpha, \beta) = 0$, $(\alpha, w\beta) = 1$, and we again have equality in (3.5).

Case 3. Suppose $(\alpha, \beta) \in \{0, 1\}$. If $(\alpha, \beta) = (w\alpha, \beta) = (w^2\alpha, \beta) = 0$, then both sides of (3.5) are 0. Otherwise the equation $(\alpha, \beta) + (w\alpha, \beta) + (w^2\alpha, \beta) = 0$ implies that either $(w\alpha, \beta) = -1$ or $(w^2\alpha, \beta) = -1$, and thus we may reduce to Case 2. This completes the proof that ρ' is a Lie algebra homomorphism.

It remains to check that ρ' is equivariant for the action of Γ. We just need to note the formulae

$$\sigma(Z_{\widetilde{\alpha}}) = \begin{cases} Z_{\sigma(\widetilde{\alpha})} & \sigma(\zeta) = \zeta; \\ -Z_{\sigma(\widetilde{\alpha})} & \sigma(\zeta) = \zeta^{-1} \end{cases}$$

and $-\zeta/(1-\zeta^{-1}) = 1/(\zeta(1-\zeta))$. □

The induced map $\mathfrak{g} \to \mathfrak{sl}(W)$ is an isomorphism, inducing an isomorphism $G^{\mathrm{ad}} \to \mathrm{PGL}(W)$ (by [Vas16] once again), hence a unique isomorphism $G^{\mathrm{sc}} \to \mathrm{SL}(W)$ which is compatible with the given map $\mathfrak{g} \to \mathfrak{sl}(W)$ ([Con14, Exercise 6.5.2]). Let $\mathscr{H}'$ denote the pre-image of $A^\theta \cong \Lambda_\theta$ in G^{sc}. Identifying the centre of G^{sc} with μ_3 via its action on W, we find that $\mathscr{H}'$ fits into a diagram

$$\begin{tikzcd}
1 \arrow[r] & \mu_3 \arrow[r] & G^{\mathrm{sc}} \arrow[r] & G \arrow[r] & 1 \\
1 \arrow[r] & \mu_3 \arrow[r] \arrow[u, "="'] & \mathscr{H}' \arrow[r] \arrow[u] & \Lambda_\theta \arrow[r] \arrow[u] & 1.
\end{tikzcd}$$

To complete the proof of Theorem 3.7, we must show that there is an isomorphism $\mathscr{H} \cong \mathscr{H}'$ of central extensions of Λ_θ by μ_3. We will show that in fact the images of $\mathscr{H}$ and $\mathscr{H}'$ in $\mathrm{SL}(W)$ coincide. This can be checked over the extension $R \to R'$.

Let $p : G^{\mathrm{sc}} \to G^{\mathrm{ad}}$ denote the projection to the adjoint group. We can characterize $\mathscr{H}$ as

$$\mathscr{H} = \{g \in G^{\mathrm{sc}} \mid p(g) \in p(\rho(\mathscr{H})), g^3 = 1\}.$$

Similarly, we can characterize $\mathscr{H}'$ as

$$\mathscr{H}' = \{g \in G^{\mathrm{sc}} \mid p(g) \in p(\Lambda_\theta), g^3 = 1\}.$$

To prove the theorem, it is therefore enough to show that the two homomorphisms $\Lambda_\theta \to \mathrm{PGL}(W)$, one derived from $\mathrm{Ad} \circ \rho$, the other derived from $\mathrm{Ad}\,|_{\mathscr{H}'}$, are the same. Since $\mathfrak{g}_{R'}$ is spanned by the elements $Z_{\widetilde{\beta}}$, and the non-trivial elements of Λ_θ are all of the form $\alpha \bmod (\theta - 1)$, for some $\alpha \in \Phi$, it is enough to show that the two possible actions of α on $Z_{\widetilde{\beta}}$ are the same for all $\alpha \in \Phi$, $\widetilde{\beta} \in \widetilde{\Phi}$.

For the first action, we see that, by definition, $\rho'(Z_{\widetilde{\beta}}) \in \mathfrak{g}_{R'} = \mathfrak{sl}(W_{R'}) \subset \mathrm{End}_{R'}(W_{R'})$ is a scalar multiple of $\rho(\pi(\widetilde{\beta}))$. Therefore we have

$$\mathrm{Ad}(\rho(\pi(\widetilde{\alpha})))(Z_{\widetilde{\beta}}) = \rho(\pi(\widetilde{\alpha}\widetilde{\beta}\widetilde{\alpha}^{-1}\widetilde{\beta}^{-1}))Z_{\widetilde{\beta}} = \langle \alpha, \beta \rangle Z_{\widetilde{\beta}}. \tag{3.7}$$

For the second action, we use the fact that $Z_{\widetilde{\beta}} = X_{\widetilde{\beta}} + X_{\theta(\zeta)(\widetilde{\beta})} + X_{\theta(\zeta^2)(\widetilde{\beta})}$. The isomorphism $\Lambda_\theta \to A^\theta$, defined by Lemma 3.6, sends a root α to the element $(1-w)\check{\alpha}(\zeta)$. We calculate the corresponding action on $Z_{\widetilde{\beta}}$ as

$$\mathrm{Ad}((1-w)\check{\alpha}(\zeta))(Z_{\widetilde{\beta}}) = \zeta^{\langle (1-w)\check{\alpha}, \beta \rangle} Z_{\widetilde{\beta}} = \langle \alpha, \beta \rangle Z_{\widetilde{\beta}}. \tag{3.8}$$

The equality of the expressions (3.7) and (3.8) concludes the proof of Theorem 3.7.

4 A stable grading of E_8

In the previous section we constructed a functor from Heisenberg groups to $\mathbb{Z}/3\mathbb{Z}$-graded Lie algebras. In order to count points, we need to have a 'reference' algebra in which one can do explicit calculations. In this section we introduce such an algebra using a principal grading as defined in [RLYG12] and give rigidifications of orbits and invariant polynomials using two special transverse slices to nilpotent orbits. The main results of this section, in §4.3, combine this work with the work done in §3 to define the map η_f described in the introduction (in other words, to construct orbits from points of Jacobians).

4.1 Definition of the grading

Let $\underline{H}$ be a split reductive group of type E_8 over $\mathbb{Z}$. Let $\underline{T} \subset \underline{H}$ be a split maximal torus, and let $\Phi_H \subset X^*(\underline{T})$ be the corresponding set of roots. Let $S_H \subset \Phi_H$ be a fixed choice of root basis. Let Φ_H^+ be the corresponding set of positive roots. We suppose that $\underline{H}$ comes with a pinning $\{X_\alpha\}_{\alpha \in S_H}$.

Let $\check{\rho} \in X_*(\underline{T})$ be the sum of the fundamental coweights with respect to S_H, and let $\theta = \check{\rho}|_{\mu_3} : \mu_3 \to \underline{H}$. Let $\underline{\mathfrak{h}} = \mathrm{Lie}(\underline{H})$. Then θ defines an action of μ_3 on $\underline{\mathfrak{h}}$ and thus determines a $\mathbb{Z}/3\mathbb{Z}$-grading

$$\underline{\mathfrak{h}} = \underline{\mathfrak{h}}(0) \oplus \underline{\mathfrak{h}}(1) \oplus \underline{\mathfrak{h}}(2). \tag{4.1}$$

We let $\underline{G} = \underline{H}^\theta$, the centralizer of θ in $\underline{H}$. We write $\underline{V} = \underline{\mathfrak{h}}(1)$; it is a representation of $\underline{G}$, free over $\mathbb{Z}$ of rank 84.

Proposition 4.1. *The group $\underline{G}$ is a split reductive group isomorphic to SL_9/μ_3. The subgroup $\underline{T} \subset \underline{G}$ is a split maximal torus. Over $\mathbb{Z}[1/3]$, θ is a stable $\mathbb{Z}/3\mathbb{Z}$-grading of $\underline{H}$, in the sense of §2.*

Proof. It follows from the discussion in [Con14, Remark 3.1.5] that $\underline{G}$ is smooth over $\mathbb{Z}$, and moreover that the connected component $\underline{G}^0$ (which agrees in each fibre $\underline{G}_s$ with the connected component of $\underline{G}_s$) is reductive. Moreover, $\underline{T} \subset \underline{G}^0$ is a split maximal torus. It remains therefore to check that $\underline{G} = \underline{G}^0$ and that its root datum is that of SL_9/μ_3. The quotient $\underline{G}/\underline{G}^0$ is étale over $\mathbb{Z}$, so both of these last points can be checked at the generic point, in which case they follow from the general theory over $\mathbb{C}$ (see e.g. [Ree10]). The final statement can be checked in geometric fibres, in which case it is [RLYG12, Corollary 5.7]. □

Let $\Phi_G = \Phi(\underline{G}, \underline{T})$. There exists a unique choice S_G of root basis for $\underline{G}$ such that $\Phi_G^+ = \Phi_G \cap \Phi_H^+$.

We write H for the $\mathbb{Q}$-fibre of $\underline{H}$, and similarly for T, G, and V. In the coming sections we will describe the invariant theory of the pair (G, V) and its relation to 3-descent on odd genus-2 curves. We will re-introduce integral structures into our discussion in §4.5 below.

We let $B = V /\!\!/ G = \mathbb{Q}[V]^G$, and write $\pi : V \to B$ for the quotient map. For a detailed study of the properties of the pair (G, V), and its analogue over fields of sufficiently large positive characteristic, see [Lev09]. We invite the reader to become familiar at least with the results in the introduction to that paper before proceeding; in particular, we will make frequent use of the existence of Jordan decomposition of elements in V and of the fact that, if k is algebraically closed, then two semisimple elements of $V(k)$ are $G(k)$-conjugate if and only if they have the same image in $B(k)$.

We write $B^{\text{rs}} \subset B$ for the open subscheme where the restriction of the discriminant of $\mathfrak{h}$ to V (which is certainly G-invariant) is non-zero. The preimage $\pi^{-1}(B^{\text{rs}})$ is the open subscheme $V^{\text{rs}} \subset V$ of regular semisimple elements. We also have the open subscheme $V^{\text{reg}} \subset V$ of regular elements, i.e. those with finite stabilizers in G. We will generally use the superscripts $(?)^{\text{rs}}$ and $(?)^{\text{reg}}$ to denote intersection with these open subschemes of regular semisimple and regular elements, respectively.

4.2 Kostant section

Let $E = \sum_{\alpha \in S_H} X_\alpha \in \mathfrak{h}$. Then E is a regular nilpotent element. Let (E, X, F) be the unique normal $\mathfrak{sl}_2$-triple containing it. By definition, this means that (E, X, F) is an $\mathfrak{sl}_2$-triple with $E \in \mathfrak{h}(1)$, $X \in \mathfrak{h}(0)$, and $F \in \mathfrak{h}(-1)$ (cf. [dG11, §3.1]; the uniqueness follows from the results stated there, together with the fact that $Z_G(E)$ is trivial). In fact, (E, X, F) is the $\mathfrak{sl}_2$-triple associated to the pinning of H (cf. [Gro97, §2]).

We define an affine linear subspace $\kappa = (E + \mathfrak{z}_{\mathfrak{h}}(F)) \cap V \subset V$.

Proposition 4.2. *The restriction of the map $\pi : V \to B$ to κ induces an isomorphism $\pi|_\kappa : \kappa \to B$. Moreover, κ is contained in the open subscheme $V^{reg} \subset V$ of regular elements.*

Proof. See [Pan05, Theorem 3.5]. □

We write $\sigma : B \to V$ for the inverse $\sigma = \pi|_\kappa^{-1}$, and call it the Kostant section. We define an action of $\mathbb{G}_m$ on κ by the formula $t \cdot x = t \operatorname{Ad}(\check{\rho}(t^{-1}))(x)$. This is a contracting action with E as its unique fixed point, and the morphism $\pi|_\kappa$ is $\mathbb{G}_m$-equivariant (when $\mathbb{G}_m$ acts on $B = V /\!\!/ G$ in the natural way, compatibly with its action on V by scalar multiplication). Hence σ is also $\mathbb{G}_m$-equivariant.

If $k/\mathbb{Q}$ is a field extension, and $f \in B^{\text{rs}}(k)$, then we can use the Kostant section to organise the set $G(k) \backslash V_f(k)$, where $V_f = \pi^{-1}(f)$. Indeed, we write $\mu_f : G \to V_f$ for the action map $g \mapsto g \cdot \sigma(f)$. Then μ_f is a torsor for the group $Z_G(\sigma(f))$ and determines a bijection

$$G(k) \backslash V_f(k) \cong \ker(H^1(k, Z_G(\sigma(f))) \to H^1(k, G)).$$

The group scheme $Z_G(\sigma(f))$ can be described explicitly as follows: $A_f := Z_H(\sigma(f))$ is a maximal torus of H. The image of θ normalizes A_f, inducing a homomorphism $\mu_3 \to N_H(A_f)/A_f = W(H, A_f)$ that is an elliptic μ_3-action on $X^*(A_f)$ in the sense of §2. Thus $Z_G(\sigma(f)) = A_f^\theta$ is a finite étale k-group of order 3^4.

More generally, the centralizer $A := Z_H(\sigma|_{B^{\text{rs}}})$ is a maximal torus in $H_{B^{\text{rs}}}$. We define $\Lambda = X^*(A)$ and $\Lambda^\vee = \operatorname{Hom}(\Lambda, \mathbb{Z})$. We define a pairing $(\cdot, \cdot) : \Lambda \times \Lambda \to \mathbb{Z}$ by the formula $(\lambda, \mu) = \check{\lambda}(\mu)$. Then Λ is an étale sheaf of E_8 root lattices on B^{rs}. The grading θ determines a homomorphism $\mu_3 \to \operatorname{Aut}(\Lambda)$ that we also denote by θ, and which is an elliptic μ_3-action on Λ. The stabilizer scheme $Z_G(\sigma|_{B^{\text{rs}}})$ is finite étale over B^{rs}, and can be identified with Λ_θ (cf. Lemma 3.6). Moreover, Λ_θ admits a symplectic, non-degenerate pairing $\langle\cdot,\cdot\rangle : \Lambda_\theta \times \Lambda_\theta \to \mu_3$ (Lemma 2.2).

Proposition 4.3. *We can choose polynomials $c_{12}, c_{16}, c_{24}, c_{30} \in \mathbb{Q}[V]^G$ with the following properties:*

1. *Each polynomial c_i is homogeneous of degree i, and $\mathbb{Q}[V]^G$ is isomorphic to the ring $\mathbb{Q}[c_{12}, c_{16}, c_{24}, c_{30}]$. Consequently, there is an isomorphism $B \cong \mathbb{A}^4_{\mathbb{Q}}$. If $\Delta_0 \in \mathbb{Q}[V]^G$ denotes the discriminant of the polynomial $f(x) = x^5 + c_{12}x^3 + c_{18}x^2 + c_{24}x + c_{30}$, then Δ_0^2 is (up to scalar) equal to the restriction to V of the usual Lie algebra discriminant of $\mathfrak{h}$.*
2. *Let $\mathscr{C}^0 \to B$ be the family of affine curves given by the equation*
$$\mathscr{C}^0 : y^2 = x^5 + c_{12}x^3 + c_{18}x^2 + c_{24}x + c_{30}, \tag{4.2}$$
and let $\mathscr{C} \to B$ be its completion inside weighted projective space $\mathbb{P}_B(1,1,3)$, projective over B. Let $\mathscr{J} \to B^{rs}$ be the Jacobian of its smooth part. Then there is an isomorphism $\Lambda_\theta \cong \mathscr{J}[3]$ of étale sheaves which sends the pairing $\langle\cdot,\cdot\rangle$ on Λ_θ to the Weil pairing on $\mathscr{J}[3]$.

The proof of this proposition will be given in §4.4.

Let $\mathscr{P} : B \to \mathscr{C}$ denote the section at infinity (which is a Weierstrass point in each smooth fibre of $\mathscr{C}$). The choice of $\mathscr{P}$ determines a symmetric line bundle $\mathscr{M} = \mathcal{O}_{\mathscr{J}}(\mathscr{C} - \mathscr{P})$ on $\mathscr{J}$. We write $\mathscr{L} = \mathscr{M}^{\otimes 3}$, and define $\mathscr{G}$ to be the 3-torsion subgroup of the Mumford theta group $\mathscr{G}(\mathscr{L})$. Thus $\mathscr{G}$ is a central extension
$$1 \to \mu_3 \to \mathscr{G} \to \mathscr{J}[3] \to 1$$
of étale group schemes over B^{rs}, and $(\Lambda, \theta, \mathscr{G})$ is an object of the category $\mathrm{Heis}_{B^{\mathrm{rs}}}$ defined in §3. We will soon show (Proposition 4.6) that the image of $(\Lambda, \theta, \mathscr{G})$ under the functor defined in Theorem 3.1 is isomorphic in the groupoid $\mathrm{GrLieT}_{B^{\mathrm{rs}}}$ to the triple $(H_{B^{\mathrm{rs}}}, \theta_{B^{\mathrm{rs}}}, A)$.

4.3 Twisting

We can now explain our construction of orbits. Let R be a $\mathbb{Q}$-algebra. We recall that in §3 we have defined groupoids Heis_R and GrLieT_R, and a functor $\mathrm{Heis}_R \to \mathrm{GrLieT}_R$. We now define some related groupoids.

We define GrLie_R to be the groupoid of pairs (H', θ'), where H' is a reductive group over R of type E_8 and $\theta' : \mu_3 \to H'$ is a stable $\mathbb{Z}/3\mathbb{Z}$-grading. Morphisms $(H', \theta') \to (H'', \theta'')$ are given by isomorphisms $H' \to H''$ intertwining θ' and θ''.

Lemma 4.4. *The following sets are in canonical bijection:*

1. *The set of isomorphism classes of objects in* GrLie_R.
2. *The set $H^1(R, G)$.*

Proof. Note that GrLie_R always contains the object (H_R, θ_R). We have proved (Lemma 2.3) that any two objects of GrLie_R are isomorphic étale locally on $\operatorname{Spec} R$. Since $\mathrm{Aut}(H, \theta) = G$, the result follows by descent. □

We define GrLieE_R to be the groupoid of tuples (H', θ', γ'), where $(H', \theta') \in \mathrm{GrLie}_R$ and $\gamma' \in \mathfrak{h}'(1)$. Morphisms $(H', \theta', \gamma') \to (H'', \theta'', \gamma'')$ are given by isomorphisms $H' \to H''$ intertwining θ' and θ'' and sending γ' to γ''. If $(H', \theta', \gamma') \in \mathrm{GrLieE}_R$, then we define an element $\pi(\gamma') \in B(R)$ as follows: after passage to a faithfully flat extension $R \to R'$, we can find an isomorphism $\alpha : (H'_{R'}, \theta'_{R'}) \cong (H_{R'}, \theta_{R'})$, and $\pi(\alpha(\gamma')) \in B(R')$ in fact lies in $B(R)$ and is independent of the choice of α. Thus there is a functor $\pi : \mathrm{GrLieE}_R \to B(R)$, compatible with arbitrary base change on R. (We view the set $B(R)$ as a discrete category, i.e. as a category with no non-identity morphisms.)

There is an obvious functor $V(R) \to \mathrm{GrLieE}_R$ (where $V(R)$ is viewed as a discrete category) given by $\gamma \mapsto (H_R, \theta_R, \gamma)$. The composite $V(R) \to \mathrm{GrLieE}_R \to B(R)$ coincides with the map $\pi : V(R) \to B(R)$ defined previously.

If $f \in B(R)$, then we define $\mathrm{GrLieE}_{R,f}$ to be the full subcategory of GrLieE_R consisting of tuples (H', θ', γ') where $\pi(\gamma') = f$.

Lemma 4.5. *Let R be a $\mathbb{Q}$-algebra, and let $f \in B^{rs}(R)$. Then any two objects of $\mathrm{GrLieE}_{R,f}$ are isomorphic étale locally on $\operatorname{Spec} R$. Consequently, the following sets are in canonical bijection:*

1. *The set of $G(R)$-orbits in $V_f(R)$.*
2. *The set $\ker(H^1(R, Z_G(\sigma(f))) \to H^1(R, G))$.*
3. *The set of isomorphism classes of objects $(H', \theta', \gamma') \in \mathrm{GrLieE}_{R,f}$ such that $(H', \theta') \cong (H_R, \theta_R)$ in GrLie_R.*

Proof. The group scheme $Z_G(\sigma(f))$ is a finite étale R-scheme, and the action map $G \to V_f$ of $\sigma(f)$ is a $Z_G(\sigma(f))$-torsor. The existence of the bijection between the first and second sets is therefore a consequence of e.g. [Con14, Exercise 2.4.11].

The category $\mathrm{GrLieE}_{R,f}$ contains the triple $(H_R, \theta_R, \sigma(f))$. Its automorphisms may be identified with the sections over R of $Z_G(\sigma(f))$. Moreover, any two objects of $\mathrm{GrLieE}_{R,f}$ are isomorphic étale locally on $\operatorname{Spec} R$. This implies the existence of the bijection between the second and third sets. □

If $f \in B^{\mathrm{rs}}(R)$, then we define $\mathrm{Heis}_{R,f}$ to be the subcategory of Heis_R consisting of triples $(f^*\Lambda, \theta, \mathscr{H})$. Morphisms $\mathscr{H} \to \mathscr{H}'$ in $\mathrm{Heis}_{R,f}$ are morphisms $(f^*\Lambda, \theta, \mathscr{H}) \to (f^*\Lambda, \theta, \mathscr{H}')$ in Heis_R which act as the identity on $f^*\Lambda$. (Recall that $\Lambda = X^*(A)$ is an étale sheaf of E_8 root lattices on B^{rs}, so $f^*\Lambda$ is an étale sheaf of E_8 root lattices on $\operatorname{Spec} R$.)

Let $f_\tau \in B^{\mathrm{rs}}(B^{\mathrm{rs}})$ be the tautological section. According to Proposition 4.3, $(\Lambda, \theta, \mathscr{G})$ defines an element of the groupoid $\mathrm{Heis}_{B^{\mathrm{rs}}, f_\tau}$, hence a tuple $(H_\tau, \theta_\tau, A_\tau) \in \mathrm{GrLieT}_{B^{\mathrm{rs}}}$ (and in fact $A_\tau = A$). The Lie algebra $\mathfrak{a}_\tau$ has a tautological section γ_τ (which is in fact none other than σ). Thus $(H_\tau, \theta_\tau, \gamma_\tau) \in \mathrm{GrLieE}_{B^{\mathrm{rs}}, f_\tau}$.

Proposition 4.6. *The objects $(H_\tau, \theta_\tau, \gamma_\tau)$ and $(H_{B^{rs}}, \theta_{B^{rs}}, \sigma(f_\tau))$ of $\mathrm{GrLieE}_{B^{rs}, f_\tau}$ are isomorphic.*

Proof. The proof relies upon the fact that for each triple, the associated $\mathbb{Z}/3\mathbb{Z}$-grading can be naturally extended to a $\mathbb{Z}/6\mathbb{Z}$-grading. A $\mathbb{Z}/6\mathbb{Z}$-grading of $\mathfrak{h}_{B^{\mathrm{rs}}}$ extending the grading of $(H_{B^{\mathrm{rs}}}, \theta_{B^{\mathrm{rs}}}, \sigma(f_\tau))$ is given by $\check{\rho}|_{\mu_6}$. Let $V' \subset \mathfrak{h}_{B^{\mathrm{rs}}}$ denote the 1-part of this $\mathbb{Z}/6\mathbb{Z}$-grading, and note that $\sigma(f_\tau) \in V'(B^{\mathrm{rs}})$.

To define a $\mathbb{Z}/6\mathbb{Z}$-grading of $\mathfrak{h}_\tau$ extending the grading of $(H_\tau, \theta_\tau, \gamma_\tau)$, observe that $\mathscr{M}$ is a symmetric line bundle. A choice of isomorphism $\mathscr{M} \cong [-1]^*\mathscr{M}$ determines an automorphism $(\omega, \alpha) \mapsto (-\omega, [-1]^*\alpha)$ of $\mathscr{G}$ which acts as the identity on the central μ_3 and as -1 on the quotient $\mathscr{J}[3]$. Since this automorphism is compatible with the action of -1 on Λ, Theorem 3.1 implies the existence of an involution $\theta' : H_\tau \to H_\tau$ that commutes with θ_τ, that normalizes the torus $Z_{H_\tau}(\gamma_\tau)$, and that acts -1 on the character group of this torus. Therefore $\theta' \cdot \theta_\tau$ defines a $\mathbb{Z}/6\mathbb{Z}$-grading of $\mathfrak{h}_\tau$ such that, if $V'_\tau \subset \mathfrak{h}_\tau$ is the 1-part of the grading, then $\gamma_\tau \in V'_\tau$.

To complete the proof, consider the B^{rs}-scheme $\mathscr{T}$ of isomorphisms $H \to H_\tau$ intertwining $\check{\rho}|_{\mu_6}$ and $\theta' \cdot \theta_\tau$ and sending $\sigma(f_\tau)$ to γ_τ. Then $\mathscr{T}$ is an étale B^{rs}-scheme, which is in fact a torsor for $Z_H(\sigma(f_\tau))^{\check{\rho}|_{\mu_6}}$ (the argument is the same as in the proof of Lemma 2.3). Since $Z_H(\sigma(f_\tau))^{\check{\rho}|_{\mu_6}} \to B^{\mathrm{rs}}$ is the trivial group scheme, we have $\mathscr{T} = B^{\mathrm{rs}}$ and it follows that there is a unique isomorphism $(H_\tau, \theta_\tau, \gamma_\tau) \cong (H_{B^{\mathrm{rs}}}, \theta_{B^{\mathrm{rs}}}, \sigma(f_\tau))$ in $\mathrm{GrLieE}_{B^{\mathrm{rs}}, f_\tau}$ that is compatible with the given $\mathbb{Z}/6\mathbb{Z}$-gradings. □

Theorem 4.7. *Let $f \in B^{rs}(R)$. Then there is an equivalence of categories $\mathrm{Heis}_{R,f} \to \mathrm{GrLieE}_{R,f}$, compatible with base change on R.*

Proof. Let $(f^*\Lambda, \theta, \mathscr{H}) \in \mathrm{Heis}_{R,f}$, and let $(H', \theta', A') \in \mathrm{GrLieT}_R$ be its image under the functor of Theorem 3.1. Since $A' = f^*A_\tau$, we have the section $\gamma' = f^*(\gamma_\tau)$. The functor $\mathrm{Heis}_{R,f} \to \mathrm{GrLieE}_{R,f}$ is defined by sending $(f^*\Lambda, \theta, \mathscr{H})$ to the triple (H', θ', γ').

It is fully faithful, by Lemma 3.6. The category $\mathrm{Heis}_{R,f}$ contains the object $f^*(\Lambda, \theta, \mathscr{G})$, which corresponds to the object $(H_R, \theta_R, f^*(\gamma_\tau))$, by Proposition 4.6. The objects of both categories are therefore classified by the group $H^1(R, \mathscr{J}_f[3]) = H^1(R, Z_G(\sigma(f)))$. This shows that our functor is essentially surjective, and completes the proof of the lemma. □

Corollary 4.8. *Let R be a $\mathbb{Q}$-algebra over which every locally free module of finite rank is free. Let $f \in B^{rs}(R)$. Then there is a canonical injection $\eta_f : \mathscr{J}_f(R)/3\mathscr{J}_f(R) \to G(R)\backslash V_f(R)$.*

Proof. The group $\mathscr{G}$ acts on $H^0(\mathscr{J}_f, \mathscr{L})$, which is a locally free R-module of rank 9. By Proposition 4.6 and Theorem 3.7, there is a diagram of R-groups with exact rows:

$$\begin{tikzcd}
1 \arrow[r] & \mu_3 \arrow[r] & G_R^{\mathrm{sc}} \arrow[r] & G_R \arrow[r] & 1 \\
1 \arrow[r] & \mu_3 \arrow[r] \arrow[u, "="'] & \mathscr{G} \arrow[r] \arrow[u] & \mathscr{J}_f[3] \arrow[r] \arrow[u] & 1.
\end{tikzcd}$$

Let $P \in \mathscr{J}_f(R)$. Let $\mathscr{L}_P = t_P^*\mathscr{M} \otimes \mathscr{M} \otimes \mathscr{M}$, and let $\mathscr{G}_P$ denote the 3-torsion subgroup of the Mumford theta group $\mathscr{G}(\mathscr{L}_P)$. Then $\mathscr{G}_P \in \mathrm{Heis}_{R,f}$. Let $(H_P, \theta_P, \gamma_P) \in \mathrm{GrLieE}_{R,f}$ denote the tuple corresponding to $\mathscr{G}_P$ under the equivalence of Theorem 4.7. Then the class $\varphi \in H^1(R, \mathscr{J}_f[3])$ corresponding to $(H_P, \theta_P, \gamma_P)$ under the bijection of Lemma 4.5 is the Kummer class of the point P (as follows from Lemma 3.6).

To prove the corollary, we will show that this class lifts to $H^1(R, \mathscr{G})$. This will imply that the image of φ in $H^1(R, G)$ lies in the image of the map $H^1(R, G^{\mathrm{sc}}) \to H^1(R, G)$, which is trivial (by our assumption on R). To show that the class lifts, it will even suffice to show that it lifts to $H^1(R, \mathscr{G}(\mathscr{L}))$, where $\mathscr{G}(\mathscr{L})$ is the Mumford theta group of $\mathscr{L}$, sitting in the short exact sequence of R-groups

$$\begin{tikzcd}
1 \arrow[r] & \mathbb{G}_m \arrow[r] & \mathscr{G}(\mathscr{L}) \arrow[r] & \mathscr{J}_f[3] \arrow[r] & 1.
\end{tikzcd}$$

Indeed, the map $H^2(R, \mu_3) \to H^2(R, \mathbb{G}_m)$ is injective, again by our assumption on R. We define $\mathscr{T}_P$ to be the scheme of pairs (ω, α), where $\omega \in \mathscr{J}_f$ and $\alpha : \mathscr{L}_P \to t_\omega^*\mathscr{L}$ is an isomorphism. Note that forgetting ω leads to a surjective map $\mathscr{T}_P \to [3]^{-1}(P)$. Thus $\mathscr{T}_P$ is a torsor for $\mathscr{G}(\mathscr{L})$, defining a class in $H^1(R, \mathscr{G}(\mathscr{L}))$ that lifts the class $\varphi \in H^1(R, \mathscr{J}_f[3])$. This completes the proof of the corollary. □

Remark 4.9. We could prove a stronger version of Corollary 4.8 where we replace our assumption that every locally free module is free with the assumption that $H^1(R, G^{\mathrm{sc}})$ is trivial, by refining the torsor for $\mathscr{G}(\mathscr{L})$ constructed in the proof to a torsor for $\mathscr{G}$ using the canonical isomorphism $\mathscr{M}^{\otimes 9} \cong [3]^*\mathscr{M}$ afforded by the theorem of the cube. However, since we don't need this extra generality we have chosen not to include the details here.

We restate the corollary in the case that $R = k$ is a field extension of $\mathbb{Q}$.

Corollary 4.10. *Let $k/\mathbb{Q}$ be a field, and let $f \in B^{rs}(k)$. Then there is a canonical injection $\eta_{f,}$: $\mathscr{J}_f(k)/3\mathscr{J}_f(k) \to G(k)\backslash V_f(k)$.*

We also record for future use the fact that when $R = \mathbb{Q}$, we can extend the above construction of orbits from rational points to 3-Selmer elements:

Proposition 4.11. *Let $f \in B^{rs}(\mathbb{Q})$. Then the map $\eta_f : J_f(\mathbb{Q})/3J_f(\mathbb{Q}) \to G(\mathbb{Q})\backslash V_f(\mathbb{Q})$ naturally extends to a map $\eta_f : \mathrm{Sel}_3(J_f) \to G(\mathbb{Q})\backslash V_f(\mathbb{Q})$.*

Proof. Taking into account Lemma 4.5, we just need to show that the map $H^1(\mathbb{Q}, G) \to \prod_v H^1(\mathbb{Q}_v, G)$ is trivial kernel, where the product runs over the set of all places v of $\mathbb{Q}$. This is an exercise using class field theory. □

4.4 Proof of Proposition 4.3

We now prove Proposition 4.3. We will use a special transverse slice to the orbit of a subregular nilpotent element in V in order to form the bridge between the group H and the family of abelian surfaces $\mathscr{J}$.

We begin by fixing a subregular nilpotent element $e \in V$ (the existence of such an element can be read off from the tables in [VÈ78], which also show that there is a unique G-orbit of subregular nilpotents in V). We can complete e to a normal $\mathfrak{sl}_2$-triple (e, h, f) in $\mathfrak{h}$. We define $\mathscr{X}_0 = e + \mathfrak{z}_{\mathfrak{h}}(f)$, an affine linear subspace of $\mathfrak{h}$. We define a μ_3-action on $\mathscr{X}_0$ by the formula $\zeta \cdot x = \zeta^{-1} \operatorname{Ad}(\theta(\zeta))(x)$. We define a $\mathbb{G}_m$-action on $\mathscr{X}_0$ by the formula $t \cdot x = t^2 \operatorname{Ad}(\lambda(t^{-1}))(x)$, where $\lambda : \mathbb{G}_m \to G$ is the cocharacter with $d\lambda(1) = h$. These two actions commute, giving a $\mu_3 \times \mathbb{G}_m$-action on $\mathscr{X}_0$. Let $B_0 = \mathfrak{h}/\!\!/H$, and let $p_0 : \mathscr{X}_0 \to B_0$ denote the restriction of the adjoint quotient $\pi_0 : \mathfrak{h} \to \mathfrak{h}/\!\!/H$ to $\mathscr{X}_0$. This is equivariant for the action of $\mu_3 \times \mathbb{G}_m$ on source and target if $\mathbb{G}_m$ acts on $\mathfrak{h}/\!\!/H$ by the square of its usual action. We identify $X^*(\mu_3 \times \mathbb{G}_m) = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}$. If v is an eigenvector for an action of $\mu_3 \times \mathbb{G}_m$, then we define its weight to be the image in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}$ of the character by which $\mu_3 \times \mathbb{G}_m$ acts on v.

Proposition 4.12. *We can choose polynomials $c_2, c_8, c_{12}, c_{14}, c_{18}, c_{20}, c_{24}, c_{30} \in \mathbb{Q}[\mathfrak{h}]^H$ and $x, y, z \in \mathbb{Q}[\mathscr{X}_0]$ with the following properties:*

1. *Each polynomial c_i is homogeneous of degree i. The polynomials c_i are algebraically independent and generate $\mathbb{Q}[\mathfrak{h}]^H$. The restriction of c_i to $\mathscr{X}_0$ has weight $(-i, 2i)$. The elements x, y, z have weights $(0, 12)$, $(0, 30)$ and $(-1, 20)$, respectively.*
2. *The restriction of the 7 elements $c_2, c_8, c_{12}, c_{14}, c_{18}, c_{20}, c_{24}$ to $\mathscr{X}_0$, together with x, y, z, are algebraically independent and generate $\mathbb{Q}[\mathscr{X}_0]$. Moreover, the morphism $p_0 : \mathscr{X}_0 \to B_0$ is given by the formula*

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

Proof. View $\mathscr{X}_0$ as a vector space with origin e; then the action of $\mu_3 \times \mathbb{G}_m$ on $\mathscr{X}_0$ is linear. By direct calculation, the weights of $\mu_3 \times \mathbb{G}_m$ in $\mathscr{X}_0$ are as follows:

$$(1, 4), (0, 12), (1, 16), (-1, 20), (0, 24), (1, 28), (0, 30), (0, 36), (1, 40), (0, 48).$$

The weights of $\mu_3 \times \mathbb{G}_m$ on $\mathfrak{h}/\!\!/H$ are as follows:

$$(1, 4), (1, 16), (0, 24), (1, 28), (0, 36), (1, 40), (0, 48), (0, 60).$$

By comparison with the results of [Slo80, §8.7], we see that the differential $dp_{0,e}$ has rank 7, mapping the subspace where $\mathbb{G}_m$ acts with weights $4, 16, 24, 28, 36, 40, 48$ isomorphically into the Zariski tangent space $T_0(\mathfrak{h}/\!\!/H)$ and annihilating the subspace where $\mathbb{G}_m$ acts with weights $12, 20$, and 30.

Following through the argument of [Slo80, §8.7, Theorem] with this $\mu_3 \times \mathbb{G}_m$-action now shows that there is a $\mu_3 \times \mathbb{G}_m$-equivariant isomorphism $(\mathscr{X}_0 \to B_0) \to (\mathscr{X}_0' \to B_0')$, where $\mathscr{X}_0' \to B_0'$ is the semi-universal $\mu_3 \times \mathbb{G}_m$-deformation of the singularity $y^2 = z^3 + x^5$ given by the formula

$$y^2 = z^3 + x^5 + z(c_2 x^3 + c_8 x^2 + c_{14} x + c_{20}) + (c_{12} x^3 + c_{18} x^2 + c_{24} x + c_{30}),$$

where x, y, z have weights $(0, 12)$, $(0, 30)$ and $(-1, 20)$, respectively, and each c_i has weight $(-i, 2i)$. We fix our invariant polynomials $c_2, \dots, c_{30} \in \mathbb{Q}[\mathfrak{h}]^H$ to be the images under this isomorphism of the elements with the same names in the affine ring of B_0'. This completes the proof of the proposition. □

We fix elements $c_2, c_8, c_{12}, c_{14}, c_{18}, c_{20}, c_{24}, c_{30}$ and x, y, z as in Proposition 4.12. Thus we have identified $\mathscr{X}_0$ explicitly as given by the equation

$$y^2 = z^3 + x^5 + z(c_2 x^3 + c_8 x^2 + c_{14} x + c_{20}) + (c_{12} x^3 + c_{18} x^2 + c_{24} x + c_{30}). \tag{4.3}$$

We view (4.3) as an affine Weierstrass equation over $\mathbb{A}^1_{B_0}$. This allows us to compactify $\mathscr{X}_0$ to obtain a projective Weierstrass fibration (in the sense of [Mir81]) $\mathscr{Y}_0 \to \mathbb{P}^1_{B_0}$ which contains $\mathscr{X}_0$ as an open subscheme. More precisely, $\mathscr{X}_0$ is the complement in $\mathscr{Y}_0$ of the zero section $\mathscr{O}$ and the fibre $\mathscr{F}$ above the point $x = \infty$ of $\mathbb{P}^1_{B_0}$.

Let $\kappa_0 = E + \mathfrak{z}_{\mathfrak{h}}(F)$, and let $\sigma_0 = \pi_0|_{\kappa_0}^{-1} : B_0 \to \mathfrak{h}$ denote the Kostant section for $\mathfrak{h}$. (Thus $\kappa = \kappa_0 \cap V$.) Let $A_0 = Z_H(\sigma_0|_{B_0^{\mathrm{rs}}})$, and let $\Lambda_0 = X^*(A_0)$. Then Λ_0 is an étale sheaf of E_8 root lattices on B_0^{rs}.

Observe that there is a A_0-torsor $\mathscr{T}_0 \to \mathscr{X}_0^{\mathrm{rs}}$ given by the formula

$$\mathscr{T}_0 = \{(h, x) \in H \times B_0^{\mathrm{rs}} \mid h \cdot \sigma_0(x) \in \mathscr{X}^{\mathrm{rs}}\}.$$

Let η_0 be the generic point of B_0, and let $\overline{\eta}_0$ be a geometric point above it. The existence of $\mathscr{T}_0$ determines a $\pi_1(\eta_0, \overline{\eta}_0)$-equivariant map $X^*(A_{0,\overline{\eta}_0}) \to \mathrm{Pic}(\mathscr{X}_{0,\overline{\eta}_0})$. (Note that this étale fundamental group can be identified with $\mathrm{Gal}(k(\overline{\eta}_0)/k(\eta_0))$.) We endow $\mathrm{Pic}(\mathscr{X}_{0,\overline{\eta}_0})$ with an intersection pairing as follows. There is a perfect intersection pairing on $\mathrm{Pic}(\mathscr{Y}_{0,\overline{\eta}_0})$, which is a free $\mathbb{Z}$-module of rank 10 ($\mathscr{Y}_{0,\overline{\eta}_0}$ is a rational elliptic surface, cf. [SS10, §8]). Let $\mathscr{W}_0 = \langle \mathscr{O}, \mathscr{F} \rangle \subset \mathrm{Pic}(\mathscr{Y}_{0,\overline{\eta}_0})$, and let $\mathscr{W}_0^\perp$ denote its orthogonal complement. Then $\mathrm{Pic}(\mathscr{Y}_{0,\overline{\eta}_0}) = \mathscr{W}_0 \oplus \mathscr{W}_0^\perp$, and so the morphism $\mathscr{W}_0^\perp \to \mathrm{Pic}(\mathscr{Y}_{0,\overline{\eta}_0}) \to \mathrm{Pic}(\mathscr{X}_{0,\overline{\eta}_0})$ induced by the open immersion $\mathscr{X}_{0,\overline{\eta}_0} \to \mathscr{Y}_{0,\overline{\eta}_0}$ is an isomorphism. We give $\mathrm{Pic}(\mathscr{X}_{0,\overline{\eta}_0})$ the perfect, negative definite pairing induced from that of $\mathscr{W}_0^\perp$.

Lemma 4.13. *The $\pi_1(\eta_0, \overline{\eta}_0)$-equivariant morphism $X^*(A_{0,\overline{\eta}_0}) \to \mathrm{Pic}(\mathscr{X}_{0,\overline{\eta}_0}) \cong \mathscr{W}_0^\perp$ just constructed is an isomorphism which intertwines the pairing $(\cdot,\cdot) : \Lambda_0 \times \Lambda_0 \to \mathbb{Z}$ with minus the intersection pairing on $\mathrm{Pic}(\mathscr{X}_{0,\overline{\eta}_0}) \cong \mathscr{W}_0^\perp$.*

Proof. To show that this morphism is an isomorphism, we use the existence of the Springer resolution. Recall that $T \subset H$ is a maximal torus with Lie algebra $\mathfrak{t}$ and root basis $S_H \subset \Phi(H, T)$. We write $P \subset H$ for the Borel subgroup corresponding to this choice of root basis. Let $\mathscr{X}_{0,\mathfrak{t}}$ denote the pullback of $\mathscr{X}_0 \to B_0$ along the finite map $\mathfrak{t} \to B_0 = \mathfrak{t} /\!\!/ W(H, T)$, and define

$$\widetilde{\mathscr{X}_{0,\mathfrak{t}}} = \{(hP, x) \in H/P \times \mathscr{X}_{0,\mathfrak{t}} \mid x \in \mathrm{Ad}(h)(\mathrm{Lie}\, P)\}.$$

Then $\widetilde{\mathscr{X}_{0,\mathfrak{t}}} \to \mathfrak{t}$ is the Springer resolution of the transverse slice $\mathscr{X}_0$: it is smooth, and the morphism $\widetilde{\mathscr{X}_{0,\mathfrak{t}}} \to \mathscr{X}_{0,\mathfrak{t}}$ is a proper morphism which is an isomorphism away from the singular points in each fibre of $\mathscr{X}_{0,\mathfrak{t}} \to \mathfrak{t}$ (cf. [Slo80, §5.3]). In particular, we can glue $\widetilde{\mathscr{X}_{0,\mathfrak{t}}}$ with $\mathscr{Y}_{0,\mathfrak{t}}$ to obtain a smooth proper surface $\widetilde{\mathscr{Y}_{0,\mathfrak{t}}} \to \mathfrak{t}$ which is itself a resolution of $\mathscr{Y}_{0,\mathfrak{t}} \to \mathfrak{t}$.

We have $\mathrm{Pic}(H/P) = X^*(T)$. The projection $\widetilde{\mathscr{X}_{0,\mathfrak{t}}} \to H/P$ therefore induces a map $X^*(T) \to \mathrm{Pic}(\widetilde{\mathscr{X}_{0,\mathfrak{t}}})$. Let ξ denote the generic point of $\mathfrak{t}$, and let $\overline{\xi}$ denote a lift of $\overline{\eta}_0$ to a geometric point above ξ. We claim that the composite

$$X^*(T) \to \mathrm{Pic}(\widetilde{\mathscr{X}_{0,\mathfrak{t}}}) \to \mathrm{Pic}(\widetilde{\mathscr{X}_{0,\mathfrak{t},\overline{\xi}}})$$

is an isomorphism. In fact, it suffices to prove the analogous claim above the central point 0 of $\mathfrak{t}$, as we now explain. In order to avoid confusing notation, let us write s for this point, and $\overline{s}$ for a geometric point above it. Then there is a commutative diagram

$$\begin{tikzcd}
X^*(T) \arrow[r] \arrow[d, "="] & \mathrm{Pic}(\widetilde{\mathscr{X}_{0,\mathfrak{t},\overline{\xi}}}) \arrow[d] \\
X^*(T) \arrow[r] & \mathrm{Pic}(\widetilde{\mathscr{X}_{0,\mathfrak{t},\overline{s}}}),
\end{tikzcd}$$

where the right vertical map is given by specialization and is injective with torsion-free cokernel (cf. [MP12, Proposition 3.6], which gives a specialization morphism for Néron–Severi groups of the fibres of the proper morphism $\widetilde{\mathscr{Y}_{0,\mathfrak{t}}} \to \mathfrak{t}$; we are using that the fibres of $\widetilde{\mathscr{Y}_{0,\mathfrak{t}}} \to \mathfrak{t}$ are rational elliptic surfaces, and that in each geometric fibre the free rank 2 subgroup $\langle \mathscr{O}, \mathscr{F} \rangle$ of the Picard group splits off as a direct summand in a way that is compatible with specialization). Since the source and target of the right vertical arrow are both free $\mathbb{Z}$-modules of rank 8, this arrow is an isomorphism. It follows that if the bottom arrow in the above diagram is an isomorphism, then so is the top arrow.

Here, however, we can make everything explicit, using the description of the exceptional fibre of the morphism $\widetilde{\mathscr{X}_{0,\mathfrak{t},\overline{s}}} \to \mathscr{X}_{0,\mathfrak{t},\overline{s}}$ given in [Hin91]. The upshot is that this exceptional divisor is a union of projective lines C_α indexed by simple roots $\alpha \in S_H$, the classes of which freely generate $\mathrm{Pic}(\widetilde{\mathscr{X}_{0,\mathfrak{t},\overline{0}}})$; and if $\alpha \in S_H$ is a simple root, then the image of $\alpha \in X^*(T)$ in the Picard group is the class of the curve C_α (this is [Hin91, 5.3, Lemma]).

The same argument shows that the morphism $X^*(T) \to \mathrm{Pic}(\widetilde{\mathscr{X}_{0,\mathfrak{t},\overline{\xi}}}) \cong \mathscr{W}_0^\perp$ intertwines the root lattice on $X^*(T)$ with the negative of the intersection pairing on $\mathscr{W}_0^\perp$. Indeed, this can be checked in the central fibre of the Springer resolution, where it follows from the formula $(C_\alpha, C_\beta) = -\check{\beta}(\alpha)$, itself a consequence of [Hin91, Proposition 5.2].

It remains to see why the above results on the map $X^*(T) \to \mathrm{Pic}(\widetilde{\mathscr{X}_{0,\mathfrak{t},\overline{\xi}}})$ imply what we need for the map $X^*(A_{\overline{\eta}_0}) \to \mathrm{Pic}(\mathscr{X}_{0,\overline{\eta}_0})$. However, the points $\overline{\xi}$ and $\sigma_0(\overline{\eta}_0)$ of $\mathfrak{h}(k(\overline{\eta}_0))$ are conjugate under the action of $H(k(\overline{\eta}_0))$, so what we really need to check is that the two maps $X^*(T) \to \mathrm{Pic}(\widetilde{\mathscr{X}_{0,\mathfrak{t},\overline{\xi}}})$, one arising by pullback from $\mathrm{Pic}(H/P)$, and the other arising from the existence of the $T_{k(\overline{\eta}_0)}$-torsor

$$\mathscr{T}' = \{h \in H_{k(\overline{\eta}_0)} \mid \mathrm{Ad}(h)(\xi) \in \mathscr{X}_{0,k(\overline{\eta}_0)}\},$$

are the same. This follows from the definitions. □

The morphism $\mathscr{X}_0 \to B_0$ is μ_3-equivariant, and μ_3 acts on $B_0 = \operatorname{Spec} \mathbb{Q}[c_2, c_8, c_{12}, c_{14}, c_{18}, c_{20}, c_{24}, c_{30}]$ by the formula $\zeta \cdot c_i = \zeta^{-i} c_i$. If $\mathscr{X}$ denotes the restriction of $\mathscr{X}_0$ to $B = \operatorname{Spec} \mathbb{Q}[c_{12}, c_{18}, c_{24}, c_{30}] = B_0^{\mu_3}$, then θ acts on the fibres of $\mathscr{X} \to B$ by the formula $\theta(\zeta)(x, y, z) = (x, y, \zeta^{-1} z)$. If we write $\mathscr{Y} \to B$ for the pullback of $\mathscr{Y}_0$ to B, then μ_3 acts on the fibres of $\mathscr{Y} \to B$ by the same formula, and we can identify the fixed locus $\mathscr{Y}^{\mu_3}$ with the projective completion $\mathscr{C}$ of the family of affine curves

$$\mathscr{C}^0 : y^2 = x^5 + c_{12}x^3 + c_{18}x^2 + c_{24}x + c_{30} \tag{4.4}$$

that is the object of our study in this paper.

We now come back to Proposition 4.3. We recall that we have defined $\Lambda = X^*(A)$, where $A = Z_H(\sigma|_{B^{\mathrm{rs}}})$ is a torus over B^{rs}. Thus Λ is an étale sheaf of E_8 root lattices, which may be identified with the pullback of Λ_0 along the closed immersion $B \to B_0$. The image of the stable $\mathbb{Z}/3\mathbb{Z}$-grading $\theta : \mu_3 \to H$ normalizes A, and determines an elliptic μ_3-action $\theta : \mu_3 \to \mathrm{Aut}(\Lambda)$. We must show that there is an isomorphism $\Lambda_\theta \to \mathscr{J}[3]$ intertwining the pairing $\langle \cdot, \cdot \rangle$ on Λ_θ, described in §2, with the Weil pairing on $\mathscr{J}[3]$.

We define the morphism $\Lambda_\theta \to \mathscr{J}[3]$ in stages. Since both Λ and $\mathscr{J}[3]$ are locally constant étale sheaves over B^{rs}, it is enough to define this morphism at the generic point η of B^{rs}. Let η now denote the generic point of B^{rs}, and let $\overline{\eta}$ be a geometric point above it. We have the following corollary of Lemma 4.13:

Corollary 4.14. *There is a $\pi_1(\eta, \overline{\eta})$-equivariant isomorphism $X^*(A_{\overline{\eta}}) \to \mathrm{Pic}(\mathscr{X}_{\overline{\eta}})$ which intertwines the Weyl-invariant pairing on the source with the negative of the intersection pairing of $\mathscr{W}^\perp$ on the target.*

The morphism $X^*(A_{\overline{\eta}}) \to \mathrm{Pic}^0(\mathscr{C}_{\overline{\eta}})$ is defined to be the composite

$$X^*(A_{\overline{\eta}}) \to \mathrm{Pic}(\mathscr{X}_{\overline{\eta}}) \to \mathrm{Pic}(\mathscr{C}^0_{\overline{\eta}}) \cong \mathrm{Pic}^0(\mathscr{C}_{\overline{\eta}}),$$

where the first arrow is the one given by Corollary 4.14, the second is pullback along $\mathscr{C}^0 \to \mathscr{X}$, and the third one is the natural isomorphism $\mathrm{Pic}(\mathscr{C}^0_{\overline{\eta}}) \cong \mathrm{Pic}(\mathscr{C}_{\overline{\eta}})/\langle \mathscr{P}_{\overline{\eta}} \rangle \cong \mathrm{Pic}^0(\mathscr{C}_{\overline{\eta}})$. We could equivalently define it as the composite

$$X^*(A_{\overline{\eta}}) \to \mathrm{Pic}(\mathscr{X}_{\overline{\eta}}) \cong \mathscr{W}^\perp \subset \mathrm{Pic}(\mathscr{Y}_{\overline{\eta}}) \to \mathrm{Pic}(\mathscr{C}_{\overline{\eta}}),$$

where $\mathscr{W} = \langle \mathscr{O}, \mathscr{F} \rangle \subset \mathrm{Pic}(\mathscr{Y}_{\overline{\eta}})$ and $\mathscr{W}^\perp \subset \mathrm{Pic}(\mathscr{Y}_{\overline{\eta}})$ is the orthogonal complement, and where the last arrow is now pullback along $\mathscr{C} \to \mathscr{Y}$.

The map $X^*(A_{\overline{\eta}}) \to \mathrm{Pic}(\mathscr{C}_{\overline{\eta}})$ is $\pi_1(\eta, \overline{\eta})$-equivariant and factors through the θ-coinvariants in $X^*(A_{\overline{\eta}})$, which are 3-torsion. We obtain a morphism $\Lambda_\theta \to \mathscr{J}[3]$ of locally constant étale sheaves on B^{rs}.

Proposition 4.15. *This morphism $\Lambda_\theta \to \mathscr{J}[3]$ is an isomorphism, which intertwines the pairing $\langle \cdot, \cdot \rangle$ on Λ_θ with the Weil pairing on $\mathscr{J}[3]$.*

Proof. It suffices to check this statement at the geometric generic point of B^{rs}. Let us write $\langle \cdot, \cdot \rangle_W$ for the Weil pairing on $\mathscr{J}[3]_{\overline{\eta}} = \mathrm{Pic}(\mathscr{C}_{\overline{\eta}})[3]$. We will consider the factorization

$$X^*(A_{\overline{\eta}}) \to \mathrm{Pic}(\mathscr{X}_{\overline{\eta}}) \to \mathrm{Pic}(\mathscr{C}^0_{\overline{\eta}}).$$

Let us write $(\cdot, \cdot)_{\mathscr{W}^\perp}$ for the (negative definite) intersection pairing on $\mathrm{Pic}(\mathscr{X}_{\overline{\eta}})$, and $(\cdot, \cdot)$ for its negative. The pairing $(\cdot, \cdot)$ corresponds under the isomorphism $X^*(A_{\overline{\eta}}) \cong \mathrm{Pic}(\mathscr{X}_{\overline{\eta}})$ of Corollary 4.14 to the pairing on $X^*(A_{\overline{\eta}})$ which is also denoted by $(\cdot, \cdot)$. To prove the proposition, it is enough to show that the map $\mathrm{Pic}(\mathscr{X}_{\overline{\eta}}) \to \mathrm{Pic}(\mathscr{C}^0_{\overline{\eta}})$ factors through an isomorphism $\psi : \mathrm{Pic}(\mathscr{X}_{\overline{\eta}})_\theta \to \mathrm{Pic}^0(\mathscr{C}_{\overline{\eta}})[3]$ which satisfies the identity

$$\zeta^{((1-\theta(\zeta))\alpha, \beta)} = \zeta^{-((1-\theta(\zeta))\alpha, \beta)_{\mathscr{W}^\perp}} = \langle \psi(\alpha), \psi(\beta) \rangle_W \tag{4.5}$$

for all $\alpha, \beta \in \mathrm{Pic}(\mathscr{X}_{\overline{\eta}})$. In order to do this, we will make everything explicit. Recall (cf. §2) that $\mathrm{Pic}(\mathscr{X}_{\overline{\eta}})_\theta$ is isomorphic as an abelian group to $(\mathbb{Z}/3\mathbb{Z})^4$. Its 80 non-trivial elements are in bijective correspondence with the θ-orbits of root vectors in $\mathrm{Pic}(\mathscr{X}_{\overline{\eta}})$. To prove the result, it will suffice to show that these 80 non-trivial elements are in bijection with the non-trivial elements of $\mathrm{Pic}(\mathscr{C}_{\overline{\eta}})[3]$, and that if $\alpha, \beta \in \mathrm{Pic}(\mathscr{X}_{\overline{\eta}})$ are two root vectors, then they satisfy the identity (4.5).

The root vectors α in $\mathrm{Pic}(\mathscr{X}_{\overline{\eta}})$ correspond exactly to the sections $s_\alpha : \mathbb{P}^1_{\overline{\eta}} \to \mathscr{Y}_{\overline{\eta}}$ of $\mathscr{Y}_{\overline{\eta}} \to \mathbb{P}^1_{\overline{\eta}}$ which do not meet the zero section $\mathscr{O}$ (see e.g. [Shi10]). If $\ell_\alpha \subset \mathscr{Y}_{\overline{\eta}}$ denotes the image of s_α, then the element of $\mathscr{W}^\perp \subset \mathrm{Pic}(\mathscr{Y}_{\overline{\eta}})$ corresponding to α is $\ell_\alpha - \mathscr{O} - \mathscr{F}$. The sections s_α admit unique expressions as $(a(x), b(x))$, where $a(x), b(x) \in k(\overline{\eta})[x]$ have degree 2, 3 respectively and satisfy $b(x)^2 = a(x)^3 + f(x)$. Suppose $s_\alpha = (a(x), b(x))$

and $s_\beta = (c(x), d(x))$ are two such sections. If $\alpha \neq \pm\beta$ then $b(x) - d(x)$ has 3 zeroes in $k(\overline{\eta})$, counted with multiplicity, and we have the formula

$$\begin{aligned}(\alpha, \beta) &= -(\ell_\alpha - \mathscr{O} - \mathscr{F}, \ell_\beta - \mathscr{O} - \mathscr{F})_{\mathscr{W}^\perp} = 1 - (\ell_\alpha, \ell_\beta)_{\mathscr{W}^\perp} \\ &= 1 - |\{\gamma \in k(\overline{\eta}) \mid b(\gamma) = d(\gamma), a(\gamma) = c(\gamma)\}|,\end{aligned}$$

(see e.g. [SS10, §8.7]).

Note that $\theta(\zeta)(s_\alpha) = (\zeta^{-1}a(x), b(x))$. Therefore we have the formula

$$\zeta^{((1-\theta(\zeta)(\alpha),\beta)} = \zeta^{-|\{\gamma\in k(\overline{\eta})|b(\gamma)=d(\gamma),a(\gamma)=c(\gamma)\}|+|\{\gamma\in k(\overline{\eta})|b(\gamma)=d(\gamma),\zeta^{-1}a(\gamma)=c(\gamma)\}|}. \tag{4.6}$$

What is $\psi(\alpha)$? It is the class of the divisor $P_1 + P_2 - 2\infty$, where $a(x)$ has roots γ_1, γ_2 in $k(\overline{\eta})$ and $P_i = (a(\gamma_i), b(\gamma_i))$.

We compare this with the Weil pairing $\langle\psi(\alpha), \psi(\beta)\rangle_W$ on a case by case basis as follows. Assuming as we may that $\alpha \neq \theta(\zeta^i)\beta$ for any $i \in \mathbb{Z}$, we see that $a(x) - c(x)$ is not the zero polynomial. Let $\Sigma(\alpha, \beta)$ denote the set of zeroes in $k(\overline{\eta})$ of $b(x) - d(x)$; it has 3 elements. For each $\gamma \in \Sigma(\alpha, \beta)$, we have $a(\gamma)^3 = c(\gamma)^3$, hence $\omega(\gamma) = c(\gamma)/a(\gamma)$ is a 3rd root of unity. We now divide into 2 cases.

The first case is where the values $\omega(\gamma)$, $\gamma \in \Sigma(\alpha, \beta)$, are pairwise distinct. In this case we see that both the Weil pairing $\langle\psi(\alpha), \psi(\beta)\rangle_W$ and the value given by (4.6) are equal to 1. Indeed, the Weil pairing can be computed using [BFT14, Lemma 5], while for (4.6) this is obvious.

The second case is where some value $\omega(\gamma)$ occurs exactly twice. Since our pairing does not depend on the choice of ζ, we can suppose without loss of generality that it is ζ that appears twice. Then we see that (4.6) gives a value of ζ^{-1} (if the other value of $\omega(\gamma)$ is 1) or ζ (if the other value of $\omega(\gamma)$ is ζ^{-1}). Again, this agrees with the result of [BFT14, Lemma 5]. This concludes the proof. □

The only part of Proposition 4.3 that remains to be proved is that $\Delta_0 = \operatorname{disc}(x^5 + c_{12}x^3 + c_{16}x^2 + c_{24}x + c_{30})$ has the property that Δ_0^2 is (up to scalar) the restriction to V of the usual Lie algebra discriminant Δ. Note that Δ_0^2 and Δ both have degree 240, that Δ_0 is irreducible, and that Δ_0^2 and Δ vanish along the same points (as follows from e.g. [Slo80, §6.6]). This implies that they are equal up to scalar, as desired.

4.5 Spreading out

So far we have described the structure of the representation (G, V) over $\mathbb{Q}$. We recall (see §4.1) that it has a natural extension $(\underline{G}, \underline{V})$ over $\mathbb{Z}$. We now observe that all of the above works equally well over $\mathbb{Z}[1/N]$ for some integer $N \geq 1$.

Indeed, we can choose the invariant polynomials $c_{12}, c_{18}, c_{24}, c_{30} \in \mathbb{Q}[V]^G$ to lie in $\mathbb{Z}[V]^G$ (by using the $\mathbb{G}_m$-equivariant structure of $\mathscr{X}_0$ described at the beginning of §4.4 to clear denominators). We set $\underline{B} = \operatorname{Spec}\mathbb{Z}[c_{12}, \ldots, c_{30}]$ and write $\pi : \underline{V} \to \underline{B}$ for the corresponding morphism (which extends the morphism between $V \to B$ on $\mathbb{Q}$-fibres already denoted by π). Note that this implies that $\Delta_0 = \operatorname{disc}(x^5 + c_{12}x^3 + c_{18}x^2 + c_{24}x + c_{30}) \in \mathbb{Z}[V]^G$ too. We define $\underline{B}^{\mathrm{rs}} = \operatorname{Spec}\mathbb{Z}[c_{12}, c_{18}, c_{24}, c_{30}][\Delta_0^{-1}]$. We extend $\mathscr{C}$ to a family of projective curves $\mathscr{C} \to \underline{B}$ given by the same equation as before.

We can now find an integer $N \geq 1$ satisfying the following properties:

1. Let $S = \mathbb{Z}[1/N]$. Then each prime p dividing the order of the Weyl group of H (i.e. $p \in \{2, 3, 5, 7\}$) is a unit in S. In particular, the morphism $\mathscr{C}_S \to \underline{B}_S$ is smooth exactly above $\underline{B}_S^{\mathrm{rs}}$.

2. $S[V]^G = S[c_{12}, c_{18}, c_{24}, c_{30}]$. The Kostant section extends to a section $\sigma : \underline{B}_S \to \underline{V}_S$ of π which satisfies the following property: for any $f \in \underline{B}(\mathbb{Z}) \subset \underline{B}(S)$, $\sigma(N \cdot f) \in \underline{V}(\mathbb{Z})$. We write $\kappa_S \subset \underline{V}_S$ for the image of the Kostant section.

3. There exist open subschemes $\underline{V}^{\text{reg}} \subset \underline{V}^{\text{rs}} \subset \underline{V}_S$ such that if $S \to k$ is a field and $v \in \underline{V}(k)$, then v is regular if and only if $v \in \underline{V}^{\text{reg}}(k)$ and v is regular semisimple if and only if $v \in \underline{V}^{\text{rs}}(k)$. Moreover, $\underline{V}^{\text{rs}}$ is the locus in $\underline{V}_S$ where Δ_0 does not vanish.

4. Let $A = Z_H(\sigma_S|_{\underline{B}_S^{\text{rs}}})$, a maximal torus in $H_{\underline{B}_S^{\text{rs}}}$, and let $\Lambda = X^*(A)$. Then Λ is an étale sheaf of E_8 root lattices on $\underline{B}_S^{\text{rs}}$, equipped with a pairing $(\cdot, \cdot) : \Lambda \times \Lambda \to \mathbb{Z}$ and an elliptic μ_3-action $\theta : \mu_3 \to \text{Aut}(\Lambda)$.

5. There is a perfect pairing $\langle \cdot, \cdot \rangle : \Lambda_\theta \times \Lambda_\theta \to \mu_3$ induced by usual formula $\langle \lambda, \mu \rangle = \zeta^{((1-\theta(\zeta))(\lambda),\mu)}$ for any primitive 3rd root of unity ζ. We can therefore extend the definition of the groupoids $\text{GrLieE}_{R,f}$ and $\text{Heis}_{R,f}$ of §4.3 to all S-algebras R.

6. Let $\mathscr{J} \to \underline{B}_S^{\text{rs}}$ denote the Jacobian of $\mathscr{C}_{\underline{B}_S^{\text{rs}}}$. Then there is an isomorphism $\Lambda_\theta \cong \mathscr{J}[3]$ of locally constant étale sheaves on $\underline{B}_S^{\text{rs}}$ which intertwines the pairing $\langle \cdot, \cdot \rangle$ on Λ_θ and the Weil pairing of $\mathscr{J}[3]$.

7. Let $\mathscr{M} = \mathcal{O}_{\mathscr{J}}(\mathscr{C} - \mathscr{P})$, a symmetric non-degenerate line bundle on $\mathscr{J}$, and let $\mathscr{L} = \mathscr{M}^{\otimes 3}$. Let $\mathscr{G} \subset \mathscr{G}(\mathscr{L})$ be the subgroup of 3-torsion elements. Then $\mathscr{G}$ is an extension

$$1 \to \mu_3 \to \mathscr{G} \to \mathscr{J}[3] \to 1.$$

Then the analogue of Proposition 4.6 holds in $\text{GrLieE}_{\underline{B}^{\text{rs}}, f_\tau}$.

With these data in hand, we can extend our constructions of orbits from sections of Jacobians. We can therefore apply the results of §4.3 for S-algebras R (and not just $\mathbb{Q}$-algebras). We mention in particular:

1. Let R be an S-algebra and let $f \in \underline{B}^{\text{rs}}(R)$. Suppose given a tuple $(H', \theta', \gamma') \in \text{GrLieE}_{R,f}$. If $(H', \theta') \cong (H_R, \theta_R)$, then (H', θ', γ') determines an element of $\underline{G}(R) \backslash \underline{V}_f(R)$, a set which is in turn in canonical bijection with the set $\ker(H^1(R, Z_G(\sigma(f))) \to H^1(R, \underline{G}))$.

2. Let R be an S-algebra, and let $f \in \underline{B}^{\text{rs}}(R)$. Suppose that every locally free R-module is free. Then there is an injective map $\eta_f : \mathscr{J}_f(R)/3\mathscr{J}_f(R) \to \underline{G}(R) \backslash \underline{V}_f(R)$ which is compatible with base change on R.

4.6 Measures

The results of this section are used in the calculations of §6 – 7. Let ω_G be a generator for the (free rank 1 $\mathbb{Z}$-module of) left-invariant top forms on $\underline{G}$. It is uniquely determined up to sign, and determines Haar measures dg on $G(\mathbb{R})$ and on $G(\mathbb{Q}_p)$ for each prime p.

Proposition 4.16. *The product* $\text{vol}(\underline{G}(\mathbb{Z}) \backslash \underline{G}(\mathbb{R})) \cdot \prod_p \text{vol}(\underline{G}(\mathbb{Z}_p))$ *converges absolutely, and equals 3.*

Proof. Note that $\underline{G}$ has class number 1 (i.e. $\underline{G}(\mathbb{Q}) \backslash \underline{G}(\mathbb{A}^\infty)/\underline{G}(\widehat{\mathbb{Z}})$ has 1 element). Therefore the product expresses the Tamagawa number of the simple group $G = \text{SL}_9/\mu_3$, which equals 3 (apply the results of [Lan66] and [Ono65]). □

Let ω_V be a generator for the for the left-invariant volume forms on $\underline{V}$, which is again determined up to sign, and determines Haar measures dv on $V(\mathbb{R})$ and on $V(\mathbb{Q}_p)$ for every prime p. We write ω_B for the volume form $dc_{12} \wedge dc_{18} \wedge dc_{24} \wedge dc_{30}$ on $\underline{B}$. It determines measures df on $B(\mathbb{R})$ and on $B(\mathbb{Q}_p)$ for every prime p.

Proposition 4.17. *There exists a constant $W_0 \in \mathbb{Q}^\times$ with the following properties:*

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

2. *Let $\underline{B}(\mathbb{Z}_p)^{rs} = \underline{B}(\mathbb{Z}_p) \cap B^{rs}(\mathbb{Q}_p)$, and let $\psi_p : \underline{V}(\mathbb{Z}_p)^{rs} \to \mathbb{R}_{\geq 0}$ be a bounded, locally constant function which is $\underline{G}(\mathbb{Q}_p)$-invariant, in the sense that if $v, v' \in \underline{V}(\mathbb{Z}_p)$ are conjugate under the action of $\underline{G}(\mathbb{Q}_p)$, then $\psi_p(v) = \psi_p(v')$. Then we have the formula*
$$\int_{v \in \underline{V}(\mathbb{Z}_p)^{rs}} \psi_p(v)\, dv = |W_0|_p \operatorname{vol}(\underline{G}(\mathbb{Z}_p)) \int_{f \in \underline{B}(\mathbb{Z}_p)^{rs}} \sum_{g \in \underline{G}(\mathbb{Q}_p)\backslash \underline{V}_f(\mathbb{Z}_p)} \frac{m_p(v)\psi_p(v)}{|Z_{\underline{G}}(v)(\mathbb{Q}_p)|}\, df.$$

3. *Let $U_0 \subset G(\mathbb{R})$ and $U_1 \subset B(\mathbb{R})^{rs}$ be open subsets such that the product morphism $\mu : U_0 \times U_1 \to V(\mathbb{R})^{rs}$, $(g, f) \mapsto g \cdot \sigma(f)$, is injective. Then we have the formula*
$$\int_{v \in \mu(U_0 \times U_1)} dv = |W_0| \int_{g \in U_0} dg \int_{f \in U_1} df.$$

Here we write $|\cdot|_p$ for the usual p-adic absolute value on $\mathbb{Q}_p$ (with $|p|_p = p^{-1}$).

Proof. All of these identities can be proved in the same way as in [RTa, Proposition 3.3] and [Tho15, Proposition 2.16]. The key input in the proof is the equality $\dim_{\mathbb{Q}} V = \sum_i \deg c_i$, which holds here since $84 = 12 + 18 + 24 + 30$. □

5 Constructing integral orbit representatives

We continue with the notation of §4. Let $\mathscr{E}$ denote the set of polynomials $f(x) = x^5 + c_{12}x^3 + c_{18}x^4 + c_{24}x + c_{30} \in \mathbb{Z}[x]$ of non-zero discriminant. If p is a prime, let $\mathscr{E}_p$ denote the set of polynomials $f(x) = x^5 + c_{12}x^3 + c_{18}x^4 + c_{24}x + c_{30} \in \mathbb{Z}_p[x]$ of non-zero discriminant. Thus we can identify $\mathscr{E}_p = \underline{B}(\mathbb{Z}_p)^{\mathrm{rs}} := \underline{B}(\mathbb{Z}_p) \cap B^{\mathrm{rs}}(\mathbb{Q}_p)$.

This section is devoted to the proof of the following theorem concerning the map η_f of Corollary 4.10.

Theorem 5.1. *Let N be the integer of §4.5. Then for each prime $p > N$, for each polynomial $f(x) \in \mathscr{E}_p$, and for each $P \in \mathscr{J}_f(\mathbb{Q}_p)$, the orbit $\eta_f(P) \in G(\mathbb{Q}_p)\backslash V_f(\mathbb{Q}_p)$ intersects $\underline{V}_f(\mathbb{Z}_p)$.*

Most of §5 is devoted to the proof of this theorem. We first prove the theorem for polynomials of square-free discriminant in §5.1. This is then used as an ingredient in the proof of the theorem in the general case in §5.2.

5.1 The case of square-free discriminant

In this section we establish Theorem 5.1 for polynomials $f(x) \in \mathscr{E}_p$ of square-free discriminant. We first prove two useful lemmas.

Lemma 5.2. *Let R be a Noetherian regular integral domain such that every locally free R-module of finite rank is free. Then the map $H^1(R, G) \to H^1(\mathrm{Frac}(R), G)$ has trivial kernel.*

Proof. The existence of the short exact sequence of *fppf* R-groups

$$1 \longrightarrow \mu_3 \longrightarrow \mathrm{SL}_9 \longrightarrow G \longrightarrow 1,$$

together with the triviality of $H^1(R, \mathrm{SL}_9)$, reduces the problem to showing that $H^2(R, \mu_3) \to H^2(K, \mu_3)$ is injective, or even that $H^2(R, \mathbb{G}_m) \to H^2(K, \mathbb{G}_m)$ is injective. This follows from [Gro68, 1.8]. □

Lemma 5.3. *Let R be a complete discrete valuation ring and let A be a quasi-finite étale commutative R-group which satisfies the "Néron mapping property" $A(R') = A(\mathrm{Frac}(R'))$ for any étale extension $R \to R'$ of discrete valuation rings. Then the natural map $H^1(R, A) \to H^1(K, A)$ is injective.*

Proof. Let $j : \operatorname{Spec} K \to \operatorname{Spec} R$ be the natural open immersion. The "Néron mapping property" says that $A = j_* j^* A$. The map $H^1(R, A) \to H^1(K, A)$ is therefore injective because it is the first map in the 5-term exact sequence associated to the spectral sequence $H^p(R, R^q j_* j^* A) \Rightarrow H^{p+q}(K, A)$. □

The following proposition contains Theorem 5.1 (in the space case $R = \mathbb{Z}_p$).

Proposition 5.4. *Let R be a discrete valuation ring in which N is a unit. Let $K = \operatorname{Frac} R$, and let $\mathrm{ord}_K : K^\times \twoheadrightarrow \mathbb{Z}$ be the normalized discrete valuation. Let $f \in \underline{B}(R)$. Suppose that $\mathrm{ord}_K \operatorname{disc}(f) \leq 1$. Then:*

1. *If $x \in \underline{V}_f(R)$, then $Z_{\underline{G}}(x)(K) = Z_{\underline{G}}(x)(R)$.*
2. *The natural map $\alpha : \underline{G}(R) \backslash \underline{V}_f(R) \to \underline{G}(K) \backslash \underline{V}_f(K)$ is injective and its image contains $\eta_f(\mathscr{J}_f(K)/3\mathscr{J}_f(K))$.*
3. *If further R is complete and has finite residue field then the image of α equals $\eta_f(\mathscr{J}_f(K)/3\mathscr{J}_f(K))$.*

Proof. We first note that we can assume that R is complete. To see this, we need to use the equality $\underline{G}(\widehat{K}) = \underline{G}(K)\underline{G}(\widehat{R})$, where $\widehat{R}$ is the completion of R and $\widehat{K} = \operatorname{Frac} \widehat{R}$ (see [Nis84, Théorème 3.2]). We therefore assume that R is complete.

If $\mathrm{ord}_K \operatorname{disc} f = 0$, then $\mathscr{J}_f$ is a smooth projective R-scheme and $\mathscr{J}_f(R) = \mathscr{J}_f(K)$. In particular the map $\mathscr{J}_f(K)/3\mathscr{J}_f(K) \to \underline{G}(K) \backslash \underline{V}_f(K)$ factors through $\underline{G}(R) \backslash \underline{V}_f(R)$. We therefore just need to check that $\underline{G}(R) \backslash \underline{V}_f(R) \to \underline{G}(K) \backslash \underline{V}_f(K)$ is injective. In fact, the map $H^1(R, \mathscr{J}_f[3]) \to H^1(K, \mathscr{J}_f[3])$ is injective (a special case of Lemma 5.3), so this follows from Lemma 4.5.

If the residue field of R is finite, then $H^1(R, \underline{G}) = \{1\}$ and the map $\mathscr{J}_f(R)/3\mathscr{J}_f(R) \to H^1(R, \mathscr{J}_f[3])$ is an isomorphism, as $H^1(R, \mathscr{J}_f)$ is trivial, by Lang's theorem.

Now suppose that $\mathrm{ord}_K \operatorname{disc} f = 1$. Roughly the same principles apply. Let $\mathcal{J}_f$ denote the Néron model of $\mathscr{J}_f$. It is a smooth group scheme over R with generic fibre $\mathscr{J}_f$, and $\mathscr{J}_f(K) = \mathcal{J}_f(R)$. Our assumptions imply that $\mathcal{J}_f$ has connected fibres and that the special fibre of $\mathcal{J}_f$ is an extension of an elliptic curve by a rank 1 torus. (Indeed, $\mathscr{C}_f$ is projective over R and regular. Its special fibre is integral and has a unique singularity, which is a node. Now one can compute using the results of [BLR90, Ch. 9].) In particular, the quasi-finite étale group scheme $\mathcal{J}_f[3]$ over R has generic fibre of order 3^4 and special fibre of order 3^3.

We claim that $\underline{V}_f^{\mathrm{reg}}(R) = \underline{V}_f(R)$. To prove this, we must show that any element x of $\underline{V}_f(R)$ has regular image $x_k \in \underline{V}_f(k)$, where k is the residue field of R. Consider the direct sum decomposition $\underline{\mathfrak{h}}_R = \underline{\mathfrak{h}}_{0,R} \oplus \underline{\mathfrak{h}}_{1,R}$, where $\mathrm{ad}(x)$ acts topologically nilpotently in $\underline{\mathfrak{h}}_0$ and invertibly in $\underline{\mathfrak{h}}_1$. Let ϖ be a uniformizer of R. The reduction modulo ϖ of this decomposition is the direct sum decomposition $\underline{\mathfrak{h}}_k = \underline{\mathfrak{h}}_{0,k} \oplus \underline{\mathfrak{h}}_{1,k}$, where $\mathrm{ad}(x_k)$

acts nilpotently in $\underline{\mathfrak{h}}_{0,k}$ and invertibly in $\underline{\mathfrak{h}}_{1,k}$. In fact, if $x_k = y_s + y_n$ is the Jordan decomposition of x_k as a sum of its semisimple and nilpotent parts, then $\underline{\mathfrak{h}}_{0,k} = \mathfrak{z}_{\underline{\mathfrak{h}}}(y_s)$. We must show that y_n is a regular nilpotent element of $\mathfrak{z}_{\underline{\mathfrak{h}}}(y_s)$.

To see this, we first observe that there exists a unique closed subgroup $\underline{L} \subset \underline{H}_R$ such that $\mathrm{Lie}\, \underline{L} = \underline{\mathfrak{h}}_{0,R}$ and such that $\underline{L}$ is smooth over R with connected fibres. Moreover, we have $\underline{L}_k = Z_{\underline{H}}(y_s)$. The uniqueness follows from [SGA70, Exp. XIV, Proposition 3.12]. To show existence, choose a regular semisimple element $\overline{r} \in \mathfrak{z}_{\underline{\mathfrak{h}}}(y_s)$ and an arbitrary lift $r \in \underline{\mathfrak{h}}_{R,0}$. The centralizer $Z_{\underline{H}}(r)$ is a maximal torus of $\underline{H}_R$ with Lie algebra contained in $\underline{\mathfrak{h}}_{R,0}$, and we can construct a Levi subgroup of $\underline{H}_R$ with Lie algebra $\mathfrak{h}_{R,0}$ after passage to an étale extension $R \to R'$ where $Z_{\underline{H}}(r)$ is split.

Using the results of [Slo80, §6.6], we see that the derived group of $\underline{L}$ has type A_2 and that the centre $Z_{\underline{L}}$ has rank 6. Moreover, the action of μ_3 determined by θ restricts to an action on $\underline{L}$, and the induced morphism $\theta_{\underline{L}} : \mu_3 \to \mathrm{Aut}(\underline{L})$ is a stable $\mathbb{Z}/3\mathbb{Z}$-grading. (We have defined this notion in §2 for a reductive group of type E_8, but the definition is the same here: in each geometric fibre, there is a maximal torus of $\underline{L}$ on which $\theta_{\underline{L}}$ defines an elliptic μ_3-action.)

To show that x_k is regular in $\underline{\mathfrak{h}}_k$, we must show that y_n is a regular nilpotent element in $\mathfrak{h}_{0,k}$. After passage to an étale extension $R \to R'$ of discrete valuation rings, we can find an isomorphism $\underline{\mathfrak{h}}_{0,R}^{\mathrm{der}} \cong \mathfrak{sl}_{3,R}$ under which $\theta_{\underline{L}}$ corresponds to the homomorphism $\zeta \mapsto \mathrm{Ad}(\mathrm{diag}(1, \zeta, \zeta^2))$. (The proof is the same as the proof of Lemma 2.3, using that the automorphism group of the A_2 root lattice contains a unique conjugacy class of elements of order 3.) Let Δ' denote the Lie algebra discriminant of $\underline{\mathfrak{h}}_{0,R}$. Then $\mathrm{ord}_K\, \Delta(x) = \mathrm{ord}_K\, \Delta'(x)$. Let x' denote the projection of x to $\underline{\mathfrak{h}}_{0,R}^{\mathrm{der}}$ (this projection exists because of our assumption on the residue characteristic of R).

The image of x' in $\mathfrak{sl}_{3,R}$ is given by a matrix

$$x' = \begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix},$$

and the discriminant $\Delta'(x)$ equals $(abc)^2$. If $\mathrm{ord}_K(abc)^2 = 2$ then exactly one of a, b or c is divisible by ϖ, and in this case we see that the reduction modulo ϖ of x' (which coincides with y_n) is a regular nilpotent element. This proves our claim that $\underline{V}_f^{\mathrm{reg}}(R) = \underline{V}_f(R)$.

We next claim that $Z_{\underline{G}}(\sigma(f))$ satisfies the "Néron mapping property" $Z_{\underline{G}}(\sigma(f))(R') = Z_{\underline{G}}(\sigma(f))(\mathrm{Frac}(R'))$ for any étale extension $R \to R'$ of discrete valuation rings. In view of the identification of $Z_{\underline{G}}(\sigma(f))_K$ with $\mathscr{J}_f[3]$, we just need to show that the isomorphism $Z_{\underline{G}}(\sigma(f))_K \cong \mathscr{J}_f[3]$ extends uniquely to an isomorphism $Z_{\underline{G}}(\sigma(f)) \cong \mathcal{J}_f[3]$. This will follow if we can show that the special fibre of $Z_{\underline{G}}(\sigma(f))$ has order 3^3. This is the case. Writing now $y_s + y_n$ for the Jordan decomposition of $\sigma(f)_k$ and carrying through the above computation, we see that $Z_{\underline{G}}(\sigma(f))_k$ can be identified with the $\theta_{\underline{L}}$-fixed points in the centre of the group $\underline{L}_k$. Since the centre is a rank-6 torus on which $\theta_{\underline{L}}$ defines an elliptic μ_3-action, this group indeed has order 3^3. (See [Tho13, Proposition 2.8] for a similar calculation.)

The map $\underline{G} \to \underline{V}_f^{\mathrm{reg}}$, $g \mapsto g \cdot \sigma(f)$ is surjective and étale, and in fact a torsor for the étale group scheme $Z_{\underline{G}}(\sigma(f))$. The only part of this claim that we have not already established is the fact that this map is surjective in the special fibre $\underline{G}_k \to \underline{V}_{f,k}^{\mathrm{reg}}$. This is equivalent to showing that if $y_s \in \underline{V}_k$ is a semisimple element such that $Z_{\underline{H}}(y_s)$ has derived group of type A_2, then $Z_{\underline{G}}(y_s) = Z_{\underline{H}}(y_s)^{\theta}$ acts transitively on the regular nilpotent elements of $\mathfrak{z}_{\underline{\mathfrak{h}}}(y_s)(1)$. This is true. (Note that in the $(\mathbb{Z}/3\mathbb{Z})$-grading of $\mathfrak{sl}_{3,k}$ given by $\xi : \zeta \mapsto \mathrm{Ad}(1, \zeta, \zeta^2)$, SL_3^{ξ} does not act transitively on the regular nilpotent elements, but PGL_3^{ξ} does. Luckily in our situation the group $Z_{\underline{H}}(y_s)$ fits into a θ-equivariant short exact sequence

$$1 \to C \to Z_{\underline{H}}(y_s) \to \mathrm{PGL}_3 \to 1,$$

where C is a θ-elliptic torus. This implies that the map $Z_{\underline{H}}(y_s)^\theta \to \mathrm{PGL}_3^\theta$ is surjective.)

It follows that the set $\underline{G}(R)\backslash \underline{V}_f(R)$ is in bijection with $\ker(H^1(R, Z_{\underline{G}}(\sigma(f))) \to H^1(R, \underline{G}))$. By Lemma 5.3, the map $H^1(R, Z_{\underline{G}}(\sigma(f))) \to H^1(K, Z_{\underline{G}}(\sigma(f)))$ is injective, implying that the map $\alpha : \underline{G}(R)\backslash \underline{V}_f(R) \to \underline{G}(K)\backslash \underline{V}_f(K)$ is injective (cf. [Con14, Exercise 2.4.11]). To show that the image of α contains the image of η_f, we observe that we have a commutative diagram

$$\begin{tikzcd}
\mathcal{J}_f(R)/3\mathcal{J}_f(R) \arrow[r] \arrow[d] & \mathscr{J}_f(K)/3\mathscr{J}_f(K) \arrow[d] \\
H^1(R, \mathcal{J}_f[3]) \arrow[r] & H^1(K, \mathscr{J}_f[3]).
\end{tikzcd}$$

We therefore just need to show that each class in the image of $\mathcal{J}_f(R)/3\mathcal{J}_f(R)$ in $H^1(R, \mathcal{J}_f[3]) \cong H^1(R, Z_{\underline{G}}(\sigma(f)))$ has trivial image in $H^1(R, \underline{G})$. This follows from the fact that the map $H^1(R, \underline{G}) \to H^1(K, \underline{G})$ is injective (Lemma 5.2).

Finally, suppose once more that R has finite residue field. Lang's theorem once again implies that $H^1(R, \underline{G}) = \{1\}$ and $H^1(R, \mathcal{J}_f) = \{1\}$. This completes the proof. □

Corollary 5.5. *Let R be a PID in which N is a unit, and let $f \in \underline{B}(R)$ be a polynomial such that* $\operatorname{disc}(f)$ *is square-free (as an element of R). Let $K = \operatorname{Frac}(R)$. Let $P \in \mathscr{J}_f(K)$, and let $\gamma_P \in \underline{V}_f(K)$ be a representative of the orbit $\eta_f(P)$. Then there exists $g \in \underline{G}(K)$ such that $g \cdot \gamma_P \in \underline{V}_f(R)$.*

Proof. We show that the tuple $(H_K, \theta_K, \gamma_P) \in \mathrm{GrLieE}_{K,f}$ extends to a tuple $(H_0, \theta_0, \gamma_0) \in \mathrm{GrLieE}_{R,f}$. By Lemma 5.2 and Lemma 4.4, we have $(H_0, \theta_0) \cong (\underline{H}_R, \theta_R)$, and the corollary will follow from this.

After localizing, we can assume that R is a DVR. In this case, Proposition 5.4 implies that we can find $g \in \underline{G}(K)$ such that $g \cdot \gamma_P \in \underline{V}_f(R)$. In other words, g defines an isomorphism between $(H_K, \theta_K, \gamma_K)$ and $(H_K, \theta_K, g \cdot \gamma_P)$, and the latter triple extends naturally to $(\underline{H}_R, \theta_R, g \cdot \gamma_P) \in \mathrm{GrLieE}_{R,f}$. □

5.2 The general case

We now use the results just established in §5.1 to complete the proof of Theorem 5.1. Let us therefore take a prime $p > N$, a polynomial $f(x) \in \mathscr{E}_p$, and a point $P \in \mathscr{J}_f(\mathbb{Q}_p)$. We must show that the orbit $\eta_f(P) \subset V_f(\mathbb{Q}_p)$ contains an element of $\underline{V}_f(\mathbb{Z}_p)$.

We first give an explicit representation of the point P. Arguing as in the proof of [BG13, Proposition 19], we can assume (after possibly changing P without changing its image in $\mathscr{J}_f(\mathbb{Q}_p)/3\mathscr{J}_f(\mathbb{Q}_p)$) that P corresponds to a decomposition $f(x) = u_0(x)v_0(x) + r_0(x)^2$, where for some $\nu \in \{0, 1, 2\}$, $u_0(x), v_0(x) \in \mathbb{Z}_p[x]$ are monic of degrees ν and $5 - \nu$, respectively, and $r_0(x)$ has degree at most $\nu - 1$. (This is the Mumford representation of P: thus P corresponds to the linear equivalence class of the divisor $D - \nu\infty$, where $D \subset \mathscr{C}^0_{f,\mathbb{Q}_p}$ is the effective divisor of degree ν determined by the equations $y = r_0(x), u_0(x) = 0$.)

Let D_ν denote the scheme (over $\mathbb{Z}_p$) of tuples of polynomials $(u(x), v(x), r(x))$, where $u(x), v(x)$ are monic of degrees ν and $5 - \nu$, respectively, and $r(x)$ has degree at most $\nu - 1$, and $u(x)v(x) + r(x)^2 = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ satisfies $a_1 = 0$. Thus the tuple $(u_0(x), v_0(x), r_0(x))$ determines a point of $D_\nu(\mathbb{Z}_p)$. Let $\delta \in H^0(D_\nu, \mathcal{O}_{D_\nu})$ denote the discriminant of the (monic, degree 5) polynomial $u(x)v(x) + r(x)^2$, and let $D_\nu^\delta \subset D_\nu$ denote the closed subscheme defined by the vanishing of δ. Then D_ν^δ has codimension 1 in each fibre of D_ν over $\mathbb{Z}_p$. (In fact, D_ν^δ is flat over $\underline{B}_{\mathbb{Z}_p}$).

Let λ be a formal variable. We can find a point $(u_1(x), u_1(x), r_1(x)) \in D_\nu(\mathbb{Z}_p[\lambda])$ with the following properties:

- We have $(u_1(x), v_1(x), r_1(x)) \bmod \lambda = (u_0(x), v_0(x), r_0(x))$.
- Let $f_1(x) = u_1(x)v_1(x) + r_1(x)^2 \in \mathbb{Z}_p[\lambda][x]$. Then $\operatorname{disc} f_1 = \delta(u_1, v_1, r_1)$ is square-free, when viewed as an element of the ring $\mathbb{Q}_p[\lambda]$, and its image in $\mathbb{F}_p[\lambda]$ is non-zero.

(We can accomplish this by choosing e.g. $u_1 = u_0 + \lambda u_0'$, $v_1 = v_0 + \lambda v_0', r_1 = r_0 + \lambda r_1'$ for some polynomials $u_0', v_0', r_0' \in \mathbb{Z}_p[x]$. We first choose them so that the discriminant of $f_1(x)$ is not zero in $\mathbb{F}_p[\lambda]$. If the discriminant is not already square-free in $\mathbb{Q}_p[\lambda]$ then by Bertini's theorem we can choose a small p-adic perturbation to make it so.)

Let $U_1 = \operatorname{Spec} \mathbb{Z}_p[\lambda][\operatorname{disc}(f_1)^{-1}]$. We have constructed a smooth projective curve $\mathscr{C}_{f_1} \to U_1$, together with a section $P_1 \in \mathscr{J}_{f_1}(U_1)$. Applying the construction described in §4.5, we obtain a tuple $(H_1, \theta_1, \gamma_1) \in \mathrm{GrLieE}_{U_1, f_1}$. The pullback of this tuple to $\mathrm{GrLieE}_{\mathbb{Q}_p, f}$ along the point $\{\lambda = 0\} \in U_1(\mathbb{Q}_p)$ corresponds to the orbit $\eta_f(P)$ under the bijection of Lemma 4.5.

Let $U_2 = \operatorname{Spec} \mathbb{Q}_p[\lambda]$. Using that $\operatorname{disc}(f_1)$ is square-free when viewed as an element of $\mathbb{Q}_p[\lambda]$, we can apply Corollary 5.5 to find that there is an extension of the triple $(H_1[1/p], \theta_1[1/p], \gamma_1[1/p])$ to a similar triple $(H_2, \theta_2, \gamma_2)$ over U_2. We can glue these triples to obtain a similar triple $(H_0, \theta_0, \gamma_0)$ over $U_0 = U_1 \cup U_2 \subset \operatorname{Spec} \mathbb{Z}_p[\lambda]$. Observe that by construction, θ_0 is a stable $\mathbb{Z}/3\mathbb{Z}$-grading of H_0.

Note that the complement of U_0 in $\operatorname{Spec} \mathbb{Z}_p[\lambda]$ is a union of finitely many closed points in the special fibre. We now apply the following lemma.

Lemma 5.6. *Let T be an integral regular scheme of dimension 2, and let $Z \subset T$ be a closed subset of dimension 0. Let $U = T - Z$. Then restriction $M \mapsto M_U$ defines an equivalence between the following two categories:*

1. *The category of reductive groups over T, with morphisms given by isomorphisms of group schemes.*
2. *The category of reductive groups over U, with morphisms given by isomorphisms of group schemes.*

Moreover, if M is a reductive group over T, then $H^0(T, \mathfrak{m}) = H^0(U, \mathfrak{m}_U)$.

Proof. The essential surjectivity is [CTS79, Theorem 6.13]. If M, M' are reductive group schemes over T, then the scheme of isomorphisms between M and M' is T-affine; this shows that the functor is fully faithful (cf. [CTS79, Lemma 2.1]). □

Applying Lemma 5.6, we see that H_0 extends uniquely to a reductive group H_2 over $\operatorname{Spec} \mathbb{Z}_p[\lambda]$, and that θ_0 extends uniquely to a grading $\theta_2 : \mu_3 \to H_2$, and γ_0 comes from a unique section $\gamma_2 \in V_2 = \mathfrak{h}_2(1)$. Note that θ_2 is a stable $\mathbb{Z}/3\mathbb{Z}$-grading of H_2. It follows that $(H_2, \theta_2, \gamma_2)$ is an object of the category $\mathrm{GrLieE}_{\mathbb{Z}_p[\lambda], f_1}$ considered in §4.3. By construction, its pullback to $\mathrm{GrLieE}_{\mathbb{Q}_p, f}$ along the map $\lambda = 0$ corresponds, under the bijection of Lemma 4.5, to the orbit $\eta_f(P) \in G(\mathbb{Q}_p)\backslash V_f(\mathbb{Q}_p)$.

Let $(H_3, \theta_3, \gamma_3) \in \mathrm{GrLieE}_{\mathbb{Z}_p, f}$ denote the pullback of $(H_2, \theta_2, \gamma_2)$ to $\mathbb{Z}_p$. Since $H^1(\mathbb{Z}_p, \underline{G}) = \{1\}$, this triple determines an orbit in $\underline{G}(\mathbb{Z}_p)\backslash \underline{V}_f(\mathbb{Z}_p)$ mapping to $\eta_f(P)$ under the natural map $\underline{G}(\mathbb{Z}_p)\backslash \underline{V}_f(\mathbb{Z}_p) \to G(\mathbb{Q}_p)\backslash V_f(\mathbb{Q}_p)$. This completes the proof of Theorem 5.1.

5.3 Complements

We conclude §5 with a weak result that holds for every prime (not just primes $p > N$). The $\mathbb{G}_m$-action on $\underline{B}$ here is the standard one (where $t \cdot c_i = t^i c_i$).

Proposition 5.7. *Let p be a prime, and let $f_0(x) \in \mathscr{E}_p$. Then there exists an integer $n \geq 1$ and an open neighbourhood W_p of f_0 in $\mathscr{E}_p$ such that for all $f \in W_p$ and for all $y \in \mathscr{J}_{p^n\cdot f}(\mathbb{Q}_p)$, the orbit $\eta_{p^n\cdot f}(y) \in G(\mathbb{Q}_p)\backslash V_{p^n\cdot f}(\mathbb{Q}_p)$ contains an element of $\underline{V}_{p^n\cdot f}(\mathbb{Z}_p)$.*

Proof. Choose $n \geq 1$ such that each orbit in the image of $\eta_{p^n\cdot f_0}$ intersects $\underline{V}_{p^n\cdot f_0}(\mathbb{Z}_p)$. Let $\sigma_1, \dots, \sigma_r \in \underline{V}_{p^n\cdot f_0}(\mathbb{Z}_p)$ be representatives for the distinct $G(\mathbb{Q}_p)$-orbits in the image of $\eta_{p^n\cdot f_0}$. For each $i = 1, \dots, r$, we can find an open neighbourhood $U'_{p,i} \subset \underline{V}(\mathbb{Z}_p)$ of σ_i with the following properties:

1. The image $\pi(U'_{p,i}) = U_p \subset \underline{B}(\mathbb{Z}_p)$ is independent of i, and $\pi|_{U'_{p,i}} : U'_{p,i} \to U_p$ is a homeomorphism. Let $s_i = \pi|_{U'_{p,i}}^{-1}$.
2. $U_p \subset \underline{B}(\mathbb{Z}_p)^{\mathrm{rs}} = \underline{B}(\mathbb{Z}_p) \cap B^{\mathrm{rs}}(\mathbb{Q}_p)$.
3. For each $g \in U_p$, the elements $s_i(g)$ represent the distinct $G(\mathbb{Q}_p)$-orbits in the image of η_g.

This essentially follows from the fact that the action map $G \to V_f$ attached to any $f \in B^{\mathrm{rs}}(\mathbb{Q}_p)$, $x \in V_f(\mathbb{Q}_p)$, is étale. After possibly shrinking U_p, we can assume that it has the form $p^n \cdot W_p$ for some open compact subset $W_p \subset \underline{B}(\mathbb{Z}_p)^{\mathrm{rs}}$ which contains f_0. This completes the proof. □

Corollary 5.8. *Let $f_0(x) \in \mathscr{E}$. Then for each prime $p \leq N$ we can find an open compact neighbourhood W_p of $f_0(x)$ in $\mathscr{E}_p$ and an integer $n_p \geq 0$ with the following property. Let $M = \prod_{p\leq N} p^{n_p}$. Then for all $f \in \mathscr{E} \cap (\prod_{p\leq N} W_p)$, and for all $y \in \mathrm{Sel}_3(\mathscr{J}_{M\cdot g})$, the orbit $\eta_{M\cdot f}(y) \in G(\mathbb{Q}_p)\backslash V_{M\cdot f}(\mathbb{Q}_p)$ contains an element of $\underline{V}_{M\cdot f}(\mathbb{Z})$.*

Proof. We have $G(\mathbb{A}^\infty) = G(\mathbb{Q})G(\widehat{\mathbb{Z}})$. It follows that for a given element $v \in V(\mathbb{Q})$, finding $g \in G(\mathbb{Q})$ such that $g \cdot v \in \underline{V}(\mathbb{Z})$ is equivalent to finding for each prime p an element $g_p \in G(\mathbb{Q}_p)$ such that $g \cdot v \in \underline{V}(\mathbb{Z}_p)$. The result therefore follows on combining Theorem 5.1 and Proposition 5.7. □

6 Counting points

We retain the notation of §4. In particular, we have a reductive group $\underline{G}$ over $\mathbb{Z}$ acting on a free $\mathbb{Z}$-module $\underline{V}$, and a $\underline{G}$-equivariant morphism $\pi : \underline{V} \to \underline{B} = \operatorname{Spec} \mathbb{Z}[c_{12}, c_{18}, c_{24}, c_{30}]$ (where $\underline{G}$ acts trivially on $\underline{B}$). For $f \in \underline{B}(\mathbb{Z})$, we define $\mathrm{ht}(f) = \sup_i |c_i(f)|^{120/i}$. If $v \in \underline{V}(\mathbb{Z})$, then we define $\mathrm{ht}(v) = \mathrm{ht}(\pi(v))$.

6.1 Counting points with finitely many congruence conditions

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

$$N(X, a) = \sum_{\substack{v \in \underline{G}(\mathbb{Z})\backslash X \\ \mathrm{ht}(v) < a}} \frac{1}{|Z_{\underline{G}}(v)(\mathbb{Z})|}.$$

Suppose given an integer $M \geq 1$ and a $\underline{G}(\mathbb{Z}/M\mathbb{Z})$-invariant function $w : \underline{V}(\mathbb{Z}/M\mathbb{Z}) \to \mathbb{R}_{\geq 0}$. We define

$$N_w(X, a) = \sum_{\substack{s \in \underline{G}(\mathbb{Z})\backslash X \\ \mathrm{ht}(v) < a}} \frac{w(v \bmod M)}{|Z_{\underline{G}}(v)(\mathbb{Z})|}.$$

We define μ_w to be the average value of w (where $\underline{V}(\mathbb{Z}/M\mathbb{Z})$ gets its uniform probability measure).

For a field $k/\mathbb{Q}$, we say that $v \in V(k)$ is k-reducible if v has zero discriminant or if v is $G(k)$-conjugate to the Kostant section $\sigma(\pi(v)) \in V(k)$. Otherwise we say that v is k-irreducible. If $X \subset V(\mathbb{Q})$ is any subset, then we write X^{irr} for its intersection with the set of $\mathbb{Q}$-irreducible elements.

The first main result of this section concerns the number of $\underline{G}(\mathbb{Z})$-orbits of $\mathbb{Q}$-irreducible elements of $\underline{V}(\mathbb{Z})$ of bounded height:

Theorem 6.1. *We have*

$$N_w(\underline{V}(\mathbb{Z})^{irr}, a) = \frac{|W_0|}{9}\mu_w \operatorname{vol}(\underline{G}(\mathbb{Z})\backslash G(\mathbb{R}))a^{7/10} + o(a^{7/10}),$$

where W_0 denotes the constant of Proposition 4.17.

The proof of Theorem 6.1 is very similar to the proofs of earlier results like [BG13, Theorem 36] (see also [Tho15, §3]). Rather than repeat details word for word here, we instead give the key propositions, which can be inserted into the arguments at the appropriate points. In comparing what we prove here with the results of [BG13] it's useful to note that because $\sigma(B^{\mathrm{rs}}(\mathbb{R}))$ contains exactly one representative for each orbit of $G(\mathbb{R})$ on $V(\mathbb{R})^{\mathrm{rs}}$, it may be used to construct a fundamental set for the action of $\mathbb{R}_{>0} \times G(\mathbb{R})$ on $V(\mathbb{R})^{\mathrm{rs}}$ (cf. [BG13, Section 9.1]), and also that the stabilizer in $G(\mathbb{R})$ of every element in $V(\mathbb{R})^{\mathrm{rs}}$ has order 9 (because for any $f \in B^{\mathrm{rs}}(\mathbb{R})$, $\mathscr{J}_f(\mathbb{R})[3]$ has order 9).

Following, e.g., [BG13, Section 10], the only arguments that do not carry over easily are those that show we can bound the contribution from the cusp region in a fundamental domain for the action of $\underline{G}(\mathbb{Z})$ on $V(\mathbb{R})$. To do this, by the same logic as in the proof of [Tho15, Theorem 3.6], it suffices to check that certain combinatorial properties hold in the set of weights for the action of G on V.

We start by defining some notation. We write $S_G = \{\beta_1, ..., \beta_8\}$ for the root basis of Φ_G fixed in §4.1. Then any $\gamma \in X^*(\underline{T})$ may be written uniquely as $\gamma = \sum_{i=1}^{8} n_i(\gamma)\beta_i$ for some $n_i(\gamma) \in \mathbb{Q}$. Note that the Cartan decomposition $\underline{\mathfrak{h}} = \underline{\mathfrak{t}} \oplus \sum_{\alpha\in\Phi_H} \underline{\mathfrak{h}}_\alpha$ of $\underline{\mathfrak{h}}$ is preserved by the action of μ_3 via θ. We define $\Phi_V = \{\alpha \in \Phi_H \mid \underline{\mathfrak{h}}_\alpha \subset \underline{V}\}$; then $\underline{V} = \oplus_{\alpha\in\Phi_V} \underline{\mathfrak{h}}_\alpha$. Given a vector $v \in \underline{V}$, we write $v = \sum_{\alpha\in\Phi_V} v_\alpha$ for its decomposition as a sum $\underline{T}$-eigenvectors. We write Φ_V^+ for $\Phi_H^+ \cap \Phi_V$. Given a subset $M \subset \Phi_V$, we define $\underline{V}(M) = \{v \in \underline{V} \mid v_\alpha = 0 \text{ for all } \alpha \text{ in } M\}$. The following lemma, which is a variant of [RTa, Proposition 2.15], gives criteria for the vectors in $\underline{V}(M)$ to be reducible.

Lemma 6.2. *Let $k/\mathbb{Q}$ be a field. Given a subset $M \subset \Phi_V$, suppose one of the following three conditions is satisfied:*

1. *We have $\Phi_V^+ - S_H \subset M$.*

2. *There exist integers $a_1, \dots, a_8$ not all equal to zero such that if $\alpha \in \Phi_V$ and $\sum_{i=1}^{8} a_i n_i(\alpha) > 0$, then $\alpha \in M$.*

3. *There exist $\beta \in \Phi_G$, $\alpha \in \Phi_V - M$, and integers $a_1, \dots, a_8$ 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 $\gamma \in M \cup \{\alpha\}$.

4. *There exist $\beta \in \Phi_G$, $\alpha \in \Phi_V - M$, integers $a_1, \dots, a_8$ not all equal to zero, and integers $b_1, ..., b_8$ not all equal to zero such that the following conditions hold:*

(a) $\{\gamma + \beta \mid \gamma \in M\} \cap \Phi_V \subset M$.

(b) $\alpha + \beta \in \Phi_V$.

(c) *If* $\gamma \in \Phi_V$ *and* $\sum_{i=1}^8 a_i n_i(\gamma) > 0$, *then* $\gamma \in M \cup \{\alpha\}$, *and if* $\gamma \in \Phi_V$ *and* $\sum_{i=1}^8 b_i n_i(\gamma) > 0$, *then* $\gamma \in M \cup \{\alpha + \beta\}$.

Then every element of $\underline{V}(M)(k)$ *is* k*-reducible.*

Proof. If one of the first three conditions is satisfied, the fact that the elements of $\underline{V}(M)(k)$ are k-reducible is given by a proof identical to that of [RTa, Proposition 2.15]. To prove that the fourth criterion implies reducibility, suppose $v \in \underline{V}(M)(k)$. If $v_\alpha = 0$ or $v_{\alpha+\beta} = 0$, then v is in $\underline{V}(M \cup \{\alpha\})(k)$ or $\underline{V}(M \cup \{\alpha + \beta\})(k)$ and so is reducible by condition 2 of the lemma. Thus we may assume $v_\alpha \neq 0$ and $v_{\alpha+\beta} \neq 0$. Let $U_{-\beta} \subset G$ be the root subgroup corresponding to $-\beta \in \Phi_G$. Note that there exists $u \in U_{-\beta}$ such that $u \cdot (v_\alpha + v_{\alpha+\beta}) = cv_{\alpha+\beta}$ for some constant c. By condition (a), we have $u \cdot v \in \underline{V}(M)(k)$, and so by our choice of u we have $u \cdot v \in \underline{V}(M \cup \{\alpha\})$. Thus v is k-reducible as desired. □

We call a pair (M_0, M_1) of disjoint subsets of Φ_V a cusp datum. Given a cusp datum (M_0, M_1), let $\underline{V}(M_0, M_1) = \{v \in \underline{V}(M_0) \mid v_\alpha \neq 0 \text{ for all } \alpha \in M_1\}$. The significance of the next result can be appreciated by looking at the proof of [Tho15, Proposition 3.6]; it is the essential ingredient in proving that there are few irreducible elements of $\underline{V}(\mathbb{Z})$ which are 'in the cusp' of a fundamental domain in $V(\mathbb{R})$ for the action of $\underline{G}(\mathbb{Z})$.

Proposition 6.3. *There exists a unique root* $\lambda_0 \in \Phi_V$ *that is maximal with respect to the partial ordering induced by the root basis* S_G*, or in other words such that* $n_i(\lambda_0) \geq n_i(\lambda)$ *for all* $i \in \{1, \ldots, 8\}$ *and all* $\lambda \in \Phi_V$*. There exists a collection* $\mathcal{C}$ *of cusp data such that*

- $\underline{V}(\{\lambda_0\})(\mathbb{Q})^{irr} \subset \bigcup_{(M_0,M_1)\in\mathcal{C}} \underline{V}(M_0, M_1)(\mathbb{Q})$ *and*
- *For each* $(M_0, M_1) \in \mathcal{C}$ *there exists a function* $f : M_1 \to \mathbb{R}_{\geq 0}$ *with* $\sum_{\alpha \in M_1} f(\alpha) < \# M_0$ *and*

$$\sum_{\alpha \in \Phi_G^+} n_i(\alpha) - \sum_{\alpha \in M_0} n_i(\alpha) + \sum_{\alpha \in M_1} f(\alpha) n_i(\alpha) > 0$$

for all $i \in \{1, ..., 8\}$.

Proof. Each weight $\lambda \in \Phi_V$ admits a unique expression $\lambda = \sum_{i=1}^8 n_i(\lambda)\beta_i$ for some $n_i(\lambda) \in \mathbb{Q}$. One checks that the height $h_G(\lambda) := \sum_{i=1}^8 n_i(\lambda)$ achieves its maximal value 9 exactly once, at the maximal weight λ_0 (which we note is not in this case the highest root of Φ_H with respect to the root basis S_H).

We use a computer to generate the collection $\mathcal{C}$ using a procedure very similar to the proof of [RTa, Proposition 4.5]. Yet here the criteria corresponding to [RTa, Proposition 2.15] is not enough to complete the proof: we must use part 4 of Lemma 6.2 to eliminate additional cusp data (M_0, M_1) such that $\underline{V}(M_0, M_1)(\mathbb{Q})^{\text{irr}} = \emptyset$. The details of this computation can be found in the Mathematica notebook `https://www.dpmms.cam.ac.uk/~jat58/E8(3)CuspData.nb`. □

Let N be the integer of §4.5, and let $p > N$ be a prime. We define $V_p^{\text{red}} \subset \underline{V}(\mathbb{Z}_p)$ to be the set of vectors $v \in \underline{V}(\mathbb{Z}_p)$ such that either $p | \Delta_0(v)$, or $p \nmid \Delta_0(v)$ and the image $\overline{v}$ of v in $\underline{V}(\mathbb{F}_p)$ is $\underline{G}(\mathbb{F}_p)$-conjugate to $\sigma(\pi(\overline{v}))$. Similarly, we define $V_p^{\text{bigstab}} \subset \underline{V}(\mathbb{Z}_p)$ to be the set of vectors $v \in \underline{V}(\mathbb{Z}_p)$ such that either $p | \Delta_0(v)$, or $p \nmid \Delta_0(v)$ and the image $\overline{v}$ of v in $\underline{V}(\mathbb{F}_p)$ has non-trivial stabilizer in $\underline{G}(\mathbb{F}_p)$.

Proposition 6.4. *We have*

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

and

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

Proof. This can be proved using [Ser12, Proposition 9.15]. We illustrate the method for V_p^{bigstab}. The number of points of $\underline{V}(\mathbb{F}_p)$ of zero discriminant is $O(p^{83})$. The number of points of $\underline{V}(\mathbb{F}_p)$ of non-zero discriminant equals $|B^{\text{rs}}(\mathbb{F}_p)||\underline{G}(\mathbb{F}_p)|$. For a prime $p\equiv 1 \bmod 3$, let $C\subset \mathrm{Sp}_4(\mathbb{F}_3)$ be the set of elements γ which have 1 as an eigenvalue. Then [Ser12, Proposition 9.15] gives

$$\int_{v\in V_p^{\text{bigstab}}} dv = \frac{1}{p^{84}}(|\{f\in B^{\text{rs}}(\mathbb{F}_p)\mid \mathrm{Frob}_f\in C\}|\cdot|\underline{G}(\mathbb{F}_p)|+O(p^{83})) = \frac{|C|}{|\mathrm{Sp}_4(\mathbb{F}_3)|}+O(p^{-1/2}).$$

Since $C\neq \mathrm{Sp}_4(\mathbb{F}_3)$, this implies what we need. □

Proposition 6.3 and Proposition 6.4 imply Theorem 6.1 just as [BG13, Propositions 29, 31, 32, 33] imply [BG13, Theorem 25] and its variant [BG13, Theorem 36].

6.2 Counting points with infinitely many congruence conditions

We now observe that using the results of [Bha] (see also [BS15]), we can get a strengthened version of Theorem 6.1 where we impose infinitely many congruence conditions. This is the analogue of [BG13, Theorem 42]. We state this following [BG13]. Suppose given for each prime p a $\underline{G}(\mathbb{Z}_p)$-invariant function $w_p:\underline{V}(\mathbb{Z}_p)\to[0,1]$ satisfying the following conditions:

- w_p is locally constant outside the closed subset $\underline{V}(\mathbb{Z}_p)-\underline{V}(\mathbb{Z}_p)^{\text{rs}}\subset\underline{V}(\mathbb{Z}_p)$.
- For all sufficiently large primes p, we have $w_p(v)=1$ for all $v\in\underline{V}(\mathbb{Z}_p)$ such that $p^2\nmid\Delta_0(v)$.

Then we can define a function $w:\underline{V}(\mathbb{Z})\to[0,1]$ by the formula $w(v)=\prod_p w_p(v)$ if $\Delta_0(v)\neq 0$, and $w(v)=0$ otherwise. If $X\subset\underline{V}(\mathbb{Z})$ is an $\underline{G}(\mathbb{Z})$-invariant subset, then we define

$$N_w(X,a)=\sum_{\substack{v\in\underline{G}(\mathbb{Z})\backslash X\\ \text{ht}(v)<a}}\frac{w(v)}{|Z_{\underline{G}}(v)(\mathbb{Z})|}.$$

Our strengthened theorem is then as follows.

Theorem 6.5. *We have*

$$N_w(\underline{V}(\mathbb{Z})^{irr},a)=\frac{|W_0|}{9}\left(\prod_p\int_{v\in\underline{V}(\mathbb{Z}_p)} w_p(v)\,dv\right)\mathrm{vol}(\underline{G}(\mathbb{Z})\backslash G(\mathbb{R}))a^{7/10}+o(a^{7/10}).$$

Following the proof of [BS15, Proposition 25], for primes $p>N$ we define

$$\mathcal{W}_p=\{v\in\underline{V}(\mathbb{Z}_p)^{\text{rs}}\mid p^2\text{ divides }\Delta_0(v)\}.$$

Let $\mathcal{W}_p^1 \subset \mathcal{W}_p$ denote the set of points v such that either $\pi(v)$ mod p has either more than 1 repeated root or a triple root, or such that v mod p is not regular. (The proof of Proposition 5.4 shows that if v is such an element, then $\Delta_0(v)$ is necessarily divisible by p^2.) Let $\mathcal{W}_p^2 \subset \mathcal{W}_p$ denote the set of points v such that $\pi(v)$ mod p has 1 double root and no other repeated roots, and such that v mod p is regular. Then $\mathcal{W}_p = \mathcal{W}_p^1 \cup \mathcal{W}_p^2$. In order to prove Theorem 6.5 using the method of [Bha] (or [BS15, Theorem 24]), it will suffice to define a map

$$\psi : \underline{G}(\mathbb{Z})\backslash(\underline{V}(\mathbb{Z}) \cap \mathcal{W}_p^2) \to \underline{G}(\mathbb{Z})\backslash(\underline{V}(\mathbb{Z}) \cap \mathcal{W}_p^1)$$

with the following properties:

- $\mathrm{ht} \circ \psi = \psi$.
- The fibres of ψ have cardinality at most 3.

We will construct this map as follows: for any $v \in \mathcal{W}_p^2$, we will define an element $g_{v,p} \in G(\mathbb{Q}_p)$ with the following properties:

- $g_{v,p} \cdot v \in \mathcal{W}_p^1$
- If $k_p \in \underline{G}(\mathbb{Z}_p)$, then $g_{k_p \cdot v,p} = k_p g_{v,p} k_p^{-1}$.

This determines a map $\psi_p : \mathcal{W}_p^1 \to \mathcal{W}_p^2$, by the formula $v \mapsto g_{v,p} \cdot v$. For each $w \in \mathcal{W}_p^2$, define $\Pi_p(w) = \{h_p \in G(\mathbb{Q}_p) \mid h_p^{-1} w = v \in \mathcal{W}_p^2 \text{ and } h = g_{v,p}\}$. We will show that $\Pi_p(w)$ has the following properties:

- If $h_p \in \Pi_p(w)$, then $h_p^{-1} w \in \mathcal{W}_p^2$.
- If $k_p \in \underline{G}(\mathbb{Z}_p)$, then $\Pi_p(k_p w) = k_p \Pi_p(w) k_p^{-1}$.
- $\Pi_p(w)$ has cardinality at most 3.

Before giving the construction, we explain why it implies the existence of a map ψ with the desired properties. Note that $\underline{G}(\mathbb{Z})\backslash\underline{G}(\mathbb{Z}[1/p]) \to \underline{G}(\mathbb{Z}_p)\backslash\underline{G}(\mathbb{Q}_p)$ is bijective (because $\underline{G}$ has class number 1). It follows that given an element $v \in \mathcal{W}_p^2 \cap \underline{V}(\mathbb{Z})$, there is an element $g_v \in (G(\mathbb{Z}_p) \cdot g_{v,p}) \cap G(\mathbb{Q})$, well-defined up to left multiplication by $G(\mathbb{Z})$, and we can define $\psi(v) = g_v \cdot v$. If $\gamma \in \underline{G}(\mathbb{Z})$ then $g_{\gamma \cdot v} = \gamma g_v \gamma^{-1}$, modulo left multiplication by $\underline{G}(\mathbb{Z})$, so we get a well-defined map $\psi : \underline{G}(\mathbb{Z})\backslash(\underline{V}(\mathbb{Z}) \cap \mathcal{W}_p^2) \to \underline{G}(\mathbb{Z})\backslash(\underline{V}(\mathbb{Z}) \cap \mathcal{W}_p^1)$ which by definition satisfies $\mathrm{ht} \circ \psi = \psi$.

To bound the cardinality of the fibres of ψ, note that if $w \in \mathcal{W}_p^1 \cap \underline{V}(\mathbb{Z})$ and $w = \psi(v)$ (modulo the action of $\underline{G}(\mathbb{Z})$) for some $v \in \mathcal{W}_p^2 \cap \underline{V}(\mathbb{Z})$, then by definition $w = g_v \cdot v = k_p g_{v,p} \cdot v$, where $k_p \in \underline{G}(\mathbb{Z}_p)$, hence $k_p^{-1} w = g_{v,p} \cdot v$, hence $g_{v,p} \in \Pi_p(k_p^{-1} w) = k_p^{-1} \Pi_p(w) k_p$. This shows that $g_v \in \Pi_p(w) k_p$, hence $v = g_v^{-1} w \in (G(\mathbb{Z}_p) \Pi_p(w)^{-1} \cap G(\mathbb{Q})) \cdot w$. Again using the class number 1 property of $\underline{G}$, we see that $G(\mathbb{Z}_p) \Pi_p(w)^{-1} \cap G(\mathbb{Q})$ consists of at most 3 $\underline{G}(\mathbb{Z})$-orbits under left multiplication, hence that the fibre of ψ above the $\underline{G}(\mathbb{Z})$-orbit of w indeed has cardinality at most 3.

We now construct the element $g_{v,p}$. We will use similar arguments to those of the proof of Proposition 5.4. Let $v \in \mathcal{W}_p^2$, and let $v_{\mathbb{F}_p}$ denote its reduction modulo p. Let $v_{\mathbb{F}_p} = y_s + y_n$ be its Jordan decomposition. There is a decomposition $\underline{\mathfrak{h}}_{\mathbb{Z}_p} = \underline{\mathfrak{h}}_{0,\mathbb{Z}_p} \oplus \underline{\mathfrak{h}}_{1,\mathbb{Z}_p}$, where $\mathrm{ad}(v)$ acts topologically nilpotently in $\underline{\mathfrak{h}}_{0,\mathbb{Z}_p}$ and invertibly in $\underline{\mathfrak{h}}_{1,\mathbb{Z}_p}$; and moreover, there is a unique closed subgroup $\underline{L} \subset \underline{H}_{\mathbb{Z}_p}$ with Lie algebra $\underline{\mathfrak{h}}_{0,\mathbb{Z}_p}$ and which is smooth with connected fibres over $\mathbb{Z}_p$ (the argument is the same as in the proof of Proposition 5.4). By assumption, y_n is a regular nilpotent element in $\underline{\mathfrak{h}}_{0,\mathbb{F}_p} = \mathfrak{z}_{\underline{\mathfrak{h}}}(y_s)$.

There is an isomorphism $\underline{\mathfrak{h}}_{0,\mathbb{Z}_p}^{\mathrm{der}} \cong \mathfrak{sl}_{3,\mathbb{Z}_p}$ which intertwines $\theta|_{\underline{\mathfrak{h}}_{0,\mathbb{Z}_p}^{\mathrm{der}}}$ with $\zeta \mapsto \mathrm{Ad}(\mathrm{diag}(1,\zeta,\zeta^2))$, and which sends y_n to the element

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

of $\mathfrak{sl}_{3,\mathbb{F}_p}$. (Indeed, there is a unique such isomorphism modulo p, which then lifts by Hensel's lemma to an isomorphism over $\mathbb{Z}_p$.) Similarly, there is a map $\varphi_v : \mathrm{SL}_{3,\mathbb{Z}_p} \to \underline{L}$ which intertwines $\mathrm{Ad}(\mathrm{diag}(1,\zeta,\zeta^2))$ with $\theta_{\underline{L}} = \theta|_{\underline{L}}$ and which is compatible with the above isomorphism on Lie algebras. The map φ_v is uniquely determined up to conjugation by diagonal matrices in $\mathrm{PGL}_3(\mathbb{Z}_p)$; the element $g_{v,p} = \varphi_v(\mathrm{diag}(p,1,p^{-1})) \in \underline{L}(\mathbb{Q}_p)$ is therefore independent of any choices.

To see that this $g_{v,p}$ has the desired properties, let v' denote the projection of v to $\mathfrak{h}_{0,\mathbb{Z}_p}^{\mathrm{der}}$, and note that the image of v' in $\mathfrak{sl}_{3,\mathbb{Z}_p}$ has the form

$$v = \begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix},$$

where $a \equiv b \equiv 1 \bmod p$ and $p^2|c$ (because of our assumption that p^2 divides $\Delta_0(v)$). Thus we have

$$g_{v,p} \cdot v' = \begin{pmatrix} 0 & pa & 0 \\ 0 & 0 & pb \\ c/p^2 & 0 & 0 \end{pmatrix}.$$

The reduction modulo p of $g_{v,p} \cdot v$ is no longer regular, showing that $g_{v,p} \cdot v \in \mathcal{W}_p^1$. This defines the map ψ_p.

We now need to describe the set $\Pi_p(w)$ for $w \in \mathcal{W}_p^1$. Let $w_{\mathbb{F}_p} = z_s + z_n$ be the Jordan decomposition. As before, we get a decomposition $\underline{\mathfrak{h}}_{\mathbb{Z}_p} = \underline{\mathfrak{h}}_{0,\mathbb{Z}_p} \oplus \underline{\mathfrak{h}}_{1,\mathbb{Z}_p}$ where $\mathrm{ad}(w)$ acts topologically nilpotently in $\underline{\mathfrak{h}}_{0,\mathbb{Z}_p}$ and invertibly in $\underline{\mathfrak{h}}_{1,\mathbb{Z}_p}$, and $\underline{\mathfrak{h}}_{0,\mathbb{Z}_p}$ is the Lie algebra of a Levi subgroup $\underline{L} \subset \underline{H}_{\mathbb{Z}_p}$.

Observe that if $w = g_{v,p} \cdot v$ for some $v \in \mathcal{W}_p^2$, then the derived subalgebra of $\mathfrak{z}_{\underline{\mathfrak{h}}}(z_s)$ is isomorphic to $\mathfrak{sl}_{3,\mathbb{F}_p}$ (i.e. is split) and its grading is conjugate to the $\mathbb{Z}/3\mathbb{Z}$-grading given by the formula $\zeta \mapsto \mathrm{Ad}(\mathrm{diag}(1,\zeta,\zeta^2))$ (in fact, it coincides with the derived subalgebra of $\mathfrak{z}_{\underline{\mathfrak{h}}}(y_s)$ in the above discussion). We can therefore assume without loss of generality that $\mathfrak{z}_{\underline{\mathfrak{h}}}(z_s)$ is split and has a grading of this form (otherwise $\Pi_p(w)$ is empty).

If we fix an isomorphism between $\mathfrak{z}_{\underline{\mathfrak{h}}}(z_s)^{\mathrm{der}}$ and $\mathfrak{sl}_{3,\mathbb{F}_p}$ which identifies $\theta|_{\mathfrak{z}_{\underline{\mathfrak{h}}}(z_s)^{\mathrm{der}}}$ with the $\mathbb{Z}/3\mathbb{Z}$-grading $\zeta \mapsto \mathrm{Ad}(\mathrm{diag}(1,\zeta,\zeta^2))$, then there is a compatible morphism $\mathrm{SL}_{3,\mathbb{Z}_p} \to \underline{L}$, uniquely determined up to conjugation by diagonal elements of $\mathrm{PGL}_3(\mathbb{Z}_p)$, and we get an element $h_p \in H(\mathbb{Q}_p)$, image of $\mathrm{diag}(p^{-1},1,p) \in \mathrm{SL}_3(\mathbb{Q}_p)$.

There are three possible choices of isomorphism between $\mathfrak{z}_{\underline{\mathfrak{h}}}(z_s)^{\mathrm{der}}$ and $\mathfrak{sl}_{3,\mathbb{F}_p}$, up to $\mathrm{SL}_{3,\mathbb{F}_p}^{\theta}$-conjugacy, so we get three elements $h_p \in \underline{L}(\mathbb{Q}_p)$. The set $\Pi_p(w)$ is contained in the set of elements h_p constructed this way, showing that $\Pi_p(w)$ has cardinality at most 3. The other claimed properties of the set $\Pi_p(w)$ follow from the definition. We have therefore completed the proof of Theorem 6.5.

7 The main theorem

We can now prove the theorems stated in the introduction. We begin by re-establishing notation. Thus $\mathscr{E}$ denotes the set of polynomials $f(x) = x^5 + c_{12}x^3 + c_{18}x^2 + c_{24}x + c_{30} \in \mathbb{Z}[x]$ of non-zero discriminant, and $\mathscr{E}_{\mathrm{min}} \subset \mathscr{E}$ denotes the set of polynomials $f(x)$ not of the form $n \cdot g = n^{10}g(x/n^2) \in \mathscr{E}$ for any $g \in \mathscr{E}$ and integer $n \geq 2$. If $f \in \mathscr{E}$, then we define the height of f by the formula

$$\mathrm{ht}(f) = \sup_i |c_i|^{120/i}.$$

Thus for any $a > 0$, the set $\{f \in \mathscr{E} \mid \mathrm{ht}(f) < a\}$ is finite. We recall that the set $\mathscr{E}_{\min}$ is in bijection with the set of isomorphism classes of pairs $(\mathscr{C}, \mathscr{P})$ where $\mathscr{C}$ is a (smooth, projective, connected) genus-2 curve over $\mathbb{Q}$ and $\mathscr{P} \in \mathscr{C}(\mathbb{Q})$ is a marked Weierstrass point, via the map which takes $f \in \mathscr{E}$ to the projective completion of the affine curve $\mathscr{C}_f^0 : y^2 = f(x)$.

Theorem 7.1. *We have*

$$\lim_{a \to \infty} \frac{\sum_{f \in \mathscr{E}_{min}, \mathrm{ht}(f) < a} |\operatorname{Sel}_3(\mathscr{J}_f)|}{|\{f \in \mathscr{E}_{min} \mid \mathrm{ht}(f) < a\}|} = 4.$$

We first prove a 'local' result. Let $\underline{G}, \underline{V}$ be the group and representation defined in §4, and let $N \geq 1$ be the integer of §4.5; thus our main constructions make sense over $\mathbb{Z}[1/N]$. If p is a prime, then we write $\mathscr{E}_p$ for the set of polynomials $f(x) = x^5 + c_{12}x^3 + c_{18}x^2 + c_{24}x + c_{30} \in \mathbb{Z}_p[x]$ of non-zero discriminant, and $\mathscr{E}_{p,\min} \subset \mathscr{E}_p$ for the set of polynomials not of the form $p^{10}g(x/p^2)$ for any polynomial $g(x) \in \mathscr{E}_p$.

Proposition 7.2. *Let $f_0(x) \in \mathscr{E}_{min}$. Then we can find for each prime $p \leq N$ an open compact neighbourhood W_p of $f_0(x)$ in $\mathscr{E}_p$ such that the following condition holds. Let $\mathscr{E}_W = \mathscr{E} \cap (\prod_{p \leq N} W_p)$, and let $\mathscr{E}_{W,min} = \mathscr{E}_W \cap \mathscr{E}_{min}$. Then we have*

$$\lim_{a \to \infty} \frac{\sum_{f \in \mathscr{E}_{W,min}, \mathrm{ht}(f) < a} |\operatorname{Sel}_3(\mathscr{J}_f)|}{|\{f \in \mathscr{E}_{W,min} \mid \mathrm{ht}(f) < a\}|} = 4.$$

(The intersection $\mathscr{E} \cap (\prod_{p \leq N} W_p))$ is taken in $\prod_{p \leq N} \mathscr{E}_p$, where we view $\mathscr{E}$ as a subset via the diagonal embedding.)

Proof. We choose the sets W_p for $p \leq N$, together with integers $n_p \geq 0$, so that the conclusion of Corollary 5.8 holds. If $p > N$, let $W_p = \mathscr{E}_{p,\min}$ and $n_p = 0$. Let $M = \prod_p p^{n_p}$. After possibly shrinking the W_p with $p \leq N$, we can assume that the W_p with $p \leq N$ satisfy $W_p \subset \mathscr{E}_{p,\min}$.

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

$$w(v) = \begin{cases} \left(\sum_{v' \in \underline{G}(\mathbb{Z}) \backslash (\underline{G}(\mathbb{Q}) \cdot v \cap \underline{V}(\mathbb{Z}))} \frac{|Z_{\underline{G}}(v')(\mathbb{Q})|}{|Z_{\underline{G}}(v')(\mathbb{Z})|}\right)^{-1} & \text{if } f \in M \cdot \mathscr{E}_{W,\min} \text{ and } \underline{G}(\mathbb{Q}) \cdot v' \in \eta_f(\operatorname{Sel}_3(\mathscr{J}_f)) \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$\sum_{\substack{f \in \mathscr{E}_{W,\min} \\ \mathrm{ht}(f) < a}} \frac{|\operatorname{Sel}_3(\mathscr{J}_f)| - 1}{|\mathscr{J}_f[3](\mathbb{Q})|} = \sum_{\substack{v \in \underline{G}(\mathbb{Z}) \backslash \underline{V}(\mathbb{Z})^{\mathrm{irr}} \\ \mathrm{ht}(v) < M^{120} a}} w(v).$$

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

$$w_p(v) = \begin{cases} \left(\sum_{v' \in \underline{G}(\mathbb{Z}_p) \backslash (\underline{G}(\mathbb{Q}_p) \cdot v \cap \underline{V}(\mathbb{Z}_p)} \frac{|Z_{\underline{G}}(v')(\mathbb{Q}_p)|}{|Z_{\underline{G}}(v')(\mathbb{Z}_p)|}\right)^{-1} & \text{if } f \in p^{n_p} W_p \text{ and } \underline{G}(\mathbb{Q}_p) \cdot v' \in \eta_f(\mathscr{J}_f(\mathbb{Q}_p)) \\ 0 & \text{otherwise.} \end{cases}$$

Then for any $v \in \underline{V}(\mathbb{Z})$, we have $w(v) = \prod_p w_p(v)$, and the function w satisfies the conditions described before the statement of Theorem 6.5.

Let $W_0 \in \mathbb{Q}^\times$ be the constant of Proposition 4.17. That proposition implies that for any prime p, we have the formula

$$\int_{v \in \underline{V}(\mathbb{Z}_p)} w_p(v)\, dv = |W_0/9|_p p^{-\dim_{\mathbb{Q}} V \cdot n_p} \operatorname{vol}(W_p) \operatorname{vol}(\underline{G}(\mathbb{Z}_p)),$$

where we have used the equality $|\mathscr{J}_f(\mathbb{Q}_p)/3\mathscr{J}_f(\mathbb{Q}_p)| = |1/9|_p |Z_{\underline{G}}(\sigma(f))(\mathbb{Q}_p)|$ for any $f \in \mathscr{E}_p$. By Theorem 6.5 and Proposition 4.16, we therefore have

$$\begin{aligned}\lim_{a \to \infty} \sum_{\substack{f \in \mathscr{E}_{W,\min} \\ \mathrm{ht}(f) < a}} \frac{|\operatorname{Sel}_3(\mathscr{J}_f)| - 1}{a^{7/10} |\mathscr{J}_f[3](\mathbb{Q})|} &= \frac{M^{120}}{9} |W_0|_\infty \operatorname{vol}(\underline{G}(\mathbb{Z}) \backslash \underline{G}(\mathbb{R})) \prod_p |W_0/9|_p p^{-\dim V \cdot n_p} \operatorname{vol}(W_p) \operatorname{vol}(\underline{G}(\mathbb{Z}_p)) \\ &= 3 \prod_p \operatorname{vol}(W_p).\end{aligned}$$

On the other hand, we have

$$\lim_{a \to \infty} \frac{|\{f \in \mathscr{E}_{W,\min} \mid \mathrm{ht}(f) < a\}|}{a^{7/10}} = \prod_p \operatorname{vol}(W_p).$$

At this point we have proved that

$$\lim_{a \to \infty} \left(\sum_{\substack{f \in \mathscr{E}_{W,\min} \\ \mathrm{ht}(f) < a}} \frac{|\operatorname{Sel}_3(\mathscr{J}_f)| - 1}{\mathscr{J}_f[3](\mathbb{Q})|} \right) (|\{f \in \mathscr{E}_{W,\min} \mid \mathrm{ht}(f) < a\}|)^{-1} = 3.$$

It remains to eliminate the appearance of the term $|\mathscr{J}_f[3](\mathbb{Q})|$. This can be done by combining Proposition 6.4 and Theorem 6.1. □

To deduce Theorem 7.1 from Proposition 7.2, we choose for each $i \geq 1$ sets $W_{p,i}$ ($p \leq N$) giving a countable partition $\mathscr{E}_{\min} = \mathscr{E}_{W_1,\min} \sqcup \mathscr{E}_{W_2,\min} \sqcup \mathscr{E}_{W_3,\min} \sqcup \dots$. We will show that for all $\epsilon > 0$, there exists $k \geq 1$ such that

$$\limsup_{a \to \infty} \frac{\sum_{f \in \sqcup_{i \geq k} \mathscr{E}_{W_i,\min}, \mathrm{ht}(f) < a} |\operatorname{Sel}_3(\mathscr{J}_f)| - 1}{|\{f \in \mathscr{E}_{W,\min} \mid \mathrm{ht}(f) < a\}|} < \epsilon.$$

Combined with Proposition 7.2, which applies to each set $\mathscr{E}_{W_i,\min}$ taken individually, this will imply the desired result. For each $f \in \mathscr{E}$, let

$$\operatorname{Sel}_3(\mathscr{J}_f)^r = \ker(\operatorname{Sel}_3(\mathscr{J}_f) \to \prod_{p \leq N} \mathscr{J}_f(\mathbb{Q}_p)/3\mathscr{J}_f(\mathbb{Q}_p)).$$

Then there exists an integer $N_0 \geq 1$, depending only on N, such that for any $f \in \mathscr{E}$, $|\operatorname{Sel}_3(\mathscr{J}_f)| \leq N_0 |\operatorname{Sel}_3(\mathscr{J}_f)^r|$. It will therefore suffice to show that for all $\epsilon > 0$, there exists $k \geq 1$ such that

$$\limsup_{a \to \infty} \frac{\sum_{f \in \sqcup_{i \geq k} \mathscr{E}_{W_i,\min}, \mathrm{ht}(f) < a} |\operatorname{Sel}_3(\mathscr{J}_f)^r| - 1}{|\{f \in \mathscr{E}_{W,\min} \mid \mathrm{ht}(f) < a\}|} < \epsilon.$$

Fix $k \geq 1$ and let $\mathscr{E}_k = \sqcup_{i \geq k} \mathscr{E}_{W_i,\min}$. We now use that for any $f \in \underline{B}(\mathbb{Z})$, $\sigma(N \cdot f) \in \underline{V}(\mathbb{Z})$ (see §4.5). It follows that we have

$$\sum_{f \in \mathscr{E}_k, \mathrm{ht}(f) < a} \frac{|\operatorname{Sel}_3(\mathscr{J}_f)^r| - 1}{|\mathscr{J}_f[3](\mathbb{Q})|} = \sum_{\substack{v \in \underline{G}(\mathbb{Z}) \backslash \underline{V}(\mathbb{Z})^{\mathrm{irr}} \\ \mathrm{ht}(v) < N^{120} a}} w^r(v),$$

where the weight $w^r(v)$ is defined in the formula

$$w^r(v) = \begin{cases} \left(\sum_{v' \in \underline{G}(\mathbb{Z}) \backslash (\underline{G}(\mathbb{Q}) \cdot v \cap \underline{V}(\mathbb{Z}))} \frac{|Z_{\underline{G}}(v')(\mathbb{Q})|}{|Z_{\underline{G}}(v')(\mathbb{Z})|} \right)^{-1} & \text{if } f \in N \cdot \mathscr{E}_k \text{ and } G(\mathbb{Q}) \cdot v' \in \eta_f(\operatorname{Sel}_3(\mathscr{J}_f)^r) \\ 0 & \text{otherwise.} \end{cases}$$

Running through the same argument as in the proof of Proposition 7.2, we get

$$\limsup_{a\to\infty}\frac{\sum_{f\in\mathscr{E}_k,\mathrm{ht}(f)<a}|\operatorname{Sel}_3(\mathscr{J}_f)^r|-1}{a^{7/10}|\mathscr{J}_f[3](\mathbb{Q})|}\leq 3\prod_{p\leq N}\operatorname{vol}(\sqcup_{i\geq k}W_{p,i}),$$

which becomes arbitrarily small as $k\to\infty$. This completes the proof of Theorem 7.1.

Remark 7.3. Using Theorem 6.5 and [BG13, Theorem 44], one can prove the analogue of Theorem 7.1 for any 'large' subset of $\mathscr{E}_{\min}$, where 'large' has the same meaning as in [BG13, §11]; this includes in particular any subset defined by finitely many congruence conditions on the cofficients of $f(x)=x^5+c_{12}x^3+c_{18}x^2+c_{24}x+c_{30}$.

Our final result (Theorem 1.2 of the introduction) follows readily from the above techniques and from the work of Poonen–Stoll:

Theorem 7.4. *We have*

$$\liminf_{a\to\infty}\frac{|\{f\in\mathscr{E}_{min}\mid \mathrm{ht}(f)<a,|\mathscr{C}_f(\mathbb{Q})|=1\}|}{|\{f\in\mathscr{E}_{min}\mid \mathrm{ht}(f)<a\}|}>0.$$

Proof. According to [PS14, Remark 10.5], this follows if one can establish property $\mathrm{Eq}_2(3)$ of *op. cit.*, which asserts that after fixing a 'trivializing congruence class' $U_3\subset\mathscr{E}_{3,\min}$ in which the groups $\mathscr{J}_f(\mathbb{Q}_3)/3\mathscr{J}_f(\mathbb{Q}_3)=F$ are independent of $f\in U_3$, the images $x|_3$ of 3-Selmer elements $x\in\operatorname{Sel}_3(\mathscr{J}_f)$ in the local groups $\mathscr{J}_f(\mathbb{Q}_3)/3\mathscr{J}_f(\mathbb{Q}_3)=F$ are equidistributed for $f\in\mathscr{E}_{\min}\cap U_3$. This can be proved by a small modification of the proof of Theorem 7.1, analogous to the proof of [BG13, Theorem 47]. We omit the details. □

References

[BFT14] Nils Bruin, E. Victor Flynn, and Damiano Testa. Descent via $(3,3)$-isogeny on Jacobians of genus 2 curves. *Acta Arith.*, 165(3):201–223, 2014.

[BG13] Manjul Bhargava and Benedict H. Gross. The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point. In *Automorphic representations and L-functions*, volume 22 of *Tata Inst. Fundam. Res. Stud. Math.*, pages 23–91. Tata Inst. Fund. Res., Mumbai, 2013.

[Bha] Manjul Bhargava. The geometric sieve and the density of squarefree values of invariant polynomials. Preprint. Available at `https://arxiv.org/abs/1402.0031`.

[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.

[BS15] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math. (2)*, 181(2):587–621, 2015.

[Con14] Brian Conrad. Reductive group schemes. In *Autour des schémas en groupes. Vol. I*, volume 42/43 of *Panor. Synthèses*, pages 93–444. Soc. Math. France, Paris, 2014.

[CTS79] J.-L. Colliot-Thélène and J.-J. Sansuc. Fibrés quadratiques et composantes connexes réelles. *Math. Ann.*, 244(2):105–134, 1979.

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

[Gro68] Alexander Grothendieck. Le groupe de Brauer. II. Théorie cohomologique. In *Dix exposés sur la cohomologie des schémas*, volume 3 of *Adv. Stud. Pure Math.*, pages 67–87. North-Holland, Amsterdam, 1968.

[Gro97] Benedict H. Gross. On the motive of G and the principal homomorphism $\mathrm{SL}_2 \to \widehat{G}$. *Asian J. Math.*, 1(1):208–213, 1997.

[Hin91] V. Hinich. On Brieskorn's theorem. *Israel J. Math.*, 76(1-2):153–160, 1991.

[HLHN14] Q. P. H, V. B. Lê Hùng, and B. C. Ngô. Average size of 2-Selmer groups of elliptic curves over function fields. *Math. Res. Lett.*, 21(6):1305–1339, 2014.

[Lan66] R. P. Langlands. The volume of the fundamental domain for some arithmetical subgroups of Chevalley groups. In *Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965)*, pages 143–148. Amer. Math. Soc., Providence, R.I., 1966.

[Lep85] J. Lepowsky. Calculus of twisted vertex operators. *Proc. Nat. Acad. Sci. U.S.A.*, 82(24):8295–8299, 1985.

[Lev09] Paul Levy. Vinberg's θ-groups in positive characteristic and Kostant-Weierstrass slices. *Transform. Groups*, 14(2):417–461, 2009.

[Mir81] Rick Miranda. The moduli of Weierstrass fibrations over $\mathbf{P}^1$. *Math. Ann.*, 255(3):379–394, 1981.

[MP12] Davesh Maulik and Bjorn Poonen. Néron-Severi groups under specialization. *Duke Math. J.*, 161(11):2167–2206, 2012.

[Ngô 10] Bao Châu Ngô . Le lemme fondamental pour les algèbres de Lie. *Publ. Math. Inst. Hautes Études Sci.*, (111):1–169, 2010.

[Nis84] Yevsey A. Nisnevich. Espaces homogènes principaux rationnellement triviaux et arithmétique des schémas en groupes réductifs sur les anneaux de Dedekind. *C. R. Acad. Sci. Paris Sér. I Math.*, 299(1):5–8, 1984.

[Ono65] Takashi Ono. On the relative theory of Tamagawa numbers. *Ann. of Math. (2)*, 82:88–111, 1965.

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

[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.

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

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

[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.

[Rom] Beth Romano. On elliptic gradings of simply laced Lie algebras. In preparation.

[RS] Eric Rains and Steven Sam. Invariant theory of $\wedge^3(9)$ and genus 2 curves. Preprint. Available at `https://arxiv.org/abs/1702.04840`.

[RTa] Beth Romano and Jack. A. Thorne. On the arithmetic of simple singularities of type E. To appear in Research in Number Theory.

[RTb] Beth Romano and Jack A. Thorne. On the arithmetic of simple singularities of type E, II. In preparation.

[Ser12] Jean-Pierre Serre. *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL, 2012.

[SGA70] *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*. Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 152. Springer-Verlag, Berlin-New York, 1970.

[Shi10] Tetsuji Shioda. Gröbner basis, Mordell-Weil lattices and deformation of singularities. I. *Proc. Japan Acad. Ser. A Math. Sci.*, 86(2):21–26, 2010.

[Slo80] Peter Slodowy. *Simple singularities and simple algebraic groups*, volume 815 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[SS10] Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. In *Algebraic geometry in East Asia—Seoul 2008*, volume 60 of *Adv. Stud. Pure Math.*, pages 51–160. Math. Soc. Japan, Tokyo, 2010.

[Sta18] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu`, 2018.

[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.

[Vas16] Adrian Vasiu. Extension theorems for reductive group schemes. *Algebra Number Theory*, 10(1):89–115, 2016.

[VÈ78] È. B. Vinberg and A. G. Èlašvili. A classification of the three-vectors of nine-dimensional space. *Trudy Sem. Vektor. Tenzor. Anal.*, 18:197–233, 1978.

Beth Romano `blr24@dpmms.cam.ac.uk`
Department of Pure Mathematics and Mathematical Statistics, Wilberforce Road, Cambridge, CB3 0WB, UK

Jack A. Thorne `thorne@dpmms.cam.ac.uk`
Department of Pure Mathematics and Mathematical Statistics, Wilberforce Road, Cambridge, CB3 0WB, UK