On the average number of 2-Selmer elements of elliptic curves over $\mathbb{F}_q(X)$ with two marked points

Jack A. Thorne*

July 4, 2016

Abstract

We consider elliptic curves over global fields of positive characteristic with two distinct marked non-trivial rational points. Restricting to a certain subfamily of the universal one, we show that the average size of the 2-Selmer groups of these curves exists, in a natural sense, and equals 12. Along the way, we consider a map from these 2-Selmer groups to the moduli space of G-torsors over an algebraic curve, where G is isogenous to SL_2^4, and show that the images of 2-Selmer elements under this map become equidistributed in the limit.

Contents

1 Introduction

Let K be a global field. To any elliptic curve E/K and integer $n \geq 1$ not dividing the characteristic of K, one can attach the n-Selmer group

$$\mathrm{Sel}_n(E) = \ker(H^1(K, E[n]) \to \prod_v H^1(K_v, E)).$$

The cohomology groups here are Galois cohomology, and the product is over the set of all places v of the global field K. The n-Selmer group then fits into a short exact sequence of finite abelian groups

$$0 \longrightarrow E(K)/nE(K) \longrightarrow \mathrm{Sel}_n(E) \longrightarrow \mathrm{TS}(K, E)[n] \longrightarrow 0.$$

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

Since it is often easier to compute $\mathrm{Sel}_n(E)$ than the group $E(K)/nE(K)$, this provides a useful tool for studying the group of rational points $E(K)$. However, computing $\mathrm{Sel}_n(E)$ for reasonably complicated curves E, even when an algorithm is known, can require a large amount of effort. For these reasons, it is of interest to understand the behaviour of the groups $\mathrm{Sel}_n(E)$ on average. Recent years have seen striking progress in problems of this type; for some work of particular relevance to this paper, we refer the reader to any of the papers [dJ02, BS15, HLHN14].

In this paper, we prove new results about the average size of the 2-Selmer group of elliptic curves over global fields of positive characteristic. Such a field is, by definition, the function field $K = \mathbb{F}_q(X)$ of an algebraic curve over a finite field. We will consider the universal family of elliptic curves with two marked rational points and calculate the average size of the 2-Selmer groups of the curves in this family satisfying certain conditions. We will accomplish this by relating these 2-Selmer groups to the invariant theory of a representation constructed and studied in [Tho13], and then counting sections of certain associated vector bundles on X.

In order to state our main theorems precisely, we must introduce some notation. If E/K is an elliptic curve, we can associate its relatively minimal regular model $p_E : \mathcal{E} \to X$ with identity section $O : X \to \mathcal{E}$. The isomorphism class of the line bundle $\mathcal{L}_E = (R^1 p_{E,*}\mathcal{O}_{\mathcal{E}})^{\otimes -1}$ is an invariant of E, and there are only finitely many elliptic curves over K up to isomorphism with a given $\mathcal{L}_E$, this number tending to infinity as $\deg \mathcal{L}_E \to \infty$.

If $\mathcal{L}$ is a line bundle on X, then we write $\mathcal{X}_{\mathcal{L}}$ for the finite set of isomorphism classes of triples (E, P, Q) as follows:

1. E/K is an elliptic curve such that $\mathcal{L}_E \cong \mathcal{L}^{\otimes 2}$ and the fibres of p_E are all of type I_0 or I_1.
2. $P, Q \in E(K)$ are distinct non-trivial rational points such that sections $\mathcal{O}, \mathcal{P}, \mathcal{Q} : X \to \mathcal{E}$ associated to the origin of E and the points P, Q, respectively, do not intersect.

Provided that the characteristic of K does not divide 6, an elliptic curve E with two non-trivial marked points can be represented by an equation

$$Y(XY + 2q_4Z^2) = X^3 + p_2X^2Z + p_4XZ^2 + p_6Z^3, \tag{1.1}$$

which sends the marked points, together with the origin, to the line at infinity. The curves in $\mathcal{X}_{\mathcal{L}}$ are exactly those for which the discriminant $\Delta(p_2, \dots, p_6)$ of this equation vanishes to order at most 1 everywhere, when viewed as a section of $H^0(X, \mathcal{L}^{\otimes 24})$; see §2 below.

We can now state our first main theorem.

Theorem 1.1. *Suppose that* $\mathrm{char}\, K > 19$. *The limit*

$$\lim_{\deg \mathcal{L} \to \infty} \sum_{(E,P,Q) \in \mathcal{X}_{\mathcal{L}}} \frac{|\,\mathrm{Sel}_2(E)| \times |\,\mathrm{Aut}(E, P, Q)|^{-1} \times |E(K)[2]|^{-1}}{|\mathcal{X}_{\mathcal{L}}|}$$

exists and equals 12.

Remark 1.2.

1. This result is what one might expect given known results about the 2-Selmer groups of elliptic curves without marked points: for the curves in our family, there is a 'trivial subgroup' $A_{(E,P,Q)} \subset \mathrm{Sel}_2(E)$, generated by the classes of the points P, Q, and which generically has size 4. It follows that the remainder $\mathrm{Sel}_2(E)/A_{(E,P,Q)}$ should have average size 3.
2. We believe that the weighting of Selmer elements by automorphisms is natural; similarly for the weighting by K-rational 2-torsion points (which can be thought of as K-rational automorphisms of the trivial 2-covering $[2] : E \to E$). In fact, the contribution of $E(K)[2]$ can be suppressed: for the curves we consider, the groups $E(K)[\mathrm{tors}]$ are trivial (because they inject into the product of fibral component groups; but these component groups are all trivial, by hypothesis).
3. The restriction on the characteristic arises because we need to apply Jacobson–Morozov style results to the Lie algebra over $\mathbb{F}_q$ of type D_4, for example in the construction of the Kostant section (see Proposition 3.3 below). It may be possible to relax this restriction slightly.

Let $G = (\mathrm{SO}_4 \times \mathrm{SO}_4)/\Delta(\mu_2)$, where SO_4 is the split special orthogonal group over $\mathbb{F}_q$, and μ_2 is its centre. A key role in our proof of Theorem 1.1 is played by a family of canonically defined invariant maps

$$\mathrm{inv} = \mathrm{inv}_{(E,P,Q)} : \mathrm{Sel}_2(E) \to G(K)\backslash G(\mathbb{A}_K)/\prod_v G(\mathcal{O}_{K_v}). \tag{1.2}$$

In fact, our consideration of these maps leads to the following generalization of Theorem 1.1, which is a kind of equidistribution result:

Theorem 1.3. *Suppose that* $\mathrm{char}\, K > 19$. *Let* $f : G(K)\backslash G(\mathbb{A}_K)/\prod_v G(\mathcal{O}_{K_v}) \to \mathbb{R}$ *be a bounded function, and let* τ_G *denote the Tamagawa measure on* $G(K)\backslash G(\mathbb{A}_K)/\prod_v G(\mathcal{O}_{K_v})$. *Then the limit*

$$\lim_{\deg \mathcal{L}\to\infty} \sum_{(E,P,Q)\in\mathcal{X}_\mathcal{L}} \sum_{x\in \mathrm{Sel}_2(E)-A_{(E,P,Q)}} \frac{f(\mathrm{inv}\, x) \times |\,\mathrm{Aut}(E,P,Q)|^{-1} \times |E(K)[2]|^{-1}}{|\mathcal{X}_\mathcal{L}|}$$

exists and equals $\int_{g\in G(K)\backslash G(\mathbb{A}_K)/\prod_v G(\mathcal{O}_{K_v})} f(g)\, d\tau_G$.

Taking $f = 1$ to be the constant function, we recover Theorem 1.1 (after accounting for the average number of elements in the group $A_{(E,P,Q)}$, which is a simple task). In general, Theorem 1.3 can be interpreted as saying that the invariants of non-trivial Selmer elements of elliptic curves in $\mathcal{X}_\mathcal{L}$ become equidistributed in $G(K)\backslash G(\mathbb{A}_K)/\prod_v G(\mathcal{O}_{K_v})$ as $\deg \mathcal{L} \to \infty$. It would be very interesting to get a better understanding of this phenomenon, which persists in other situations (for example, in the case of 2-Selmer groups of elliptic curves without marked points, in which case G should be replaced by the group PGL_2). Can one relate Theorem 1.3 to existing conjectures about statistics of ranks of 2-Selmer groups, as in [PR12]?

The proofs of Theorem 1.1 and Theorem 1.3 rely on a connection between the universal family of elliptic curves (E, P, Q) with two marked points and a certain representation (G, V) which was analyzed in [Tho13] from the point of view of Vinberg theory, and which is constructed using the adjoint group over $\mathbb{F}_q$ of type D_4; the link here exists because the family of curves (1.1) is a miniversal deformation of the simple curve singularity of type D_4. This connection reduces the problem of counting elements of Selmer groups to that of counting orbits in certain representations of V. Using the map inv described above, we reduce this to a problem of counting sections of certain vector bundles over X.

An interesting point in our proof is the calculation of the invariants of trivial elements of the 2-Selmer group. We can describe these explicitly using the principal cocharacter of the ambient group H of type D_4 (inside which the pair (G, V) is constructed); see Lemma 5.7. This gives a quantitative version of the intuitive statement that 'trivial elements appear far into the cusp of V'.

Aside from the intrinsic interest of results like Theorem 1.1, one of our motivations was to understand how the techniques of Bhargava–Shankar for counting integral orbits in coregular representations (see e.g. [BS15]) can be transferred to this function field setting. Instead of reduction theory we use the Harder–Narasimhan (or Shatz) stratification of the space $G(K)\backslash G(\mathbb{A}_K)/\prod_v G(\mathcal{O}_{K_v})$ by the canonical reduction of G-torsors. After some reinterpretation, we find that the methods of Bhargava–Shankar are still very effective. In particular, the technique of 'cutting off the cusp' works in a very similar way (compare e.g. [Tho15, §5] and the proof of Theorem 5.9 below).

We have restricted ourselves to pointed curves (E, P, Q) satisfying conditions 1. and 2. above, since this simplifies our analysis of the invariant map (1.2). From the point of view of the invariant theory of (G, V), it corresponds to restricting to orbits with square-free discriminant Δ. It would be possible to remove this restriction, at the cost of a more detailed analysis of integral orbits; for example, the invariant map would become multi-valued, since the uniqueness of integral representatives (see Theorem 5.5) does not hold in general. Compare [BS15, §3.2] for the kinds of problems that arise.

We now describe the structure of this paper. In §2, we introduce the universal family of elliptic curves with two marked points, and study their projective embeddings and integral models. In §3, we introduce the representation (G, V) and describe its invariant theory. We also introduce the discriminant Δ and the important notion of trivial orbits in $G(K)\backslash V(K)$; these are the orbits that will eventually correspond to elements of the trivial subgroup $A_{(E,P,Q)}$ of the 2-Selmer group. We also give some useful criteria for elements in $V(K)$ either to have vanishing discriminant, or to lie in a trivial orbit. In §4, we describe the

Harder–Narasimhan stratification of $G(K)\backslash G(\mathbb{A}_K)/\prod_v G(\mathcal{O}_{K_v})$ (at the level of points only) and the relation between summing over strata and integrating over the adelic points of parabolic subgroups of G. Finally, in §5, we describe the relation between the pair (G, V) and the family of curves (1.1), and exploit this to prove our main theorems Theorem 5.9 and Theorem 5.11.

1.1 Notation

In this paper, we will generally use the letter K to denote a global field of positive characteristic, therefore the function field $\mathbb{F}_q(X)$ of a smooth, projective, geometrically connected curve X over $\mathbb{F}_q$. If v is a place of K, then we will write K_v for the completion of K at v, $\mathcal{O}_{K_v}$ for the ring of integers of v, and $\varpi_v \in \mathcal{O}_{K_v}$ for a choice of uniformizer. We will write $\mathrm{ord}_{K_v} : K_v^\times \to \mathbb{Z}$ for the corresponding normalized discrete valuation, $k(v) = \mathcal{O}_{K_v}/(\varpi_v)$ for the residue field, and $q_v = |k(v)|$ for the cardinality of the residue field. We will generally fix a separable closure K^s/K and separable closures K_v^s/K_v, together with compatible embeddings $K^s \hookrightarrow K_v^s$. We then define $\Gamma_K = \mathrm{Gal}(K^s/K)$ and $\Gamma_{K_v} = \mathrm{Gal}(K_v^s/K_v)$; there are canonical maps $\Gamma_{K_v} \to \Gamma_K$. We let $\kappa(v)$ denote the residue field of K_v^s, which is an algebraic closure of $k(v)$. We write $I_{K_v} \subset \Gamma_{K_v}$ for the inertia group.

We write $\widehat{\mathcal{O}}_K = \prod_v \mathcal{O}_{K_v}$ for the maximal compact subring of the adele ring $\mathbb{A}_K = \prod_v' K_v$. We will write $|\cdot|_v : K_v^\times \to \mathbb{R}_{>0}$ for the valuation satisfying $|\varpi_v| = q_v^{-1}$, and $\|\cdot\| = \prod_v |\cdot|_v : \mathbb{A}_K^\times \to \mathbb{R}_{>0}$ for the adelic norm; it satisfies the product formula $\|\gamma\| = 1$ for all $\gamma \in K^\times$. If Y is a integral smooth scheme over K_v, and ω_Y is a non-vanishing differential form of top degree on Y, then we write $|\omega_Y|_v$ for the corresponding measure on $Y(K_v)$.

If S is a scheme, a reductive group over S is a smooth group scheme $G \to S$ with geometric fibres which are (connected and) reductive. If G is a group scheme over S which acts on another scheme $X \to S$, then for $x \in X(S)$ we write $Z_G(x)$ for the scheme-theoretic stabilizer of x. If $Z \subset X$ is a closed subscheme, then we write $Z_G(Z)$ and $N_G(Z)$ for the scheme-theoretic centralizers and normalizers of Z. If G is a reductive group over a field then we write $Z_0(G)$ for the identity component of the centre Z_G of G. Lie algebras will be denoted using gothic letters (e.g. $\mathrm{Lie}\, G = \mathfrak{g}$).

If G is a smooth group scheme over $\mathbb{F}_q$, and $K = \mathbb{F}_q(X)$, then we write μ_G for the right-invariant Haar measure on $G(\mathbb{A}_K)$ which gives measure 1 to the open compact subgroup $G(\widehat{\mathcal{O}}_K) \subset G(\mathbb{A}_K)$. If G is semisimple, then we will write τ_G for the Tamagawa measure on $G(\mathbb{A}_K)$; these two measures are related by the formula (see [Wei95]):

$$\tau_G = q^{\dim G(1-g_X)} \left[\prod_v \int_{G(\mathcal{O}_{K_v})} |\omega_G|_v \right] \mu_G,$$

where ω_G is a non-vanishing invariant differential form of top degree on G (hence defined over $\mathbb{F}_q$) and g_X denotes the genus of X.

2 Elliptic curves with two marked points

Let k be a field of characteristic not dividing 6. We consider tuples (E, P, Q), where E is an elliptic curve over k (with origin point $O \in E(k)$) and $P, Q \in E(k)$ are distinct, non-trivial marked points.

Such pointed curves have a distinguished class of plane embeddings which are different to the usual Weierstrass embeddings, being defined by the linear system associated to the degree 3 divisor $O + P + Q$. Indeed, this linear system is very ample, so embeds E into the projective plane $\mathbb{P}_k^2$ in such a way that the points O, P, Q are collinear. If X, Y, Z are the co-ordinates on $\mathbb{P}_k^2$ then we can assume, after a projective transformation, that O, P, Q are given respectively by $[0:1:0]$, $[1:1:0]$, and $[-1:1:0]$. The co-ordinate system is then uniquely determined up to substitutions of the form $X \rightsquigarrow aX + bZ$ and $Y \rightsquigarrow aY + cZ$ with $a \in k^\times$, $b, c \in k$. It is easy to check that there is a unique such substitution with $a = 1$ leading to an equation of the form

$$Y(XY + 2q_4 Z^2) = X^3 + p_2 X^2 Z + p_4 X Z^2 + p_6 Z^3. \tag{2.1}$$

We define the associated polynomial $f(x) = x^4 + p_2 x^2 + p_4 x + p_6 + q_4^2$, and $\Delta(p_2, p_4, q_4, p_6) = \mathrm{disc}\, f \in \mathbb{Z}[p_2, \ldots, p_6]$. The following is elementary:

Lemma 2.1. *Let $p_2, p_4, q_4, p_6 \in k$, and let E be the plane curve over k defined by the equation (2.1). Then E is smooth if and only if $\Delta(p_2, p_4, q_4, p_6) \neq 0$. The assignment $(E, P, Q, t) \mapsto (p_2, p_4, q_4, p_6)$ defines a bijection between the following two sets:*

- *The set of tuples (E, P, Q, t), where E is an elliptic curve over k and $P, Q \in E(k)$ are distinct non-trivial rational points, and t is a basis for $H^0(E, \mathcal{O}_E(O)/\mathcal{O}_E)$. These tuples are considered up to isomorphism (i.e. isomorphisms $\varphi : E \to E'$ of elliptic curves which preserve the other data).*
- *The set of tuples $(p_2, p_4, q_4, p_6) \in k^4$ such that $\Delta(p_2, p_4, q_4, p_6) \neq 0$.*

Under this bijection, a tuple $(E, P, Q, \lambda t)$ $(\lambda \in k^\times)$ corresponds to $(\lambda p_2, \lambda^2 p_4, \lambda^2 q_4, \lambda^3 p_6)$.

Proof. The only thing to note is that the bijection is normalized by the requirement that $Y/Z \in H^0(E, \mathcal{O}_E(O+P+Q))$ has image in $\mathcal{O}_E(O)/\mathcal{O}_E$ equal to t. □

A similar story works over a more general base:

Proposition 2.2. *Let S be a $\mathbb{Z}[1/6]$-scheme, and let $p : E \to S$ be a family of elliptic curves equipped with identity section $O \in E(S)$ and sections $P, Q \in E(S)$ such that on every fibre, the associated points are distinct and non-trivial. Let $\mathcal{L} = (p_*[\mathcal{O}_E(O)/\mathcal{O}_E])^{\otimes -1}$. Then $\mathcal{L}$ is an invertible $\mathcal{O}_S$-module, and there are canonically determined sections $p_2 \in H^0(S, \mathcal{L})$, $p_4, q_4 \in H^0(S, \mathcal{L}^{\otimes 2})$, and $p_6 \in H^0(S, \mathcal{L}^{\otimes 3})$, such that E is isomorphic to the subscheme of $\mathbb{P}(\mathcal{L} \oplus \mathcal{L} \oplus \mathcal{O}_S)$ defined by the equation*

$$Y(XY + 2q_4 Z^2) = X^3 + p_2 X^2 Z + p_4 X Z^2 + p_6 Z^3, \tag{2.2}$$

where (X, Y, Z) is the co-ordinate system relative to the decomposition $\mathcal{L} \oplus \mathcal{L} \oplus \mathcal{O}_S$. Moreover, $\Delta(p_2, \dots p_6) \in H^0(S, \mathcal{L}^{\otimes 12})$ is an everywhere non-vanishing section.

Conversely, suppose given an invertible $\mathcal{O}_S$-module $\mathcal{L}$, together with sections $p_2, \dots, p_6$ as above such that $\Delta(p_2, p_4, q_4, p_6)$ is a non-vanishing section of $\mathcal{L}^{\otimes 12}$. Then the relative curve defined by the equation (2.2) is an elliptic curve with marked points at infinity that are distinct and non-trivial in each fibre.

We can use this theory to describe integral models of such triples (E, P, Q) over a Dedekind scheme. Let S be a Dedekind scheme on which 6 is a unit, let $K = K(S)$, and let $\mathcal{L}$ be an invertible $\mathcal{O}_S$-module. Suppose given sections $p_2 \in H^0(S, \mathcal{L})$, $p_4, q_4 \in H^0(S, \mathcal{L}^{\otimes 2})$, and $p_6 \in H^0(S, \mathcal{L}^{\otimes 3})$ such that $\Delta(p_2, p_4, q_4, p_6) \in H^0(S, \mathcal{L}^{12})$ is non-zero. Then the equation (2.2) defines a proper flat morphism $p : \mathcal{E} \to S$ with smooth generic fibre (and indeed, singular fibres exactly above those points of S where Δ vanishes).

We call the data of $(\mathcal{L}, p_2, \dots, p_6)$ minimal if we cannot find an invertible subsheaf $\mathcal{M} \subset \mathcal{L}$ such that the sections $p_2, \dots, p_6$ all come from $\mathcal{M}$. The minimal data is uniquely determined by the triple (E, P, Q) over K, in the following sense: if $(\mathcal{L}, p_2, \dots, p_6)$ and $(\mathcal{M}, p_2', \dots, p_6')$ are two sets of minimal data associated to E, then we can find an isomorphism $f : \mathcal{L} \to \mathcal{M}$ of invertible $\mathcal{O}_S$-modules such that $f(p_2, \dots, p_6) = (p_2', \dots, p_6')$. Indeed, it follows from Lemma 2.1 that we can find an isomorphism $f_\eta : \mathcal{L}_\eta \to \mathcal{M}_\eta$ over the generic point η of S such that $f(p_2, \dots, p_6) = (p_2', \dots, p_6')$. Choosing an isomorphism $\mathcal{L}_\eta \cong K$, we see that both $\mathcal{L}$ and $\mathcal{M}$ can be characterized as the smallest invertible subsheaves of K containing the sections $p_2, \dots, p_6$ in their respective tensor powers.

We refer to the morphism $p : \mathcal{E} \to S$ associated to minimal data $(\mathcal{L}, p_2, \dots, p_6)$ as a minimal integral model of the triple (E, P, Q). By the above discussion, it is also uniquely determined up to isomorphism by (E, P, Q). We can describe this minimal model in elementary terms in case $K = \mathbb{F}_q(X)$ is the function field of a smooth, projective, geometrically connected algebraic curve over $\mathbb{F}_q$. Let (E, P, Q) be an elliptic curve over K with two distinct non-trivial marked rational points, and choose an arbitrary equation of type (2.2) with $p_2, \dots, p_6 \in K$. Then for each place v of K there is a unique integer n_v satisfying the following conditions:

1. The tuple $(\varpi_v^{n_v} p_2, \varpi_v^{2n_v} p_4, \varpi_v^{2n_v} q_4, \varpi_v^{3n_v} p_6)$ has co-ordinates in $\mathcal{O}_{K_v}$.
2. The integer n_v is minimal with respect to this property.

We then define $\mathcal{L} \subset K$ to be the invertible subsheaf whose sections over a Zariski open $U \subset X$ are given by the formula

$$\mathcal{L}(U) = K \cap \left[\prod_{v \in U} \varpi_v^{-n_v} \mathcal{O}_{K_v} \right].$$

Then $p_2, \ldots, p_6$ are sections of the tensor powers of $\mathcal{L}$, and the tuple $(\mathcal{L}, p_2, \ldots, p_6)$ is minimal.

In this paper we will ultimately only be interested in those curves (E, P, Q) for which the associated minimal data $(\mathcal{L}, p_2, \ldots, p_6)$ satisfies the following two conditions:

1. The line bundle $\mathcal{L}$ is a square: $\mathcal{L} \cong \mathcal{M}^{\otimes 2}$.
2. The discriminant $\Delta(p_2, \ldots, p_6) \in H^0(S, \mathcal{L}^{12}) \cong H^0(S, \mathcal{M}^{24})$ is square-free.

The reason for this restriction is that these are exactly the curves which are related to orbits of squarefree discriminant in a certain representation, to be considered in the next section. We now give a geometric characterization of curves of square-free discriminant.

Lemma 2.3. *Let R be a DVR in which 6 is a unit, let $K = \operatorname{Frac} R$, and let $S = \operatorname{Spec} R$. Let (E, P, Q) be an elliptic curve over K together with distinct non-trivial marked points $P, Q \in E(K)$. Let $\Delta \in R$ denote the discriminant of a minimal integral model of (E, P, Q) over S, therefore determined up to $R^\times$-multiple. Then $\operatorname{ord}_K \Delta \leq 1$ if and only if the following conditions are satisfied:*

1. *The minimal regular model of E over S has special fibre of type I_0 or I_1.*
2. *The reductions modulo $\mathfrak{m}_R$ in the minimal regular model of E of the points $P, Q \in E(K)$ are distinct and non-trivial.*

Proof. First let $\mathcal{E}$ denote a minimal integral model of E over S. If $\Delta \in R^\times$, then $\mathcal{E} \to S$ is smooth, E has good reduction and the points P, Q indeed remain distinct in the special fibre. If the discriminant vanishes to order 1, then the model $\mathcal{E}$ is regular, with irreducible special fibre. It follows that $\mathcal{E}$ is the minimal regular model of E, which therefore has reduction of type I_1.

Now let us assume that E has reduction of type I_0 or I_1, with the points O, P, Q remaining distinct in the special fibre of the minimal regular model. Let $\mathcal{E}$ denote the minimal regular model of E, and let $D \subset \mathcal{E}$ denote the divisor $O + P + Q$ in $\mathcal{E}$. Fix an isomorphism $H^1(\mathcal{E}, \mathcal{O}_E) \cong R$; there is a canonical isomorphism

$$H^0(\mathcal{E}, \mathcal{O}_E(O)|_O) \cong H^1(\mathcal{E}, \mathcal{O}_E) \cong R,$$

and similarly with O replaced by P or Q. The exact sequence of sheaves

$$0 \longrightarrow \mathcal{O}_\mathcal{E} \longrightarrow \mathcal{O}_\mathcal{E}(D) \longrightarrow \mathcal{O}_\mathcal{E}(D)|_D \longrightarrow 0$$

gives rise to a long exact sequence

$$0 \longrightarrow R \longrightarrow H^0(\mathcal{E}, \mathcal{O}_\mathcal{E}(D)) \longrightarrow R^3 \longrightarrow R \longrightarrow 0,$$

where the map $R^3 \to R$ is summing co-ordinates. This sequence of finite free R-modules remains exact after applying $- \otimes_R k$, from which we see that each map in the sequence has saturated image. We can therefore choose $x, y \in H^0(\mathcal{E}, \mathcal{O}_\mathcal{E}(D))$ which map to $(0, 1, -1)$ and $(-2, 1, 1)$, respectively, in R^3; then the elements $1, x, y \in H^0(\mathcal{E}, \mathcal{O}_\mathcal{E}(D))$ span this free R-module, and define a map $\mathcal{E} \to \mathbb{P}^2_R$. The elements

$$1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3 \in H^0(\mathcal{E}, \mathcal{O}_\mathcal{E}(3D))$$

generate this free rank 9 R-module, and therefore must satisfy an R-linear relation. After dividing out by as many as possible powers of the uniformizer we see that this relation is unique up to multiplication by elements of $R^\times$, and has degree 3 term $ay(y^2 - x^2)$ for some $a \in R^\times$; after multiplying through, we can assume $a = 1$. We are free to replace x, y by $x + b$, $y + c$ for $b, c \in R$, and there is a unique such transformation which puts our given relation in the form

$$y(xy + 2q_4) = x^3 + p_2x^2 + p_4x + p_6$$

for some $p_2, p_4, q_4, p_6 \in R$. Let $Z \subset \mathbb{P}^2_R$ denote the closed subscheme defined by this equation. Then Z is normal and R-flat, and we therefore get a morphism $\mathcal{E} \to Z$. By Zariski's main theorem, this is in fact an isomorphism and we see that Z is regular, which can happen only if $\Delta(p_2, p_4, q_4, p_6)$ has order of vanishing at most 1. □

If D is a divisor on X, then we will write $\mathcal{X}_D$ for the set of isomorphism classes of triples (E, P, Q) of elliptic curves over K with two marked points such that the minimal data $(\mathcal{L}, p_2, \ldots, p_6)$ satisfies $\mathcal{L} \cong \mathcal{O}_X(2D)$, and the discriminant $\Delta(p_2, \ldots, p_6) \in H^0(X, \mathcal{L}^{\otimes 12}) \cong H^0(X, \mathcal{O}_X(2D))$ is square-free. Lemma 2.3 shows that this is the same as the set $\mathcal{X}_{\mathcal{O}_X(D)}$ defined in §1.

We also write $B_D = \mathcal{O}_X(2D) \oplus \mathcal{O}_X(4D) \oplus \mathcal{O}_X(4D) \oplus \mathcal{O}_X(6D)$, a vector bundle over X, and write $H^0(X, B_D)^{\mathrm{sf}} \subset H^0(X, B_D)$ for the set of sections $(p_2, p_4, q_4, p_6) \in H^0(X, B_D)$ for which the discriminant $\Delta(p_2, \ldots, p_6) \in H^0(X, \mathcal{O}_X(24D))$ is square-free. We can summarize the results of this section as follows:

Corollary 2.4. *The assignment $\iota : (p_2, \ldots, p_6) \mapsto (E, P, Q)$ which sends sections of $H^0(X, B_D)^{sf}$ to the curve given by the equation (2.2) is surjective, each fibre having finite cardinality equal to $|\mathbb{F}_q^\times| \cdot |\operatorname{Aut}(E, P, Q)|^{-1}$.*

Proof. The only thing left to check is the cardinality of the fibres. Let $\mathbb{F}_q^\times$ act on $H^0(X, B_D)$ by the formula $\lambda \cdot (p_2, p_4, q_4, p_6) = (\lambda p_2, \lambda^2 p_4, \lambda^2 q_4, \lambda^3 p_6)$. Lemma 2.1 shows that $\mathbb{F}_q^\times$ acts transitively on the fibres of ι, and that the stabilizer of any point is $\operatorname{Aut}(E, P, Q)$. The result follows. □

3 Invariant theory

In this section, we introduce the semisimple group G and its representation V, the orbits of which will eventually be interpreted as elements of the 2-Selmer groups of elliptic curves of the type considered in §2. For the moment, $\mathbb{F}_q$ denotes a finite field of characteristic prime to 6; we will soon impose more severe restrictions on the characteristic.

3.1 Preliminaries

Let J denote the 4×4 matrix with 1's on the anti-diagonal and 0's elsewhere, and define a block matrix

$$\Psi = \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix} \in M_{8\times 8}(\mathbb{Z}). \tag{3.1}$$

We write SO_8 for the special orthogonal group over $\mathbb{F}_q$ defined by Ψ, $H = \mathrm{SO}_8/\mu_2$ for its adjoint group, and $H^{\mathrm{sc}} = \mathrm{Spin}_8$ for its simply connected double cover. We write $\mathfrak{h} = \operatorname{Lie} H$. We write θ for the inner involution of H given by conjugation by the element

$$s = \operatorname{diag}(1, -1, -1, 1, 1, -1, -1, 1). \tag{3.2}$$

We define $G = (H^\theta)^\circ$ (i.e. the identity component of the θ-fixed subgroup of H), and $V = \mathfrak{h}^{d\theta = -1}$. There is an isomorphism $G \cong (\mathrm{SO}_4 \times \mathrm{SO}_4)/\Delta(\mu_2)$, where SO_4 is a split special orthogonal group and $\Delta(\mu_2)$ is the diagonally embedded centre.

We write T' for the (split) diagonal maximal torus of SO_8; a general element has the form

$$\operatorname{diag}(a, b, b^{-1}, a^{-1}, c, d, d^{-1}, c^{-1}).$$

We write T for the image of T' in H. We observe that T is also a maximal torus of G. The group H^θ is disconnected. Its component group H^θ/G can be computed as follows: let $W_H = N_H(T)/T$ denote the Weyl group of of H, $W = N_G(T)/T$ the Weyl group of G. Then the map $Z_{W_H}(s) \to H^\theta/G$ is surjective, with kernel equal to $Z_W(s)$ (see [Hum95, §2.2]). A calculation shows that the component group is therefore isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Explicit representatives can be given by the elements $\sigma, \tau \in W_H$ satisfying

$$\sigma(a, b, c, d) = (a, b, c^{-1}, d^{-1}), \tau(a, b, c, d) = (b, a, d, c),$$

which generate a subgroup $W_0 \subset W_H$ which projects isomorphically to H^θ/G.

We introduce sets of simple roots as follows. A set $R_H \subset X^*(T)$ of simple roots for H consists of the characters

$$\alpha_1 = a/b, \alpha_2 = b/c, \alpha_3 = c/d, \alpha_4 = cd.$$

We let $\alpha_0 = ab$; it is the highest root of H. A set $R \subset X^*(T)$ of simple roots for G consists of the characters

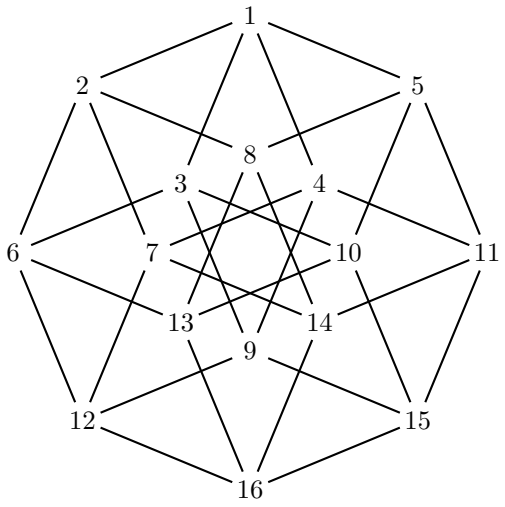
$$a_1 = ac, a_2 = a/c, a_3 = bd, a_4 = b/d.$$

The group G is isogenous to SL_2^4, and the group $W_0 \subset W$ commutes with the action of W_G on $X^*(T)$ and leaves invariant the set $\{a_1, \dots, a_4\}$. Its action on this set is faithful, and identifies W_0 with the Klein 4-group $\{e, (12)(34), (13)(24), (14)(23)\}$. The characters of T appearing in the representation V are exactly the combinations

$$\frac{1}{2}(\pm a_1 \pm a_2 \pm a_3 \pm a_4),$$

and can thus be thought of as the vertices of a hypercube. Each weight space is 1-dimensional and we thus have $\dim_{\mathbb{F}_q} V = 16$. We write Φ_V for the set of weights appearing in V. Any vector $v \in V$ admits a decomposition $v = \sum_{a \in \Phi_V} v_a$. There is a decomposition $\Phi_V = \Phi_V^+ \sqcup \Phi_V^-$ coming from the decomposition of the roots of H into positive and negative roots. We write $n_1, \dots, n_4$ for the basis of $X_*(T)_{\mathbb{Q}}$ dual to $a_1, \dots, a_4$. We define a partial order on Φ_V by setting $a \geq b$ if $n_i(a) \geq n_i(b)$ for each $i = 1, \dots 4$. We label these weights in Φ_V as follows:

#	$2n_1$	$2n_2$	$2n_3$	$2n_4$
1	1	1	1	1
2	-1	1	1	1
3	1	-1	1	1
4	1	1	-1	1
5	1	1	1	-1
6	-1	-1	1	1
7	-1	1	-1	1
8	-1	1	1	-1
9	1	-1	-1	1
10	1	-1	1	-1
11	1	1	-1	-1
12	-1	-1	-1	1
13	-1	-1	1	-1
14	-1	1	-1	-1
15	1	-1	-1	-1
16	-1	-1	-1	-1



The figure above shows the Hasse diagram of Φ_V with respect to this partial order. The weight labelled 1 is α_0. If $M \subset \Phi_V$ is a subset, we will write $\lambda(M) \subset \Phi_V - M$ for the set of maximal elements of $\Phi_V - M$, i.e. the set

$$\{a \in \Phi_V - M \mid \forall b \in \Phi_V - M, a \leq b \Rightarrow a = b\}.$$

It is useful to note that the action of W_0 preserves the partial order on Φ_V, and consequently commutes with application of the function λ.

In the paper [Tho13], we have summarised part of the invariant theory of the pair (G, V) over a field of characteristic 0; in this case, the most important results were established by Kostant–Rallis [KR71]. They have been extended to positive characteristic in many cases by Levy [Lev07]. We now discuss this.

Proposition 3.1. *Let $k/\mathbb{F}_q$ be a field, and let k^s/k be a separable closure.*

1. *The natural inclusions $\mathbb{F}_q[V]^G \to \mathbb{F}_q[V]^{H^\theta} \to \mathbb{F}_q[\mathfrak{h}]^H$ are isomorphisms, and all of these rings are isomorphic to polynomial algebras over $\mathbb{F}_q$ on four homogeneous generators of degrees $2, 4, 4,$ and 6, respectively. We write $\Delta \in \mathbb{F}_q[V]^G$ for the restriction of the standard discriminant polynomial of the Lie algebra $\mathfrak{h}$. It is non-zero.*

2. *Let $B = \operatorname{Spec} \mathbb{F}_q[V]^G$, and let $\pi : V \to B$ denote the natural map. Then π has reduced, G^θ-invariant fibres.*

3. *Let $v \in V_k$. Then $Z_{G_k}(v)$ and $Z_{H_k}(v)$ are smooth over k.*

4. *Let $\mathfrak{c} \subset V_k$ be a subspace. We call $\mathfrak{c}$ a Cartan subspace if there exists a maximal torus $C \subset H_k$ such that $\theta(t) = t^{-1}$ for all $t \in C$ and $\operatorname{Lie} C = \mathfrak{c}$. All such subspaces are conjugate under the action of $G(k^s)$.*

5. *Let $\mathfrak{c} \subset V_k$ be a Cartan subspace. Then the map $N_{G_k}(\mathfrak{c}) \to W(H_k, \mathfrak{c}) = N_{H_k}(\mathfrak{c})/Z_{H_k}(\mathfrak{c})$ is surjective, and the natural restriction map $k[V]^G \to k[\mathfrak{c}]^{W(H_k,\mathfrak{c})}$ is an isomorphism.*

6. *Let $v \in V_k$. Then the following are equivalent:*

   (a) *v is semisimple as an element of $\mathfrak{h}_k$.*

   (b) *$G_k \cdot v \subset V_k$ is closed.*

   (c) *v is contained in a Cartan subspace of V_k.*

   Any such element is called a semisimple element of V_k.

7. *Let $v \in V_k$. Then the following are equivalent:*

   (a) *$\dim Z_{H_k}(v) = \dim T$.*

   (b) *$\dim Z_{G_k}(v) = 0$.*

   Any such element is called a regular element of V_k. The condition of being regular is open, and we write $V^{reg} \subset V$ for the open subscheme of regular elements.

8. *Let $b \in B(k)$, and let $V_b = \pi^{-1}(b) \subset V$. Then $V_b(k^s)$ contains regular semisimple elements if and only if $\Delta(b) \neq 0$. In this case, $G(k^s)$ acts transitively on $V_b(k^s)$ and for any $v \in V_b(k^s)$, $\mathfrak{z}_{\mathfrak{h}_k}(v) = \operatorname{Lie} Z_{H_k}(v)$ is the unique Cartan subspace of V_k containing v.*

Proof. Rather than give detailed references to [Lev07], we simply refer the reader to the introduction of that paper, which features a thorough summary of the results therein. □

The group $\mathbb{G}_m$ acts on V by scalar multiplication; there is an induced $\mathbb{G}_m$-action on the quotient B which makes the morphism $\pi : V \to B$ equivariant. We write $B^{\mathrm{rs}} \subset B$ for the open subscheme where Δ is non-zero; by the proposition, $\pi^{-1}(B^{\mathrm{rs}}) = V^{\mathrm{rs}}$ is the open subscheme of regular semisimple elements of V.

3.2 Singular and trivial orbits

Let $k/\mathbb{F}_q$ be a field. We are now going to give simple criteria in terms of vanishing of certain matrix entries for elements $v \in V_k$ either to satisfy $\Delta(v) = 0$, or to be trivial in a sense we will soon define.

Lemma 3.2. *Let $k/\mathbb{F}_q$ be a field, and let $v = \sum_{a \in \Phi_V} v_a \in V_k$.*

1. *Let $S \subset \{1, 2, 3, 4\}$ be a two-element subset, and suppose that $v_a = 0$ if $n_i(a) > 0$ for each $i \in S$. Then $\Delta(v) = 0$.*

2. *Suppose that $v_a = 0$ if $n_i(a) < 0$ for at most one $i \in \{1, 2, 3, 4\}$. Then $\Delta(v) = 0$.*

Proof. We will use the following criterion: let $\mathfrak{p} \subset \mathfrak{h}$ be a θ-stable parabolic subalgebra which contains $\mathfrak{t} = \operatorname{Lie} T$, and let $v \in \mathfrak{p}_k^{d\theta=-1}$. Then $\Delta(v) = 0$. Indeed, if $\Delta(v) \neq 0$ then v is regular semisimple, hence its centralizer $\mathfrak{c} = \mathfrak{z}_{\mathfrak{h}_k}(v)$ is a Cartan subalgebra of $\mathfrak{h}_k$ which is contained in V_k. We have $\dim_k \mathfrak{c} \leq \dim_k \mathfrak{z}_{\mathfrak{p}_k}(v) \leq \dim_k \mathfrak{c}$, hence $\mathfrak{c} = \mathfrak{z}_{\mathfrak{p}_k}(v)$ and $\mathfrak{c} \subset \mathfrak{p}_k^{d\theta=-1}$. Let $C \subset H_k$ denote the unique maximal torus with $\operatorname{Lie} C = \mathfrak{c}$. We have $\dim Z_{P_k}(v) \geq \dim C$, hence $Z_{P_k}(v) = C$ is smooth and $C \subset P_k$. There is a unique Levi subgroup $L \subset P_k$ containing C, which is necessarily stable under the action of θ. The centre Z_L is contained in C, on which θ acts by $t \mapsto t^{-1}$. On the other hand, L projects isomorphically and θ-equivariantly to the Levi

quotient of P_k, and θ acts on the centre of this quotient trivially (because it acts trivially on T). This contradiction implies that we must have $\Delta(v) = 0$.

If $S \subset \Phi_V$ is a subset, we write $V_S \subset V$ for the subspace given by the equations $v_a = 0$ ($a \in S$). The four maximal proper parabolic subalgebras $\mathfrak{p} \subset \mathfrak{h}$ which contain the Borel subalgebra corresponding to the root basis R_H have $\mathfrak{p}^{d\theta=-1} = V_S$ for the following sets of weights:

$$\begin{aligned} S =&\{\frac{1}{2}(a_1 + a_2 \pm a_3 \pm a_4)\},\ \{\frac{1}{2}(a_1 \pm a_2 \pm a_3 + a_4)\},\ \{\frac{1}{2}(a_1 \pm a_2 + a_3 \pm a_4)\},\ \text{and} \\ &\{\frac{1}{2}(a_1 + a_2 + a_3 + a_4), \frac{1}{2}(-a_1 + a_2 + a_3 + a_4), \frac{1}{2}(a_1 - a_2 + a_3 + a_4), \\ &\qquad \frac{1}{2}(a_1 + a_2 - a_3 + a_4), \frac{1}{2}(a_1 + a_2 + a_3 - a_4)\}. \end{aligned} \tag{3.3}$$

The last of these gives the subspace appearing in the second part of the lemma. On the other hand, each of the subspaces appearing in the first part of the lemma is W_0-conjugate to one of the first three appearing in (3.3). The action of W_0 leaves Δ invariant, so this implies the first part of the lemma. □

We now introduce the Kostant section. This is a section $\kappa : B \to V$ of the morphism $\pi : V \to B$, and which has image consisting of regular elements of V. We will follow Slodowy [Slo80] in constructing κ using a fixed choice of regular $\mathfrak{sl}_2$-triple and we must therefore impose the restriction that the characteristic of $\mathbb{F}_q$ exceeds $4h - 2$, where h is the Coxeter number of H, namely 6. We therefore now make the following assumption, which holds for the remainder of §3:

- The characteristic of $\mathbb{F}_q$ is at least 23.

This being the case, we define

$$E = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

and $\check{\rho} : \mathbb{G}_m \to T$ by the formula

$$\check{\rho}(t) = (t^3, t^2, t^{-2}, t^{-3}, t, 1, 1, t^{-1}).$$

(Thus in fact $\check{\rho}$, which is the sum of the fundamental coweights, lifts to $X_*(T')$.) We have the formula $\mathrm{Ad}\,\check{\rho}(t)(E) = tE$, and we can decompose $E = X_{\alpha_1} + X_{\alpha_2} + X_{\alpha_3} + X_{\alpha_4}$ as a sum of T-eigenvectors corresponding to the simple roots R_H.

Proposition 3.3. *1. There exists a unique element $F \in V$ such that $\mathrm{Ad}\,\check{\rho}(t)(F) = t^{-1}F$ and $[E, F] = d\check{\rho}(2)$.*

2. Let $\kappa = E + \mathfrak{z}_{\mathfrak{h}}(F)$, an affine linear subspace of $\mathfrak{h}$. Then $\kappa \subset V$ and the restriction $\pi|_\kappa : \kappa \to B$ is an isomorphism.

Proof. The first part is a standard property of $\mathfrak{sl}_2$-triples; we could also exhibit F directly. See for example [SS70, III, 4.10]. The second part is [Slo80, §7.4, Corollary 2]. An essential role in the proof is played by the fact that for $t \in \mathbb{G}_m$, $v \in \kappa$, we have $t\,\mathrm{Ad}\,\check{\rho}(t^{-1})(v) \in \kappa$, and this $\mathbb{G}_m$-action contracts to the central point $E \in \kappa$. The morphism $\pi|_\kappa$ is also clearly equivariant with respect to this $\mathbb{G}_m$-action. These properties of the Kostant section will appear again in §5.3 below. □

Corollary 3.4. *Let $k/\mathbb{F}_q$ be a field, and let $b \in B(k)$, and suppose that $\Delta(b) \neq 0$. Then there is a canonical bijection*

$$G(k)\backslash V(k) \cong \ker(H^1(k, Z_G(\kappa_b)) \to H^1(k, G)).$$

Proof. This follows because $V_b(k^s)$ is a single $G(k^s)$-orbit, and because of the existence of the marked base point $\kappa_b \in V_b(k)$. □

In the situation of the corollary, we refer to the $G(k)$-orbits of the elements $w \cdot \kappa_b$ ($w \in W_0$) as the trivial orbits. We call elements of $V_k = V(k)$ which lie in a trivial orbit trivial elements. Note that this notion depends on k (and indeed, all regular semisimple elements in $V(k^s)$ are trivial over k^s).

Lemma 3.5. *Let $k/\mathbb{F}_q$ be a field, and let $v = \sum_{a \in \Phi_V} v_a \in V_k$. Suppose that $v_a = 0$ for all $a \in S$ and $v_a \neq 0$ for all $a \in \lambda(S)$, where S is one of the following sets:*

$$\begin{gathered}\{a_1+a_2+a_3+a_4, a_1-a_2+a_3+a_4, a_1+a_2-a_3+a_4, a_1+a_2+a_3-a_4\},\\ \{a_1+a_2+a_3+a_4, -a_1+a_2+a_3+a_4, a_1-a_2+a_3+a_4, a_1+a_2+a_3-a_4\},\\ \{a_1+a_2+a_3+a_4, -a_1+a_2+a_3+a_4, a_1+a_2-a_3+a_4, a_1+a_2+a_3-a_4\},\\ \{a_1+a_2+a_3+a_4, -a_1+a_2+a_3+a_4, a_1-a_2+a_3+a_4, a_1+a_2-a_3+a_4\}.\end{gathered} \tag{3.4}$$

Then if $\Delta(v) \neq 0$ then v belongs to a trivial orbit of $G(k)$.

Proof. These sets S form a single W_0-orbit, so it suffices to treat one of them, say

$$S = \{a_1+a_2+a_3+a_4, a_1-a_2+a_3+a_4, a_1+a_2-a_3+a_4, a_1+a_2+a_3-a_4\}.$$

In this case, we can compute

$$\lambda(S) = \{-a_1+a_2+a_3+a_4, a_1+a_2-a_3-a_4, a_1-a_2-a_3+a_4, a_1-a_2+a_3-a_4\} = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}.$$

Thus if $v \in V(k)$ is as in the statement of the lemma, we can write

$$v = \sum_{i=1}^{4} \lambda_i X_{\alpha_i} + \sum_{a \in \Phi_V^-} v_a,$$

where each $\lambda_i \in k^\times$. Since the group H is adjoint, we can find $t \in T(k)$ such that $\alpha_i(t) = \lambda_i$ for each $i = 1, \ldots, 4$. Replacing v by $t^{-1} \cdot v$, we can assume that $\lambda_i = 1$ for each i.

We claim that this implies that v is $(U^-)^\theta(k)$-conjugate to $\kappa(k)$, where $U^- \subset H$ is the unipotent radical of the Borel subgroup $B^- \subset G$ corresponding to the set $-R_H \subset \Phi(H,T)$ of simple roots. One can show that the natural product map $U^- \times \kappa \to E + \operatorname{Lie} U^- \subset \mathfrak{h}$ is an isomorphism. (The analogous fact in characteristic 0 is employed for a very similar purpose in the proof of [Tho15, Lemma 2.6]; one can easily check that it is true here as well, under our restrictions on the characteristic.) Since v lies in $E + \operatorname{Lie} U_k^-$, we find that there is a unique pair $(u, b) \in U^-(k) \times \kappa(k)$ such that $u \cdot b = v$, and then u necessarily satisfies $\theta(u) = u$, hence $u \in G(k)$, as required. □

Corollary 3.6. *Let $k/\mathbb{F}_q$ be a field, and let $v = \sum_{a \in \Phi_V} v_a \in V_k$. Suppose that $v_a = 0$ for all $a \in S$, where S is one of the following subsets (labelling as in the figure preceding Proposition 3.1):*

$$\{1,2,3,4,5\}, \{1,4,5,11\}, \{1,3,4,9\}, \{1,3,5,10\}, \{1,3,4,5\}, \{1,2,3,5\}, \{1,2,4,5\}, \tag{3.5}$$

$$\{1,2,3,4\}, \{1,2,3,6\}, \{1,2,4,7\}, \{1,2,5,8\}. \tag{3.6}$$

Then either $\Delta(v) = 0$ or v belongs to a trivial orbit of $G(k)$.

Proof. This follows from combining Lemma 3.2 and Lemma 3.5, as we now show. Let $v \in V(k)$. The sets S appearing in (3.5) are exactly those appearing in the statement of Lemma 3.2, so the result follows immediately in this case (and indeed we have $\Delta(v) = 0$). The sets S appearing in (3.6) are exactly those appearing in the statement of Lemma 3.5. If S is one of these and $v_a = 0$ for all $a \in S$, then there are two possibilities: either $v_a \neq 0$ for all $a \in \lambda(S)$, or there exists $b \in \lambda(S)$ such that $v_a = 0$ for all $a \in S' = S \cup \{b\}$. In the first case, Lemma 3.5 shows that $\Delta(v) = 0$ or v belongs to a trivial orbit. In the second case, we see by inspection that S' is one of the sets appearing in (3.5), hence $\Delta(v) = 0$. □

4 Interlude on G-bundles, semi-stability, and integration

In this section, we review the parameterization of G-torsors on curves by adeles and its relation to integration. We also recall the theory of Harder–Narasimhan filtrations and canonical reductions for G-torsors, which will be our substitute for reduction theory when it comes to counting points later on. Let $\mathbb{F}_q$ be a finite field.

Let M be a smooth affine group scheme over $\mathbb{F}_q$. By definition, an M-torsor over a scheme $S/\mathbb{F}_q$ is a scheme $F \to S$, equipped with a right action of M_S, and locally on S (in the étale topology) isomorphic to the trivial torsor M_S. A morphism $F \to F'$ of M-torsors over S is a morphism $F \to F'$ respecting the M-action. A torsor $F \to S$ is trivial (i.e. isomorphic to the trivial torsor M_S) if and only if it admits a section. The set of isomorphism classes of torsors over S is in bijection with $H^1(S, M)$ (non-abelian étale cohomology).

If $M' \subset M$ is a closed subgroup, still smooth over $\mathbb{F}_q$, then a reduction of $F \to S$ to M' is a pair (F', φ), where $F' \to S$ is an M'-torsor and $\varphi : F' \times_{M'} M \to F$ is an isomorphism. Giving a reduction of F to M' is then equivalent to giving a section of the sheaf quotient F/M'.

Let X be a smooth, projective, geometrically connected curve over $\mathbb{F}_q$, and let $K = \mathbb{F}_q(X)$. Suppose that M is connected. We say that an M-torsor $F \to X$ is *rationally trivial* if $F_K = F \times_X \operatorname{Spec} K$ is a trivial M-torsor. This will always be the case if M satisfies the Hasse principle over K. Indeed, each pointed set $H^1(\mathcal{O}_{K_v}, M)$ is trivial (by Lang's theorem and Hensel's lemma). It is useful to note that if M is split reductive, and $P \subset M$ is a parabolic subgroup, then for any rationally trivial M-torsor $F \to X$ with a reduction $F_P \to X$ to P, F_P is also rationally trivial. Indeed, the morphism $M \to M/P$ admits Zariski local sections, and F_P/P defines a K-point of F/P.

For any connected smooth affine group M, the rationally trivial torsors over X can be parameterized using adeles. Indeed, if $\mathcal{Y}_M$ denotes the set of isomorphism classes of such torsors, then there is a canonical bijection

$$\mathcal{Y}_M \cong M(K)\backslash M(\mathbb{A}_K)/M(\widehat{\mathcal{O}}_K). \tag{4.1}$$

This is a consequence of fpqc descent; see [Gil02, Appendix]. We can describe the bijection explicitly as follows: given such a torsor $F \to X$, choose sections $x_0 \in F(K)$, $x_v \in F(\mathcal{O}_{K_v})$ for each place v. Then for each v there is a unique element $m_v \in M(K_v)$ such that $x_0 m_v = x_v$, and we assign to F the element $m_F = (m_v)_v \in M(\mathbb{A}_K)$. The class $[(m_v)_v] \in M(K)\backslash M(\mathbb{A}_K)/M(\widehat{\mathcal{O}}_K)$ is then clearly well-defined. If $m \in M(\mathbb{A}_K)$, we will write F_m for the corresponding M-torsor over X. We can describe the group of automorphisms of $F_m \to X$ in these terms: we have an isomorphism $\operatorname{Aut}(F_m) \cong M(K) \cap mM(\widehat{\mathcal{O}}_K)m^{-1}$. It follows that the correspondence (4.1) can instead be thought of as an equivalence of groupoids.

We will henceforth identify $\mathcal{Y}_M$ with this adelic double quotient. We endow $\mathcal{Y}_M$ with its counting measure ν_M, each point $F \in \mathcal{Y}_M$ being weighted by $|\operatorname{Aut}(F)|^{-1}$. If μ_M is the (right-invariant) Haar measure on $M(\mathbb{A}_K)$ which gives $M(\widehat{\mathcal{O}}_K)$ volume 1, and with modulus $\Delta_l : M(\mathbb{A}_K) \to \mathbb{R}_{>0}$ defined by the formula

$$\int_{m' \in M(\mathbb{A}_K)} f(m^{-1}m')\, d\mu_M = \Delta_l(m) \int_{m' \in M(\mathbb{A}_K)} f(m')\, d\mu_M,$$

then we have the formula for any compactly supported function $f : \mathcal{Y}_M \to \mathbb{R}$:

$$\int_{F \in \mathcal{Y}_M} f(F)\, d\nu_M = \int_{m \in M(K)\backslash M(\mathbb{A}_K)} f(F_m)\Delta_l(m)^{-1}\, d\mu_M. \tag{4.2}$$

An important special case arises when M is a split reductive group and $P \subset M$ is a parabolic subgroup with Levi decomposition $P = L_P N_P$. In this case we define a character $\delta_P \in X^*(P)$ by $\delta_P(p) = \det \operatorname{Ad}(p)|_{\operatorname{Lie} N_P}$. A right-invariant Haar measure is given by the formula

$$\int_{p \in P(\mathbb{A}_K)} f(p)\, d\mu_P = \int_{l \in L_P(\mathbb{A}_K)} \int_{n \in N_P(\mathbb{A}_K)} f(nl)\, d\mu_{N_P}\, d\mu_{L_P}, \tag{4.3}$$

and the modulus character of P is $\Delta_l(p) = \|\delta_P(p)\|$, where $\|\cdot\|$ is the adele norm. In this case (4.2) becomes

$$\int_{F \in \mathcal{Y}_P} f(F)\, d\nu_P = \int_{p \in P(K)\backslash P(\mathbb{A}_K)} f(F_p)\|\delta_P(p)\|^{-1}\, d\mu_P. \tag{4.4}$$

Now suppose that G is a reductive group over $\mathbb{F}_q$ with split maximal torus and Borel subgroup $T \subset B \subset G$. Let $P \subset G$ be a standard parabolic subgroup, i.e. one containing B, and let $P = L_P N_P$ be its standard Levi decomposition; thus L_P is the unique Levi subgroup of P containing T. If $F_P \to X$ is a P-torsor, we can associate to it an element $\sigma_{F_P} \in X_*(Z_0(L_P))_{\mathbb{Q}} \subset X_*(T)$, uniquely characterized by the requirement that for any $\chi \in X^*(P)$, the line bundle $\mathcal{L}_\chi = F_P \times_{P,\chi} \mathbb{A}^1_{\mathbb{F}_q}$ has degree $\deg \mathcal{L}_\chi = \langle \sigma_{F_P}, \chi \rangle$.

We call σ_{F_P} the slope of F_P. If $\sigma, \tau \in X_*(T)_{\mathbb{Q}}$, then we write $\sigma \leq \tau$ if $\langle \tau - \sigma, \alpha \rangle \geq 0$ for all B-positive roots $\alpha \in \Phi(G,T)$. The following formulations are taken from [Sch15].

Definition 4.1. *Let G be a split reductive group over $\mathbb{F}_q$, with split maximal torus and Borel subgroup $T \subset B \subset G$. Let $R \subset \Phi(G,T)$ denote the set of simple roots corresponding to B. Let $F \to X$ be an G-torsor.*

1. *We say that F is semi-stable if for any standard parabolic subgroup $P \subset G$ and any reduction $F_P \to X$ of F, we have $\sigma_{F_P} \leq \sigma_F$.*
2. *Let P be a standard parabolic subgroup with Levi quotient L_P, and let $F_P \to X$ be a reduction of F to P. We say that F_P is canonical if $F_P \times_P L_P$ is semi-stable and if for any simple root $\alpha \in R - \Phi(L_P, T)$, we have $\langle \sigma_{F_P}, \alpha \rangle > 0$.*

The following result justifies the use of the word 'canonical':

Theorem 4.2. *Let $F \to X$ be a G-torsor. Then there exists exactly one pair (P, F_P) consisting of a standard parabolic subgroup $P \subset G$ and a reduction $F_P \to X$ of F which is canonical.*

Proof. See [Sch15, Theorem 2.1] and the remarks following. □

This theorem allows us to decompose $\mathcal{Y}_G = \sqcup_P \mathcal{Y}_{G,P}$, where $\mathcal{Y}_{G,P}$ denotes the set of G-torsors on X which admit a canonical reduction to the standard parabolic subgroup P. We then have an identification

$$\mathcal{Y}_{G,P} = P(K) \backslash P(\mathbb{A}_K)^{\text{pos, ss}} / P(\widehat{\mathcal{O}}_K), \tag{4.5}$$

where we define

$$P(\mathbb{A}_K)^{\text{pos}} = \{p \in P(\mathbb{A}_K) \mid \forall \alpha \in R - \Phi(L_P, T), \langle m_P(p), \alpha \rangle > 0\},$$
$$P(\mathbb{A}_K)^{\text{ss}} = \{p \in P(\mathbb{A}_K) \mid F_p \times_P L_P \text{ semi-stable}\},$$

and

$$P(\mathbb{A}_K)^{\text{pos, ss}} = P(\mathbb{A}_K)^{\text{pos}} \cap P(\mathbb{A}_K)^{\text{ss}}.$$

Here we write

$$m_P : P(\mathbb{A}_K) \to \text{Hom}(X^*(L_P), \mathbb{Q}) \cong X_*(Z_0(L_P))_{\mathbb{Q}} \subset X_*(T)_{\mathbb{Q}}, p \mapsto (\chi \mapsto \log_q \|\chi(p)\|).$$

We observe the formulae

$$m_P(p) = \sigma_{F_p} \text{ and } \Delta_l(p) = \|\delta_P(p)\| = q^{\langle m_P(p), \delta_P \rangle}. \tag{4.6}$$

We define $\Lambda_P^{\text{pos}} = m_P(P(\mathbb{A}_K)^{\text{pos}}) \subset X_*(T)_{\mathbb{Q}}$. Theorem 4.2 implies that (4.5) is an isomorphism of groupoids: if $p \in P(\mathbb{A}_K)^{\text{pos, ss}}$, then the inclusion $P(K) \cap pP(\widehat{\mathcal{O}}_K)p^{-1} \to G(K) \cap pG(\widehat{\mathcal{O}}_K)p^{-1}$ is an isomorphism (because any automorphism of a G-torsor must preserve its canonical reduction). This leads to the following lemma.

Lemma 4.3. *There exists a constant $C > 0$ depending only on X such that for any standard parabolic subgroup $P \subset G$ and function $f : X_*(Z_0(L_P))_{\mathbb{Q}} \to \mathbb{R}_{\geq 0}$, we have*

$$\int_{F \in \mathcal{Y}_{G,P}} f(\sigma_{F_P}) \, d\nu_G \leq C \sum_{\sigma \in \Lambda_P^{pos}} q^{-\langle \sigma, \delta_P \rangle} f(\sigma).$$

Proof. Let $P(\mathbb{A}_K)^0 = \ker m_P$. Then $P(K) \subset P(\mathbb{A}_K)^0$ and the quotient $P(K)\backslash P(\mathbb{A}_K)^0$ has finite μ_P-volume. We choose the constant C to exceed the volume of $P(K)\backslash P(\mathbb{A}_K)^0$ for all standard parabolic subgroups of G. Then (4.4) and (4.6) give

$$\int_{F \in \mathcal{Y}_{G,P}} f(\sigma_{F_P})\, d\nu_P \leq \int_{p \in P(K)\backslash P(\mathbb{A}_K)^{\mathrm{pos}}} f(m_P(p)) \|\delta_P(p)\|^{-1}\, d\mu_P \leq C \sum_{\sigma \in \Lambda_P^{\mathrm{pos}}} q^{-\langle \sigma, \delta_P \rangle} f(\sigma),$$

as required. □

We need to discuss the behaviour of the canonical reduction under certain functorialities. For this it is useful to recall that giving a GL_n-torsor over X is equivalent to giving a vector bundle over X of rank n, via $F \mapsto F \times_{\mathrm{GL}_n} \mathbb{A}_{\mathbb{F}_q}^n$. If $\mathcal{E} \to X$ is a vector bundle, then its slope is defined to be $\mu(\mathcal{E}) = \deg \mathcal{E} / \operatorname{rank} \mathcal{E}$. A vector bundle is said to be semi-stable if for any vector subbundle $\mathcal{F} \subset \mathcal{E}$, we have $\mu(\mathcal{F}) \leq \mu(\mathcal{E})$. This is equivalent to the semi-stability of the corresponding GL_n-torsor, and Theorem 4.2 is equivalent to the following statement: given a vector bundle $\mathcal{E} \to X$ of rank n, there is a unique filtration

$$0 \subset \mathcal{E}_1 \subset \mathcal{E}_2 \subset \cdots \subset \mathcal{E}_m = \mathcal{E} \tag{4.7}$$

by vector subbundles such that each subquotient $\mathcal{E}_{i+1}/\mathcal{E}_i$ is (non-zero and) semi-stable, and we have the chain of inequalities

$$\mu(\mathcal{E}_1) > \mu(\mathcal{E}_2/\mathcal{E}_1) > \cdots > \mu(\mathcal{E}_m/\mathcal{E}_{m-1}). \tag{4.8}$$

This is the Harder–Narasimhan filtration of $\mathcal{E}$. It will play a key role for us because of the following lemma.

Lemma 4.4. *Let $\mathcal{E}$ be a semi-stable vector bundle over X of rank n. Let g_X denote the genus of X.*

1. *If $\mu(\mathcal{E}) < 0$, then $h^0(X, \mathcal{E}) = 0$.*
2. *If $0 \leq \mu(\mathcal{E}) \leq 2g_X - 2$, then $h^0(X, \mathcal{E}) \leq n(1 + \mu(\mathcal{E})/2)$.*
3. *If $\mu(\mathcal{E}) > 2g_X - 2$, then $h^0(X, \mathcal{E}) = n(1 - g_X + \mu(\mathcal{E}))$.*

Proof. The first and third points are well-known properties of semi-stable bundles and follow easily from the definition, together with the Riemann–Roch theorem. The second point is a generalization of Clifford's theorem for line bundles, see [BPGN97, Theorem 2.1]. □

Corollary 4.5. *Let $\mathcal{E} \to X$ be a vector bundle of rank n and slope $\mu(\mathcal{E}) = 0$, and let its Harder–Narasimhan filtration be as in (4.7). Let $0 \leq k \leq m+1$ be such that we have*

$$\mu(\mathcal{E}_1) > \mu(\mathcal{E}_2/\mathcal{E}_1) > \cdots > \mu(\mathcal{E}_k/\mathcal{E}_{k-1}) > 0 > \mu(\mathcal{E}_{k+1}/\mathcal{E}_k) > \cdots > \mu(\mathcal{E}_m/\mathcal{E}_{m-1}),$$

and let $q_0 = \mu(\mathcal{E}_m/\mathcal{E}_{m-1})$. Let D be a divisor on X such that $\deg D > 0$.

1. *If $\deg D + q_0 < 0$, $h^0(X, (\mathcal{E}_m/\mathcal{E}_k)(D)) = 0$ and $h^0(X, \mathcal{E}(D)) \leq n(1 + \deg D) - (\operatorname{rank} \mathcal{E}_m/\mathcal{E}_k) \cdot (1 + \mu(\mathcal{E}_m/\mathcal{E}_k) + \deg D)$.*
2. *If $\deg D + q_0 > 2g_X - 2$, then $h^0(X, \mathcal{E}(D)) = n(1 - g_X + \deg D)$.*
3. *If $0 \leq \deg D + q_0 \leq 2g_X - 2$, then $h^0(X, \mathcal{E}(D)) \leq n(1 + \deg D)$.*

Proof. We prove the second part first. There are exact sequences for each $i \geq 1$:

$$0 \longrightarrow \mathcal{E}_{m-i}/\mathcal{E}_{m-(i+1)} \longrightarrow \mathcal{E}_m/\mathcal{E}_{m-(i+1)} \longrightarrow \mathcal{E}_m/\mathcal{E}_{m-i} \longrightarrow 0.$$

We have $\mu(\mathcal{E}_{m-i}/\mathcal{E}_{m-(i+1)}) > 2g_X - 2$ for each $i \geq 1$, hence $h^1(\mathcal{E}_{m-i}/\mathcal{E}_{m-(i+1)}) = 0$. It follows that $h^0(\mathcal{E}) = \sum_{i \geq 0} h^0(\mathcal{E}_{m-i}/\mathcal{E}_{m-(i+1)}) = n(1 - g_X + \mu(\mathcal{E}(D))) = n(1 - g_X + \deg D)$. The first and third parts can be proved using the same exact sequences, except that we no longer need to calculate any H^1 (since we are only looking for upper bounds). □

Consider again a reductive group G over $\mathbb{F}_q$ with split maximal torus and Borel subgroup $T \subset B \subset G$. Let V be a finite-dimensional representation of G. If $F \to X$ is a G-torsor, then $\mathcal{V} = F \times_G V$ is a vector bundle over X. If $F = F_g$ for some $g \in G(\mathbb{A}_K)$, then we write $\mathcal{V}_g = F_g \times_G V$. For any Zariski open subset $U \subset X$, we can identify

$$H^0(U, \mathcal{V}_g) = V(K) \cap \prod_{v \in U} g_v V(\mathcal{O}_{K_v}). \tag{4.9}$$

If V has 'small height', then we can describe the Harder–Narasimhan filtration of $\mathcal{V}$ explicitly. Let $F_P \to X$ denote the canonical reduction of F. For each rational number q, we define

$$V_q = \bigoplus_{\substack{\lambda \in X^*(T) \\ \langle \sigma_{F_P}, \lambda \rangle \geq q}} V_\lambda \subset V, \tag{4.10}$$

$V_\lambda \subset V$ denoting the λ-weight space. This defines a decreasing filtration $V_\bullet$ of V. The subspaces are P-invariant, and the action of P on the graded pieces factors through the Levi quotient L_P (see [Sch15, Lemma 5.1]). By pushout, we get a filtration $\mathcal{V}_\bullet = F_P \times_P V_q$ of $\mathcal{V}$ by subbundles indexed by rational numbers q. We then have the following result.

Theorem 4.6. *Let V be a finite-dimensional representation of G, and let $\check{\rho} \in X_*(T)_{\mathbb{Q}}$ denote the sum of the fundamental coweights. Suppose that for all weights $\lambda \in X^*(T)$ such that $V_\lambda \neq 0$, we have $2\langle \check{\rho}, \lambda \rangle < \operatorname{char} \mathbb{F}_q$. (This condition depends only on the pair (G, V) and not on the choice of T or B.) Then:*

1. *Each associated bundle $\operatorname{gr}_q \mathcal{V}_\bullet \cong F_P \times_P \operatorname{gr}_q V_\bullet$ is (either non-zero or) semi-stable of slope q.*
2. *The subbundles $\mathcal{V}_q = F_P \times_P V_q$ of $\mathcal{V}$ are the constituents of the Harder–Narasimhan filtration of $\mathcal{V} = F \times_G V$.*

Proof. The calculation of [Sch15, Proposition 5.1] goes over verbatim to show that the associated bundles of the graded pieces have the claimed slopes. What we need to justify here is that they are semi-stable. In *loc. cit.* this is justified by appeal to the results of [RR84], which apply when the ground field has characteristic 0. In the present case we can appeal instead to the main theorem of [IMP03], which is extended to reductive groups G as [BH04, Proposition 4.9]. □

We conclude this section by applying the preceding results to the pair (G, V) constructed in §3. We therefore assume now that $\operatorname{char} \mathbb{F}_q > 3$. We recall that G has the root basis $R = \{a_1, a_2, a_3, a_4\}$. We write $R^- = -R$ for the negative of this root basis, and $B \subset G$ for the Borel subgroup corresponding to R^-. We call a parabolic subgroup $P \subset G$ containing B a standard parabolic; any such parabolic has a canonical Levi decomposition $P = L_P N_P$, where L_P is the unique Levi subgroup of P which contains the maximal torus T.

If $P \subset G$ is a standard parabolic subgroup, and D is a divisor on X, then we define a further decomposition of $\mathcal{Y}_{G,P} \subset \mathcal{Y}_G$ as follows:

$$\mathcal{Y}_{G,P} = \mathcal{Y}_{G,P}(D)^{<0} \sqcup \mathcal{Y}_{G,P}(D)^{\mathrm{sp}} \sqcup \mathcal{Y}_{G,P}(D)^{>2g_X-2}.$$

where $\mathcal{Y}_{G,P}(D)^{<0}$ denotes the set of G-torsors $F \to X$ for which the lowest slope piece of the Harder–Narasimhan filtration of $F \times_G V$ has slope q_0 satisfying $\deg D + q_0 < 0$; $\mathcal{Y}_{G,P}(D)^{\mathrm{sp}}$ the set for which $0 \leq \deg D + q_0 \leq 2g - 2$; and $\mathcal{Y}_{G,P}(D)^{>2g_X-2}$ the set for which $\deg D + q_0 > 2g_X - 2$. We can reformulate Corollary 4.5 as follows:

Corollary 4.7. *Let $g = [(g_v)_v] \in \mathcal{Y}_{G,P}$, and let $F_P \to X$ denote the canonical reduction of F_g. Suppose that $\deg D > 0$, and let $M \subset \Phi_V$ denote the set of weights $a \in \Phi_V$ such that $\langle \sigma_{F_P}, a \rangle + \deg D < 0$. Then:*

1. *If $g \in \mathcal{Y}_{G,P}(D)^{<0}$ (i.e. M is non-empty), then $|H^0(X, \mathcal{V}_g(D))| \leq q^{\dim V(1+\deg D) - |M|(1+\deg D + \sum_{a \in M} \langle \sigma_{F_P}, a \rangle)}$.*
2. *If $g \in \mathcal{Y}_{G,P}(D)^{sp}$, then $|H^0(X, \mathcal{V}_g(D))| \leq q^{\dim V(1+\deg D)}$.*
3. *If $g \in \mathcal{Y}_{G,P}(D)^{>2g_X-2}$, then $|H^0(X, \mathcal{V}_g(D))| = q^{\dim V(1-g_X+\deg D)}$.*

We can combine these ideas with Lemma 3.2 to obtain the following useful principle:

Corollary 4.8. *Let $P \subset G$ be a standard parabolic subgroup, and suppose that $\dim Z_0(L_P) \leq 2$. Let D be a divisor on X, and let $g \in \mathcal{Y}_{G,P}(D)^{<0}$. Then for all $v \in H^0(X, \mathcal{V}_g(D))$, we have $\Delta(v) = 0$ (as a section of $H^0(X, \mathcal{O}_X(24D))$).*

Proof. Let $D = \sum_v n_v \cdot v$. If $P \subset G$ satisfies $\dim Z_0(L_P) \leq 2$, then the lowest slope piece of the Harder–Narasimhan filtration of $\mathcal{V}_g$ has dimension at least 4. (It's helpful to recall here that G is isogenous to SL_2^4, and V is then identified with the tensor product of the four 2-dimensional standard representations.) Under the identification

$$H^0(X, \mathcal{V}_g(D)) = V(K) \cap \prod_v \varpi_v^{-n_v} g_v V(\mathcal{O}_{K_v}) \subset V(K),$$

we see that any $v \in H^0(X, \mathcal{V}_g(D))$ must satisfy the condition of the first part of Lemma 3.2, and therefore satisfy $\Delta(v) = 0$. □

5 Counting 2-Selmer elements

In this section, we describe the relation between the representation (G, V) of §3 and the family of pointed elliptic curves (E, P, Q) described in §2. We proceed from the rational theory, to the integral theory, and finally combine this with the other results established so far to prove our main theorems (Theorem 5.9 and Theorem 5.11 below).

We assume throughout §5 that $\mathbb{F}_q$ is a finite field of characteristic ≥ 19, and let (G, V) denote the representation considered in §3.

5.1 (G, V) and 2-descent

Theorem 5.1. *We can find homogeneous generators $p_2, p_4, q_4, p_6 \in \mathbb{F}_q[V]^G$ (of degrees 2, 4, 4, and 6, respectively) and a 5-dimensional affine linear subspace $\Sigma \subset V$ together with functions $x, y \in \mathbb{F}_q[\Sigma]$ such that:*

1. *The functions $p_2, p_4, q_4, x, y \in \mathbb{F}_q[\Sigma]$ generate $\mathbb{F}_q[\Sigma]$.*
2. *The relation $y(xy + 2q_4) = x^3 + p_2x^2 + p_4x + p_6$ holds on Σ.*

Proof. This theorem follows from [Tho13, Theorem 3.8] when $\mathbb{F}_q$ is replaced by a field of characteristic 0. The same proof works over $\mathbb{F}_q$, with our restrictions on the characteristic. This is unsurprising, given that the results of Slodowy [Slo80] are proved in positive characteristic with the same restrictions. We explain the construction. Define a matrix

$$e = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}$$

and a cocharacter $\check{\lambda} \in X_*(T')$

$$\check{\lambda}(t) = \mathrm{diag}(t^2, t, t^{-1}, t^{-2}, 1, t, t^{-1}, 1).$$

Then $\mathrm{Ad}\,\check{\lambda}(t)(e) = te$ and $e \in V$ is a subregular nilpotent element. Therefore we can find a unique subregular nilpotent $f \in V$ such that the triple $(e, d\check{\lambda}(2), f)$ is a normal $\mathfrak{sl}_2$-triple. We define $\Sigma = e + \mathfrak{z}_{\mathfrak{h}}(f)^{d\theta=-1}$.

If $t \in \mathbb{G}_m$, then the action $t \cdot v = t\,\mathrm{Ad}\,\check{\lambda}(t^{-1})(v)$ leaves Σ invariant and contracts Σ to the fixed base point e; moreover, the morphism $\pi|_\Sigma$ is then $\mathbb{G}_m$-equivariant. The functions $x, y \in \mathbb{F}_q[\Sigma]$ are chosen to have weight 2 with respect to this action. □

At this point there are two natural discriminant polynomials Δ in $\mathbb{F}_q[V]^G$ that one might consider; the one arising from the usual Lie algebra discriminant in $\mathfrak{h}$, and the discriminant of the polynomial $f(t) = t^4 + p_2t^3 + p_4t^2 + p_6t + q_4^2$, which is used in §2. In fact, these two functions are equal up to $\mathbb{F}_q^\times$-multiple, because they both cut out the same irreducible divisor in $B = \operatorname{Spec} \mathbb{F}_q[V]^G$. Since the precise value of Δ will not be important for us, but rather only its order of vanishing, we will use the symbol Δ to denote either one of these polynomials in $\mathbb{F}_q[V]^G = \mathbb{F}_q[p_2, p_4, q_4, p_6]$.

We write $S \to B$ for the natural compactification of Σ as a family of projective plane curves given by the equation

$$Y(XY + 2q_4Z^2) = X^3 + p_2X^2Z + p_4XZ^2 + p_6Z^3. \tag{5.1}$$

We write O, P, and Q for the three sections of $S - \Sigma$ at infinity given respectively by $[0 : 1 : 0]$, $[-1 : 1 : 0]$ and $[1 : 1 : 0]$. We write S^{rs} for the restriction of this family to B^{rs}. The fundamental relation between the pair (G, V) and this family of curves is as follows:

Theorem 5.2. *1. The morphism $S \to B$ is smooth exactly above B^{rs}. Consequently, $S^{rs} \to B^{rs}$ is a family of smooth, projective, geometrically connected curves.*

2. Let $J_{S^{rs}} = \operatorname{Pic}^0_{S^{rs}/B^{rs}}$ denote the (relative) Jacobian of this family, and let Z^{rs} denote the equalizer of the diagram

$$G \times \kappa^{rs} \underset{(g,x)\mapsto x}{\overset{(g,x)\mapsto g\cdot x}{\rightrightarrows}} V^{rs}$$

viewed as a finite étale group scheme over $\kappa^{rs} \cong B^{rs}$. Then there is a canonical isomorphism $J_{S^{rs}}[2] \cong Z^{rs}$ of finite étale group schemes over B^{rs}.

3. Let $k/\mathbb{F}_q$ be a field, and let $b \in B^{rs}(k)$. Consider the diagram

$$\begin{array}{ccc} \Sigma_b(k) & \longrightarrow & G(k)\backslash V_b(k) \\ \downarrow & & \downarrow \\ J_b(k) & \longrightarrow & H^1(k, J_b[2]), \end{array}$$

where the top arrow is the canonical inclusion; the left arrow is the map $R \mapsto [(R) - (O)]$; the right arrow is the injection of Corollary 3.4, composed with the isomorphism $H^1(k, Z_G(\kappa_b)) \cong H^1(k, J_b[2])$; and the bottom arrow is the canonical 2-descent map on the Jacobian J_b. Then there exists a class $x_b \in H^1(k, J_b[2])$ arising from a trivial orbit such that this diagram commutes up to addition of x_b.

Proof. The first part is established over a field of characteristic 0 in [Tho13, Corollary 3.16], using a reduction to [Slo80], and again the same proof works in our positive characteristic setting. This is not the case for the second part, where the corresponding fact is established in [Tho13, Corollary 4.12] using analytic techniques. However, the same construction works to show that there is a map $J_{S^{\mathrm{rs}}}[2] \to Z^{\mathrm{rs}}$ of local systems of $\mathbb{F}_2$-vector spaces on B^{rs}. To check that it is an isomorphism, it suffices to check that it is an isomorphism on a single stalk, and this can easily be accomplished by lifting to characteristic 0 and applying [Tho13, Corollary 4.12].

The third part has been established in characteristic 0 in [Tho13, Theorem 4.15], which also shows how to calculate the element x_b using the geometry of the curve S. We describe the recipe, although it is not strictly necessary for what we do here. Let $0 \in B(\mathbb{F}_q)$ be the central point. Then the curve S_0 is a union of three lines. Let $S_0' \subset S_0$ be the branch containing the section O at infinity, and let $E' \in S_0'(\mathbb{F}_q) - \{e\}$ be a rational point. Then there exists a unique $w \in W_0$ such that wE' is conjugate by $G(\overline{\mathbb{F}}_q)$ to κ_0, and for any $b \in B(k)$ we can then take x_b to be the class corresponding to the orbit of $w\kappa_b \in V(k)$.

We still need to extend this result to positive characteristic. However, this is an essentially formal consequence of the first two parts of the theorem, and follows in exactly the same way as in [Tho13, §4]. □

Theorem 5.3. *Let $k/\mathbb{F}_q$ be a field, and let $b \in B^{rs}(k)$.*

1. *The image of the injective map $G(k)\backslash V_b(k) \to H^1(k, J_b[2])$ appearing in Theorem 5.2 contains the canonical image of $J_b(k)/2J_b(k)$.*

2. *Inside this image, the trivial orbits of $G(k)\backslash V_b(k)$ correspond to the subgroup of $J_b(k)/2J_b(k)$ generated by the divisor classes $[(P) - (O)]$ and $[(Q) - (O)]$.*

Proof. By Theorem 5.2, it is enough to prove the second part of the theorem. By definition, the identity of $H^1(k, J_b[2])$ corresponds to the orbit of the Weierstrass section $\kappa_b \in V_b(k)$. We have a short exact sequence of étale homology groups (where overline denotes base change to a separable closure k^s/k):

$$0 \longrightarrow (\mu_2^3)_{\Sigma=0} \longrightarrow H_1(\overline{\Sigma}_b, \mathbb{F}_2) \longrightarrow H_1(\overline{S}_b, \mathbb{F}_2) \longrightarrow 0. \tag{5.2}$$

Here $(\mu_2^3)_{\Sigma=0} \subset \mu_2^3$ denotes the kernel of the map which sums up co-ordinates. There is a natural symplectic duality $\langle \cdot, \cdot \rangle$ on $H^1(\overline{\Sigma}_b, \mathbb{F}_2)$ with radical $(\mu_2^3)_{\Sigma=0}$, and which descends to the Poincaré duality pairing on $H_1(\overline{S}_b, \mathbb{F}_2)$. Identifying $J_b[2] = H_1(\overline{S}_b, \mathbb{F}_2)$, this allows us to describe the subgroup of $H^1(k, J_b[2])$ generated by the divisors at infinity as follows: it is the image of $(\mu_2^3)^\vee_{\Sigma=0}$ under the connecting homomorphism attached to the dual exact sequence of $\mathbb{F}_2[\Gamma_k]$-modules (with $\Gamma_k = \mathrm{Gal}(k^s/k)$):

$$0 \longrightarrow H_1(\overline{S}_b, \mathbb{F}_2) \longrightarrow H_1(\overline{\Sigma}_b, \mathbb{F}_2)^\vee \longrightarrow (\mu_2^3)^\vee_{\Sigma=0} \longrightarrow 0, \tag{5.3}$$

where we use the aforementioned pairing to identify $H_1(\overline{S}_b, \mathbb{F}_2)^\vee \cong H_1(\overline{S}_b, \mathbb{F}_2)$. We now identify these exact sequences using the representation theory of the pair (G, V). Let H^{sc} denote the simply connected cover of H, and let $G^{\mathrm{sc}} = (H^{\mathrm{sc}})^\theta$; it is a connected subgroup of H. Let C^{sc} denote the centralizer of κ_b in H^{sc}, and C its image in H. Then we can identify $Z_{G^{\mathrm{sc}}}(\kappa_b) = C^{\mathrm{sc}}[2]$, $Z_{H^\theta}(\kappa_b) = C[2]$, and $Z_G(\kappa_b) = \mathrm{im}(C^{\mathrm{sc}}[2] \to C[2])$. The short exact sequence (5.2) is canonically identified with the sequence

$$0 \longrightarrow Z_{G^{\mathrm{sc}}} \longrightarrow C^{\mathrm{sc}}[2] \longrightarrow \mathrm{im}(C^{\mathrm{sc}}[2] \to C[2]) \longrightarrow 0 \tag{5.4}$$

(compare [Tho13, Theorem 4.10] and the proof of Theorem 5.2). Its dual is canonically identified with the sequence

$$0 \longrightarrow Z_G(\kappa_b) \longrightarrow C[2] \longrightarrow \pi_0(H^\theta) \longrightarrow 0, \tag{5.5}$$

using the Weyl-invariant bilinear form on $X_*(C)$ (cf. [Tho13, Lemma 2.11]) and the canonical identification $C[2]/Z_G(\kappa_b) \cong \pi_0(H^\theta)$. The map $W_0 \to \pi_0(H^\theta)$ is an isomorphism, and the composite $W_0 \to \pi_0(H^\theta) \to H^1(k, Z_G(\kappa_b))$ sends an element $w \in W_0$ to the class corresponding to the orbit $G(k) \cdot w\kappa_b$. This concludes the proof. □

The proof of the second part of Theorem 5.3 has a useful corollary: it gives a criterion to tell when the trivial orbits generate a subgroup of $J_b(k)/2J_b(k)$ of order 4 (which one expects to be the case generically). Indeed, taking in mind the identification of the exact sequence (5.3) with the sequence (5.5), one sees that this should be the case exactly when $H^0(k, Z_G(\kappa_b)) = H^0(k, C[2])$. The action of the Galois group Γ_k on $C[2]$ arises from a homomorphism $\Gamma_k \to W(H, C) = W$ giving the action on the torus C, and this condition can be described in terms of the image of this homomorphism inside W. In particular, in the 'generic' case where this image is the whole Weyl group, there will be no additional invariants, and consequently 4 trivial orbits in $G(k)\backslash V_b(k)$.

Corollary 5.4. *Let X be a smooth, projective, geometrically connected curve over $\mathbb{F}_q$, and let $K = \mathbb{F}_q(X)$. Let $b \in B^{rs}(K)$. Then the subset $G(K)\backslash V_b(K) \subset H^1(K, J_b[2])$ appearing in Corollary 3.4 (with $k = K$) contains the 2-Selmer group* $\mathrm{Sel}_2(J_b)$.

Proof. This follows from the fact that the Hasse principle holds for G, i.e. that the map $H^1(K, G) \to \prod_v H^1(K_v, G)$ is injective. □

5.2 (G, V) and local integral orbits

In the previous section, we have studied rational orbits; we now look at the integral situation. Let X be a smooth, projective, geometrically connected curve over $\mathbb{F}_q$, and let $K = \mathbb{F}_q(X)$. Let v be a place of K, and let (E, P, Q) be tuple consisting of an elliptic curve E over K_v with two distinct, non-trivial marked rational points $P, Q \in E(K_v)$. We assume that the minimal model (as in §2) of (E, P, Q) has squarefree discriminant, and let $b = (p_2, p_4, q_4, p_6) \in B(\mathcal{O}_{K_v})$ denote the associated set of invariants. We write J_b for the Jacobian of E, which we identify with E via the map $R \mapsto (R) - (O)$.

Theorem 5.5. *With assumptions as above, let $\mathcal{J}_b$ denote the Néron model of E over $\mathcal{O}_{K_v}$. Then:*

1. *The map $H^1(\mathcal{O}_{K_v}, \mathcal{J}_b[2]) \to H^1(K_v, J_b[2])$ in étale cohomology is injective.*
2. *An orbit in $G(K_v)\backslash V_b(K_v)$ admits an integral representative (i.e. intersects $V_b(\mathcal{O}_{K_v})$) if and only if it corresponds to an element of $J_b(K_v)/2J_b(K_v)$.*
3. *Suppose that $x, y \in V_b(\mathcal{O}_{K_v})$ and $\gamma \in G(K_v)$ satisfies $\gamma x = y$. Then $\gamma \in G(\mathcal{O}_{K_v})$.*

Proof. We have $H^1(\mathcal{O}_{K_v}, \mathcal{J}_b[2]) = H^1(k(v), \mathcal{J}_b[2](\kappa(v)))$. Since the discriminant is square-free, we have $\mathcal{J}_b[2](\kappa(v)) = J_b[2](K_v^s)^{I_{K_v}}$, so the injectivity of the first part is a consequence of inflation-restriction.

For the 'if' of the second part, we use the existence of the section $\Sigma \subset V$, which shows (together with the commutative diagram of Theorem 5.2) that any element of $J_b(K_v)/2J_b(K_v)$ which can be represented by a divisor $(R) - (O)$, where $R \in \Sigma_b(\mathcal{O}_{K_v})$, is represented by an element of $V(\mathcal{O}_{K_v})$. Since the trivial orbits have integral representatives, essentially by definition, this reduces us to showing that any non-trivial orbit in $J_b(K_v)/2J_b(K_v)$ is represented by such a divisor $(R) - (O)$. We have a short exact sequence

$$0 \longrightarrow \mathcal{J}_b(\mathcal{O}_{K_v})^0 \longrightarrow J_b(\mathcal{O}_{K_v}) \longrightarrow \mathcal{J}_b(k(v)) \longrightarrow 0,$$

where the kernel is a pro-p-group ($p = \operatorname{char} \mathbb{F}_q$), hence an isomorphism

$$\mathcal{J}_b(\mathcal{O}_{K_v})/2\mathcal{J}_b(\mathcal{O}_{K_v}) \cong \mathcal{J}_b(k(v))/2\mathcal{J}_b(k(v)) \cong H^1(\mathcal{O}_{K_v}, \mathcal{J}_b[2]).$$

If $[\overline{x}] \in \mathcal{J}_b(k(v))/2\mathcal{J}_b(k(v))$ is a non-trivial class (i.e. not in the subgroup generated by the 3 marked points of E at infinity), we can choose a representative $\overline{x} \in \mathcal{J}_b(k(v))$ of the form $(\overline{R}) - (\overline{O})$, where $\overline{R} \in \Sigma_b(k(v))$. Lifting $\overline{R}$ to a point $R \in \Sigma_b(\mathcal{O}_{K_v})$ via Hensel's lemma then shows the existence of the desired integral representative in $V_b(\mathcal{O}_{K_v})$.

We now turn to the 'only if' of the second part. We first note that any element $x \in V_b(\mathcal{O}_{K_v})$ in fact lies in $V_b^{\mathrm{reg}}(\mathcal{O}_{K_v})$, i.e. $\overline{x} = x \bmod (\varpi_v)$ is regular in $V_{k(v)}$. This is clear if $\Delta(v)$ is a unit in $\mathcal{O}_{K_v}$. Otherwise, we note that $\overline{x}$ is regular in $V_{k(v)}$ if and only if it is regular in $\mathfrak{h}_{k(v)}$; and if it is not regular in $\mathfrak{h}_{k(v)}$, then its centralizer has dimension at least $\dim T + 2$ (see [SS70, III. 3.25]). Let $\mathfrak{c} = \mathfrak{z}_{\mathfrak{h}_{K_v}}(x)$, $\mathfrak{c}^0 = \mathfrak{c} \cap \mathfrak{h}_{\mathcal{O}_{K_v}}$. Let $f : \mathfrak{h}_{\mathcal{O}_{K_v}}/\mathfrak{c}^0 \to \mathfrak{h}_{\mathcal{O}_{K_v}}/\mathfrak{c}^0$ denote the morphism induced by $\operatorname{ad} x$ after passage to quotient. We have the relation $\det f = \Delta(x)$, up to units in $\mathcal{O}_{K_v}^\times$. If $\overline{x}$ is not regular, then $\overline{f} = f \bmod (\varpi_v)$ has kernel of dimension at least 2, hence $\operatorname{ord}_{K_v} \det f \geq 2$, a contradiction.

We next observe that the map $G_{\mathcal{O}_{K_v}} \to V_b^{\mathrm{reg}}$, $g \mapsto g \cdot \kappa_b$, is étale, and a torsor over its image $V_b^{\mathrm{reg},\,0} \subset V_b^{\mathrm{reg}}$ for the étale group scheme $Z_{G_{\mathcal{O}_{K_v}}}(\kappa_b)$ over $\mathcal{O}_{K_v}$. Moreover, we have $V_b^{\mathrm{reg}} = \cup_{w \in W_0} w \cdot V_b^{\mathrm{reg},\,0}$ (by [Lev07, Theorem 0.17]). It follows that there is a canonical bijection

$$G(\mathcal{O}_{K_v})\backslash V_b^{\mathrm{reg},\,0}(\mathcal{O}_{K_v}) \cong H^1(\mathcal{O}_{K_v}, Z_{G_{\mathcal{O}_{K_v}}}(\kappa_b)). \tag{5.6}$$

The isomorphism $Z_G(\kappa_b) \cong J_b[2]$ extends uniquely to an isomorphism $Z_{G_{\mathcal{O}_{K_v}}}(\kappa_b) \cong \mathcal{J}_b[2]$. If Δ is a unit, then this is immediate from Theorem 5.2. If Δ is not a unit, then it suffices to show that the isomorphism $Z_G(\kappa_b) \cong J_b[2]$ identifies $Z_G(\kappa_b)(\kappa(v)) \subset Z_G(\kappa_b)(K_v^s)^{I_v}$ with $\mathcal{J}_b[2](\kappa(v)) \subset J_b[2](K_v^s)^{I_v}$. Since the latter group has order 2, it is enough to show that $Z_G(\kappa_b)(\kappa(v))$ is non-trivial. This follows from the fact that $\Sigma_{\overline{b}}$ has a unique singularity of type A_1, as we now show. Let $\overline{b} = b \bmod (\varpi_v)$. The element $\kappa_{\overline{b}} \in V(k(v))$ has

a Jordan decomposition $\kappa_{\overline{b}} = v_s + v_n$ as a sum of commuting semi-simple and nilpotent parts, and we can compute (using the same technique as in [Tho13, Proposition 2.8])

$$Z_G(\kappa_{\overline{b}}) = Z_{Z_{G^{\mathrm{sc}}}(v_s)}[2]/Z_{G^{\mathrm{sc}}}. \tag{5.7}$$

The fact that $\Sigma_{\overline{b}}$ has a singularity of type A_1 implies ([Tho13, Corollary 3.16], the proof of which goes over without change in our setting) that $Z_{G^{\mathrm{sc}}}(v_s)$ has derived group of type A_1. In particular, its centre contains a torus of rank 3, and consequently the group appearing in (5.7) must be non-trivial.

We can thus enlarge (5.6) to a commutative diagram

$$\begin{array}{ccc} G(\mathcal{O}_{K_v})\backslash V_b^{\mathrm{reg},\,0}(\mathcal{O}_{K_v}) & \longrightarrow & H^1(\mathcal{O}_{K_v}, \mathcal{J}_b[2]) \\ \downarrow & & \downarrow \\ G(K_v)\backslash V_b(K_v) & \longrightarrow & H^1(K_v, J_b[2]). \end{array} \tag{5.8}$$

This shows that any element of $G(K_v)\backslash V_b(K_v)$ which is in the image of the left-hand vertical arrow lies in the image of $H^1(\mathcal{O}_{K_v}, \mathcal{J}_b[2]) \cong J_b(K_v)/2J_b(K_v) \subset H^1(K_v, J_b[2])$. Since we have $V_b^{\mathrm{reg}} = \cup_{w \in W_0} w V_b^{\mathrm{reg},\,0}$, and w acts on $H^1(K_v, J_b[2])$ as translation by trivial orbits, we finally see that any element of $G(K_v)\backslash V_b(K_v)$ which admits an integral representative corresponds to an element of $J_b(K_v)/2J_b(K_v)$.

Finally, we come to the third part of the theorem. The integrality is insensitive to passage to unramified extensions of K_v, so we reduce to the statement that the étale group scheme $Z_{H^\theta_{\mathcal{O}_{K_v}}}(\kappa_b)$ satisfies the Néron mapping property, i.e. its K_v-points all extend to $\mathcal{O}_{K_v}$-points. If Δ is a unit then this étale group scheme is finite étale. If $\mathrm{ord}_{K_v} \Delta = 1$, then we have seen that the action of inertia on $Z_{G_{\mathcal{O}_{K_v}}}(\kappa_b)(K_v^s)$ is non-trivial, so $|Z_{H^\theta_{\mathcal{O}_{K_v}}}(\kappa_b)(K_v)| \leq 2^3$. On the other hand, using again the Jordan decomposition $\kappa_{\overline{b}} = v_s + v_n$, we have

$$Z_{H^\theta}(\kappa_{\overline{b}})(\kappa(v)) = Z_{Z_{H^\theta}(v_s)}(\kappa(v))[2],$$

and this group has size at least 2^3. This shows that the desired property of $Z_{H^\theta_{\mathcal{O}_{K_v}}}(\kappa_b)$ does hold, and completes the proof of the theorem. □

5.3 (G, V) and global integral orbits

We can now discuss the global picture. Let X be a smooth, projective, geometrically connected curve over $\mathbb{F}_q$, and let $K = \mathbb{F}_q(X)$. Let $D = \sum_v m_v \cdot v$ be a divisor on X, and let $(E, P, Q) \in \mathcal{X}_D$. We recall (see §2) that this means that E is an elliptic curve over K with two distinct non-trivial marked rational points $P, Q \in E(K)$, and which can be represented by an equation

$$y(xy + 2q_4) = x^3 + p_2x^2 + p_4x + p_6 \tag{5.9}$$

with

$$b = (p_2, p_4, q_4, p_6) \in H^0(X, \mathcal{O}_X(2D) \oplus \mathcal{O}_X(4D) \oplus \mathcal{O}_X(4D) \oplus \mathcal{O}_X(6D)) = H^0(X, B_D) \subset B(K) \tag{5.10}$$

of square-free discriminant in $H^0(X, \mathcal{O}_X(24D))$. (The reason for restricting to curves with $\mathcal{L}_E$ a square is that the invariant degrees of the representation (G, V) then agree with the weights of the equation (5.9) defining the curve E.)

Let $x \in V_b(K)$ be an element corresponding to an element of the group $\mathrm{Sel}_2(E)$ (see Corollary 5.4). Then for every place v of K, $\varpi_v^{m_v} x$ has minimal, integral invariants $\pi(\varpi_v^{m_v} x) = \varpi_v^{m_v} \cdot b \in \mathcal{O}_{K_v}^4$ of squarefree discriminant, and Theorem 5.5 implies that we can find $g_v \in G(K_v)$ such that $\varpi_v^{m_v} x \in g_v V(\mathcal{O}_{K_v})$. For almost all places v, we have $m_v = 0$ and can choose $g_v = 1$. Moreover, g_v is defined up to right multiplication by $G(\mathcal{O}_{K_v})$, by the third part of Theorem 5.5. If we replace x by γx for some $\gamma \in G(K)$, then g_v can be replaced by γg_v. We have therefore defined a map

$$\mathrm{inv} : \mathrm{Sel}_2(E) \to G(K)\backslash G(\mathbb{A}_K)/G(\widehat{\mathcal{O}}_K). \tag{5.11}$$

It is clear that this map depends only on (E,P,Q) and not on the choice of equation $b \in H^0(X,\mathcal{O}_X(D))$ representing (E,P,Q) (since all choices differ by the action of $\mathbb{F}_q^\times$).

To any $g \in G(\mathbb{A}_K)$, we associate the G-torsor F_g and the vector bundle $\mathcal{V}_g = F_g \times_G V$, which has sections described by (4.9). The above discussion shows that if $[g] = \mathrm{inv}(x)$, then x naturally defines a element of

$$V(K) \cap \prod_v g_v \varpi_v^{-m_v} V(\mathcal{O}_{K_v}) = H^0(X, \mathcal{V}_g(D)),$$

and the image of x under the map $\pi : H^0(X,\mathcal{V}_g(D)) \to H^0(X,B_D)$ equals b. We have constructed the first map in the following:

Theorem 5.6. *Let $(E,P,Q) \in \mathcal{X}_D$ be represented by $b \in H^0(X,B_D)$. We identify $E = J_b$ using the map $R \mapsto (R)-(O)$. Let $g = (g_v)_v \in G(\mathbb{A}_K)$. Then the following two sets are in canonical bijection:*

1. *The set of elements $x \in \mathrm{Sel}_2(E)$ such that $\mathrm{inv}(x) = [(g_v)_v]$.*
2. *The set of sections $s \in H^0(X,\mathcal{V}_g(D))$ such that $\pi(s) = b$, taken up to the action of the group $\mathrm{Aut}(F_g)$.*

Proof. We have constructed the map from the first set to the second set. We now construct its inverse. Let s be a global section in

$$H^0(X,\mathcal{V}_g(D)) = V(K) \cap \prod_v g_v \varpi_v^{-m_v} V(\mathcal{O}_{K_v})$$

such that $\pi(s) = b$. Writing x for the image of s in $V(K)$ under the canonical inclusion, we obtain an orbit in $G(K)\backslash V_b(K)$. This orbit is independent of the choice of representative in the $\mathrm{Aut}(F_g)$-orbit of s; indeed, we have $\mathrm{Aut}(F_g) = G(K) \cap gG(\widehat{\mathcal{O}}_K)g^{-1}$, so replacing s by γs for $\gamma \in \mathrm{Aut}(F_g)$ would just replace x by γx, leaving the $G(K)$-orbit of x unchanged.

We need to show that x lies in the subset of $G(K)\backslash V_b(K)$ corresponding to the 2-Selmer group. However, this follows from the second part of Theorem 5.5 and the fact that s has square-free discriminant. It is clear from the construction that this map is inverse to the other, so this completes the proof. □

To illustrate the construction of this invariant map, we calculate its image when applied to the trivial elements in $J_b(K)/2J_b(K) \subset \mathrm{Sel}_2(J_b)$. Recall that we have defined $\kappa = E + \mathfrak{z}_{\mathfrak{h}}(F)$, where $(E, d\check{\rho}(2), F)$ is a regular normal $\mathfrak{sl}_2$-triple in $\mathfrak{h}$. The action $t \cdot x = t \operatorname{Ad} \check{\rho}(t^{-1})(x)$ leaves κ invariant and contracts to the unique fixed point E (see Proposition 3.3). In particular, if v is a place of K, $b \in B(K_v)$, and $\lambda \in K_v^\times$, then we have the following formula giving the behaviour of the Kostant section under scaling:

$$\kappa_{\lambda b} = \check{\rho}(\lambda^{-1})\lambda\kappa_b. \tag{5.12}$$

If $b \in B(\mathcal{O}_{K_v})$, then $\kappa_b \in V(\mathcal{O}_{K_v})$ is an integral representative of the orbit in $V_b(K)$ corresponding to the identity element of $\mathrm{Sel}_2(J_b)$. If $b \in H^0(X,B_D) \subset B(K)$ is associated to a pointed curve as above, then we find $\varpi_v^{m_v} b \in B(\mathcal{O}_{K_v})$ is the minimal integral representative, hence

$$\kappa_{\varpi_v^{m_v} b} = \check{\rho}(\varpi_v^{-m_v})\varpi_v^{m_v} b \in \varpi_v^{m_v} V(\mathcal{O}_{K_v}). \tag{5.13}$$

It then follows from the definition that we have $\mathrm{inv}(\kappa_b) = [(\check{\rho}(\varpi_v^{m_v}))_v]$. The same formalism applies to the other trivial orbits: if $w \in W_0$, then the representative of the corresponding trivial orbit in $V(K)$ is $w\kappa_b$. For each place v of K, we have

$$w\check{\rho}(\varpi_v^{-m_v})w^{-1}\varpi_v^{m_v} w\kappa_b = w\check{\rho}(\varpi_v^{-m_v})\varpi_v^{m_v}\kappa_b \in \varpi_v^{m_v} V(\mathcal{O}_{K_v}), \tag{5.14}$$

so it follows from the definition that we have $\mathrm{inv}(w\kappa_b) = [(w\check{\rho}(\varpi_v^{m_v})w^{-1})_v]$. This implies in particular:

Lemma 5.7. *Let $(E,P,Q) \in \mathcal{X}_D$ be represented by $b \in H^0(X,B_D)$, and let $x \in \mathrm{Sel}_2(J_b)$ be a trivial element. Suppose that $\deg D > 0$. Then $\mathrm{inv}(x) \in \mathcal{Y}_{G,B}(D)^{<0}$.*

Proof. We just treat the case of κ_b, since the other cases are very similar. We need to show that $g = ((\check{\rho}(\varpi_v^{m_v}))_v)$ lies in $B(\mathbb{A}_K)^{\mathrm{pos,\ ss}}$ and that the 'lowest slope' part of $\mathcal{V}_g(D)$ has strictly negative slope. Since the Levi quotient of B is a torus, the semi-stability condition is vacuous, so we must check is that for all $a \in R^-$, we have $\log_q \|a((\check{\rho}(\varpi_v^{m_v}))_v)\| > 0$. We compute

$$\log_q \|a((\check{\rho}(\varpi_v^{m_v}))_v)\| = -\langle \check{\rho}, a\rangle \cdot \deg D > 0.$$

The lowest slope part of $\mathcal{V}_g(D)$ has slope

$$\log_q \|\alpha_0((\check{\rho}(\varpi_v^{m_v}))_v)\| = -\langle \check{\rho}, \alpha_0\rangle \cdot \deg D + \deg D = -2\deg D < 0,$$

as required. □

5.4 The main theorem

We once again suppose that$X$ be a smooth, projective, geometrically connected curve over $\mathbb{F}_q$, and let $K = \mathbb{F}_q(X)$. If D is a divisor on X, then we write $H^0(X, B_D)^{\mathrm{sf}} \subset H^0(X, B_D)$ for the set of elements of square-free discriminant $\Delta \in H^0(X, \mathcal{O}_X(24D))$. Then (Corollary 2.4) there is a surjection $H^0(X, B_D)^{\mathrm{sf}} \to \mathcal{X}_D$, the fibre above a given isomorphism class $[(E, P, Q)]$ having cardinality equal to $\mathbb{F}_q^\times \cdot |\operatorname{Aut}(E, P, Q)|^{-1}$. If $g = [(g_v)_v] \in \mathcal{Y}_G$, then we write $H^0(X, \mathcal{V}_g(D))^{\mathrm{sf}} \subset H^0(X, \mathcal{V}_g(D))$ for the pre-image of $H^0(X, B_D)^{\mathrm{sf}}$. We also write $H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,nt}} \subset H^0(\mathcal{V}_g(D))^{\mathrm{sf}}$ for the set of elements of $H^0(\mathcal{V}_g(D))^{\mathrm{sf}}$ which are non-trivial when viewed inside $V(K)$ (in the sense of Lemma 3.5).

Proposition 5.8. *Let $g = (g_v)_v \in G(\mathbb{A}_K)$.*

1. *The limit*
$$\delta_B = \lim_{\deg D \to \infty} \frac{|H^0(X, B_D)^{sf}|}{|H^0(X, B_D)|}$$
exists and is strictly positive.

2. *The limit*
$$\delta_V = \lim_{\deg D \to \infty} \frac{|H^0(X, \mathcal{V}_g(D))^{sf}|}{|H^0(X, \mathcal{V}_g(D))|}$$
exists and is strictly positive, and does not depend on g.

3. *We have $\int_{g \in G(\widehat{\mathcal{O}}_K)} d\tau_G \delta_B = q^{12(g_X - 1)}\delta_V$, where τ_G denotes the Tamagawa measure on $G(\mathbb{A}_K)$.*

Proof. If v is a place of K, define

$$\alpha_v = \frac{|\{x \in B(\mathcal{O}_{K_v}/(\varpi_v^2)) \mid \Delta(x) \equiv 0 \bmod \varpi_v^2\}|}{q_v^8}$$

and

$$\beta_v = \frac{|\{x \in V(\mathcal{O}_{K_v}/(\varpi_v^2)) \mid \Delta(x) \equiv 0 \bmod \varpi_v^2\}|}{q_v^{32}}.$$

In [HLHN14, §5.1] it is proved using results of Poonen [Poo03] that the limit δ_V exists and equals $\prod_v (1-\beta_v)$. A similar argument using the results of [Poo03] shows that the limit δ_B exists and equals $\prod_v (1-\alpha_v)$. It is easy to see that both of these products are strictly positive. To finish the proof of the proposition, we need to show that $\int_{g \in G(\widehat{\mathcal{O}}_K)} d\tau_G \delta_B = q^{12(g_X-1)}\delta_V$, or even (using the definition of the Tamagawa measure) that $\int_{g \in G(\mathcal{O}_{K_v})} |\omega_G|_v (1-\alpha_v) = (1-\beta_v)$ for each place v of K, ω_G being an invariant differential form of top degree on G (over $\mathbb{F}_q$). We will establish this using an integral formula.

Let ω_V and ω_G be invariant differential forms of top degree on V and G, respectively. Let $\omega_B = dp_2 \wedge dp_4 \wedge dq_4 \wedge dp_6$, a differential form of top degree on B. Let $\varphi : B(K_v) \to \mathbb{R}$ denote the characteristic function of the open subset of $b \in B(\mathcal{O}_{K_v})$ where $\operatorname{ord}_{K_v} \Delta(b) \leq 1$. Let $f : V(K_v) \to \mathbb{R}$ denote the

characteristic function of the open subset of $x \in V(\mathcal{O}_{K_v})$ where $\mathrm{ord}_{K_v} \Delta(x) \leq 1$. Then we must show the identity

$$\int_{g \in G(\mathcal{O}_{K_v})} |\omega_G|_v \int_{b \in B(K_v)} \varphi(b)\, |\omega_B|_v = \int_{x \in V(K_v)} f(x)\, |\omega_V|_v.$$

If $\mathfrak{c} \subset V_{K_v}$ is a Cartan subspace, we write $\mu_{\mathfrak{c}} : G_{K_v} \times \mathfrak{c} \to V_{K_v}$ for the action map. Exactly the same argument as in [Tho15, Proposition 2.13] shows that for any Cartan subspace $\mathfrak{c} \subset V_{K_v}$, we have an identity

$$\mu_{\mathfrak{c}}^* \omega_V = \lambda \omega_G \wedge \pi|_{\mathfrak{c}}^* \omega_B$$

for some scalar $\lambda \in \mathbb{F}_q^\times$ which is independent of the choice of Cartan subspace.

Let $\mathfrak{c}_1, \dots, \mathfrak{c}_s \subset V_{K_v}$ denote representatives for the distinct $G(K_v)$-conjugacy classes of Cartan subspaces. Each element $v \in V^{\mathrm{rs}}(K_v)$ is contained in a unique Cartan subspace, so we obtain an identity

$$\int_{x \in V(\mathcal{O}_{K_v})} f(x)\, |\omega_V|_v = \sum_{i=1}^{s} \int_{(g, c_i) \in G(K_v) \times \mathfrak{c}_i} \frac{f(g c_i)}{N_G(\mathfrak{c}_i)(K_v)}\, |\lambda|_v |\omega_G \wedge \pi|_{\mathfrak{c}}^* \omega_B|_v.$$

Let $\mathfrak{c}_i^0 = \mathfrak{c}_i \cap [G(K_v) \cdot V(\mathcal{O}_{K_v})]$, an open subset of $\mathfrak{c}_i$. It follows from Theorem 5.5 and the invariance of the measure $|\omega_G|_v$ that this last integral is equal to

$$\sum_{i=1}^{s} \int_{g \in G(\mathcal{O}_{K_v})} |\omega_G|_v \int_{c_i \in \mathfrak{c}_i} \frac{\varphi(\pi(c_i))}{N_G(\mathfrak{c}_i)(K_v)} |\lambda|_v |\pi|_{\mathfrak{c}}^* \omega_B|_v$$

$$= \sum_{i=1}^{s} \int_{g \in G(\mathcal{O}_{K_v})} |\omega_G|_v |N_G(\mathfrak{c}_i)(K_v)|^{-1} \int_{b \in B(K_v)} \varphi(b) |\mathfrak{c}_{i,b}(K_v) \cap \mathfrak{c}_i^0| |\omega_B|_v.$$

To finish the proof, we therefore just need to show that if $b \in B(\mathcal{O}_{K_v})$ satisfies $\mathrm{ord}_K \Delta(b) \leq 1$, then

$$\sum_{i=1}^{s} |\mathfrak{c}_{i,b}(K_v) \cap \mathfrak{c}_i^0| \times |N_G(\mathfrak{c}_i)(K_v)|^{-1} = 1.$$

The left-hand side counts the number of $G(K_v)$-orbits in $V_b(K_v)$ which have an integral representative, each orbit being weighted by $|Z_G(\kappa_b)(K_v)|^{-1}$. The total number of orbits equals $|J_b(K_v)/2J_b(K_v)| = |J_b(K_v)[2]|$, by Theorem 5.5. This quantity in turn is equal to $|Z_G(\kappa_b)(K_v)|$, by Theorem 5.2. This completes the proof. □

We now come to the first main theorem of this paper. If D is a divisor on X and $(E, P, Q) \in \mathcal{X}_D$, we write $A_{(E,P,Q)} \subset \mathrm{Sel}_2(E)$ for the trivial subgroup generated by the classes of P and Q, and $\mathrm{Sel}_2(E)^{\mathrm{nt}} = \mathrm{Sel}_2(E) - A_{(E,P,Q)}$ for its complement.

Theorem 5.9. *The limit*

$$\lim_{\deg D \to \infty} \sum_{(E,P,Q) \in \mathcal{X}_D} \frac{|\mathrm{Sel}_2(E)^{nt}| \cdot |\mathrm{Aut}(E,P,Q)|^{-1} \cdot |E(K)[2]|^{-1}}{|\mathcal{X}_D|}$$

exists and equals 8.

Proof. By Corollary 2.4, we have

$$\lim_{\deg D \to \infty} \frac{|\mathcal{X}_D|}{H^0(X, B_D)^{\mathrm{sf}}} = (q-1)^{-1}.$$

By Theorem 5.6, we have

$$(q-1) \sum_{(E,P,Q) \in \mathcal{X}_D} \frac{|\mathrm{Sel}_2(E)^{\mathrm{nt}}| \cdot |\mathrm{Aut}(E,P,Q)|^{-1} \cdot |E(K)[2]|^{-1}}{|H^0(X, B_D)^{\mathrm{sf}}|} = \int_{g \in \mathcal{Y}_G} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,\ nt}}|}{|H^0(X, B_D)^{\mathrm{sf}}|}\, d\nu_G$$

$$= \int_{\mathcal{Y}_G} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,\ nt}}|}{|H^0(X, B_D)|} \times \frac{|H^0(X, B_D)|}{|H^0(X, B_D)^{\mathrm{sf}}|}\, d\nu_G,$$

hence

$$\lim_{\deg D \to \infty} \sum_{(E,P,Q) \in \mathcal{X}_D} \frac{|\operatorname{Sel}_2(E)^{\mathrm{nt}}| \cdot |\operatorname{Aut}(E,P,Q)|^{-1} \cdot |E(K)[2]|^{-1}}{|\mathcal{X}_D|} = \delta_B^{-1} \times \lim_{\deg D \to \infty} \int_{\mathcal{Y}_G} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,\ nt}}|}{|H^0(X, B_D)|}\, d\nu_G.$$

We would like to compute the pointwise limit of the integrand and then interchange the order of the integral and the limit. This can be justified only after a process of 'cutting off the cusp'. Applying the decomposition of §4, we get

$$\int_{\mathcal{Y}_G} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,\ nt}}|}{|H^0(\mathcal{X}, B_D)|}\, d\nu_G = \sum_P \int_{\mathcal{Y}_{G,P}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,\ nt}}|}{|H^0(X, B_D)|}\, d\nu_G$$

$$= \sum_P \left[\int_{\mathcal{Y}_{G,P}(D)^{>2g_X-2}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,\ nt}}|}{|H^0(X, B_D)|}\, d\nu_G + \int_{\mathcal{Y}^{\mathrm{sp}}_{G,P}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,\ nt}}|}{|H^0(X, B_D)|}\, d\nu_G + \int_{\mathcal{Y}^{<0}_{G,P}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,\ nt}}|}{|H^0(X, B_D)|}\, d\nu_G \right],$$

where the sums are over the set of standard parabolic subgroups of G. (We recall that these are the parabolics containing the Borel subgroup $B \subset G$ corresponding to the set $R^- = \{-a_1, -a_2, -a_3, a_4\}$ of simple roots of G.) Applying Lemma 5.7, we see that when $\deg D > 0$, this equals

$$\sum_P \left[\int_{\mathcal{Y}_{G,P}(D)^{>2g_X-2}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X, B_D)|}\, d\nu_G + \int_{\mathcal{Y}^{\mathrm{sp}}_{G,P}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X, B_D)|}\, d\nu_G + \int_{\mathcal{Y}^{<0}_{G,P}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,\ nt}}|}{|H^0(X, B_D)|}\, d\nu_G \right].$$

We will see that the terms corresponding to $\mathcal{Y}_{G,P}(D)^{>2g_X-2}$ dominate, while the others vanish in the limit. Note that for any $g \in \mathcal{Y}_{G,P}$, we have $g \in \mathcal{Y}_{G,P}(D)^{>2g_X-2}$ for all divisors D of sufficiently large degree (depending on g). For divisors of degree greater than $2g_X - 2$ we have $|H^0(X, B_D)| = q^{4(1-g_X)+16\deg D}$, and an application of Corollary 4.5 shows that such D we have

$$\int_{\mathcal{Y}_{G,P}(D)^{>2g_X-2}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X, B_D)|}\, d\nu_G = \int_{\mathcal{Y}_{G,P}(D)^{>2g_X-2}} \frac{|H^0(X, \mathcal{V}_g(D))|}{|H^0(X, B_D)|} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X, \mathcal{V}_g(D))|}\, d\nu_G.$$

$$= q^{12(1-g_X)} \int_{\mathcal{Y}_{G,P}(D)^{>2g_X-2}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X, \mathcal{V}_g(D))|}\, d\nu_G.$$

The integrand in this expression is bounded by 1, and as $\deg D \to \infty$ its value tends to a limit δ_V which is independent of the choice of g, by Proposition 5.8. Applying the dominated convergence theorem, we find that

$$\lim_{\deg D \to \infty} \int_{\mathcal{Y}_P(D)^{>2g_X-2}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X, B_D)|}\, d\nu_G = q^{12(1-g_X)} \delta_V \int_{\mathcal{Y}_{G,P}} d\nu_G.$$

To take care of the contribution in special range, we calculate using Corollary 4.7 and Lemma 4.3:

$$\int_{\mathcal{Y}^{\mathrm{sp}}_{G,P}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X, B_D)|}\, d\nu_G \le \int_{\mathcal{Y}^{\mathrm{sp}}_{G,P}} \frac{|H^0(X, \mathcal{V}_g(D))|}{|H^0(X, B_D)|}\, d\nu_G = O\left(\sum_{\substack{\sigma \in \Lambda_P^{\mathrm{pos}} \\ \deg D + \langle \sigma, \alpha_0 \rangle \in [0, 2g_X-2]}} q^{-\langle \sigma, \delta_P \rangle} \right),$$

where the implied constant depends only on X. This tends to 0 as $\deg D \to \infty$. To take care of the remaining contributions, we note that Corollary 4.8 implies that

$$\int_{\mathcal{Y}^{<0}_{G,P}} \frac{|H^0(X, \mathcal{V}_g(D))^{\mathrm{sf,\ nt}}|}{|H^0(X, B_D)|}\, d\nu_G = 0$$

unless $P = B$ or the Levi quotient of P has semisimple rank 1. In these cases we will show that

$$\lim_{\deg D \to \infty} \int_{\mathcal{Y}_{G,P}^{<0}} \frac{|H^0(X, \mathcal{V}_g(D))^{\text{sf, nt}}|}{|H^0(X, B_D)|}\, d\nu_G = 0. \tag{5.15}$$

Let us first treat the (harder) case of $P = B$. Let $\mathcal{C}$ denote the set of non-empty subsets $M \subset \Phi_V$ which are closed under the relation $\geq$: i.e. if $a \in \Phi_V$, $b \in M$, and $a \geq b$, then $a \in M$. Note that $\alpha_0 \in M$ for all $M \in \mathcal{C}$. Then we have $\mathcal{Y}_{G,B}(D)^{<0} = \sqcup_{M \in \mathcal{C}} \mathcal{Y}_{G,B}(D)^{<0,M}$, where we define $\mathcal{Y}_{G,B}(D)^{<0,M}$ to be the set of G-torsors $F \in \mathcal{Y}_{G,B}(D)^{<0}$ such that for $a \in \Phi_V$, the slope σ_{F_B} of the canonical reduction F_B satisfies $\langle \sigma_{F_B}, a \rangle + D < 0$ if and only if $a \in M$. This allows us to decompose

$$\int_{\mathcal{Y}_{G,P}^{<0}} \frac{|H^0(X, \mathcal{V}_g(D))^{\text{sf, nt}}|}{|H^0(X, B_D)|}\, d\nu_G = \sum_{M \in \mathcal{C}} \int_{\mathcal{Y}_{G,P}^{<0,M}} \frac{|H^0(X, \mathcal{V}_g(D))^{\text{sf, nt}}|}{|H^0(X, B_D)|}\, d\nu_G. \tag{5.16}$$

Let $\mathcal{C}_0 \subset \mathcal{C}$ denote the set of subsets $M \in \mathcal{C}_0$ not containing any of the sets S appearing in the statement of Corollary 3.6; then the summand in (5.16) corresponding to $M \in \mathcal{C}$ can be non-zero only if $M \in \mathcal{C}_0$. To show (5.15) in case $P = B$, it is therefore enough to show that the equality

$$\lim_{\deg D \to \infty} \int_{\mathcal{Y}_{G,B}^{<0,M}} \frac{|H^0(X, \mathcal{V}_g(D))|}{|H^0(X, B_D)|}\, d\nu_G = 0. \tag{5.17}$$

holds for each $M \in \mathcal{C}_0$. If $M \in \mathcal{C}$ and $\mathcal{Y}_{G,B}^{<0,M}$, then Corollary 4.7 implies that we have

$$\frac{|H^0(X, \mathcal{V}_g(D))|}{|H^0(X, B_D)|} = O(q^{-|M| \deg D - \langle \sigma, \sum_{a \in M} a \rangle}),$$

where the implied constant depends only on X. Combining this with Lemma 4.3, we get for any $M \in \mathcal{C}$:

$$\int_{\mathcal{Y}_{G,B}^{<0,M}} \frac{|H^0(X, \mathcal{V}_g(D))|}{|H^0(X, B_D)|}\, d\nu_G = O\left(\sum_{\substack{\sigma \in \Lambda_B^{\text{pos}} \\ \forall a \in M, \langle \sigma, a \rangle + \deg D < 0 \\ \forall a \in \Phi_V - M, \langle \sigma, a \rangle + \deg D \geq 0}} q^{-|M| \deg D - \langle \sigma, \delta_B + \sum_{a \in M} a \rangle} \right), \tag{5.18}$$

where the implied constant again depends only on X. If $a \in \lambda(M)$ then $q^{\langle \sigma, a \rangle + \deg D} \geq 1$. It follows that for any function $p : \lambda(M) \to \mathbb{R}_{\geq 0}$, (5.18) is bounded above by a constant multiple of

$$\sum_{\substack{\sigma \in \Lambda_B^{\text{pos}} \\ \forall a \in M, \langle \sigma, a \rangle + \deg D < 0 \\ \forall a \in \Phi_V - M, \langle \sigma, a \rangle + \deg D \geq 0}} q^{\deg D (\sum_{a \in \lambda(M)} p(a) - |M|) + \langle \sigma, \sum_{a \in \lambda(M)} p(a) a - \sum_{a \in M} a - \delta_B \rangle}$$

$$\leq q^{\deg D (\sum_{a \in \lambda(M)} p(a) - |M|)} \sum_{\sigma \in \Lambda_B^{\text{pos}}} q^{\langle \sigma, \sum_{a \in \lambda(M)} p(a) a - \sum_{a \in M} a - \delta_B \rangle}.$$

This last expression tends to 0 as $\deg D$ tends to infinity provided the function p is chosen so that the following conditions are satisfied:

- $|M| > \sum_{a \in \lambda(M)} p(a)$.
- Define $w(M) = -\sum_{a \in M} a - \delta_B$ and $w(M, p) = \sum_{a \in \lambda(M)} p(a) a - \sum_{a \in M} a - \delta_B \in X^*(T)_{\mathbb{R}}$. Then $n_i(w(M, p)) > 0$ for each $i = 1, \ldots, 4$.

We show that we can find such a function p simply by exhibiting one for each possible choice of $M \in \mathcal{C}_0$ in the following table (the weights being labelled as in §3.1):

M	$\lambda(M)$	$\lvert M\rvert$	$2w(M)$				p	$2w(M,p)$			
1	2, 3, 4, 5	1	1	1	1	1	$(0,0,0,0)$	1	1	1	1
1,2	3,4,5	2	2	0	0	0	$(0.5,0.5,0.5)$	3.5	0.5	0.5	0.5
1,3	2,4,5	2	0	2	0	0	$(0.5,0.5,0.5)$	0.5	3.5	0.5	0.5
1,4	2,3,5	2	0	0	2	0	$(0.5,0.5,0.5)$	0.5	0.5	3.5	0.5
1,5	2,3,4	2	0	0	0	2	$(0.5,0.5,0.5)$	0.5	0.5	0.5	3.5
1,2,3	4,5,6	3	1	1	-1	-1	$(0.5,0.5,1.5)$	0.5	0.5	0.5	0.5
1,2,4	3,5,7	3	1	-1	1	-1	$(0.5,0.5,1.5)$	0.5	0.5	0.5	0.5
1,2,5	3,4,8	3	1	-1	-1	1	$(0.5,0.5,1.5)$	0.5	0.5	0.5	0.5
1,3,4	2,5,9	3	-1	1	1	-1	$(0.5,0.5,1.5)$	0.5	0.5	0.5	0.5
1,3,5	2,4,10	3	-1	1	-1	1	$(0.5,0.5,1.5)$	0.5	0.5	0.5	0.5
1,4,5	2,3,11	3	-1	-1	1	1	$(0.5,0.5,1.5)$	0.5	0.5	0.5	0.5

This shows that the equality (5.15 holds in case $P = B$. We now treat the four remaining cases. By symmetry, we can assume that P is the standard parabolic subgroup of G generated by B and the root subgroup corresponding to the root a_1. Then the Levi quotient L_P of P is isogenous to SL_2, and the same argument as above shows that we need to show that

$$\lim_{\deg D\to\infty} \int_{\mathcal{Y}_{G,P}^{<0,M}} \frac{|H^0(X,\mathcal{V}_g(D))^{\text{sf, nt}}|}{|H^0(X,B_D)|}\, d\nu_G = 0 \tag{5.19}$$

for each $M \in \mathcal{C}_0$. We observe that $\mathcal{Y}_{G,P}^{<0,M}$ is non-empty only when M satisfies the condition $a \in M \Rightarrow a' \in M$, where $a' \in \Phi_V$ is defined by $n_1(a') = -n_1(a)$, $n_i(a') = n_i(a)$ for $i = 2,3,4$. The only set $M \in \mathcal{C}_0$ which satisfies this condition is $M = \{1,2\}$, so we are reduced finally to showing that the equality (5.19) holds in the single case $M = \{1,2\}$. This can be proved using exactly the same trick as before.

Putting everything back together and applying Proposition 5.8, we find

$$\lim_{\deg D\to\infty} \sum_{(E,P,Q)\in\mathcal{X}_D} \frac{|\operatorname{Sel}_2(E)^{\text{nt}}|\cdot|\operatorname{Aut}(E,P,Q)|^{-1}\cdot|E(K)[2]|^{-1}}{|\mathcal{X}_D|} = \delta_B^{-1}\times\sum_P q^{12(1-g_X)}\delta_V\int_{\mathcal{Y}_{G,P}} d\nu_G$$

$$= \int_{G(\widehat{\mathcal{O}}_K)} d\tau_G \int_{G(K)\backslash G(\mathbb{A}_K)} d\mu_G = \int_{G(K)\backslash G(\mathbb{A}_K)} d\tau_G = \tau(G),$$

the Tamagawa number of G. Since the fundamental group of G is isomorphic to μ_2^3, we have $\tau(G) = 8$. This completes the proof. □

Corollary 5.10. *The limit*

$$\lim_{\deg D\to\infty} \sum_{(E,P,Q)\in\mathcal{X}_D} \frac{|\operatorname{Sel}_2(E)|\cdot|\operatorname{Aut}(E,P,Q)|^{-1}\cdot|E(K)[2]|^{-1}}{|\mathcal{X}_D|}$$

exists and equals 12.

Proof. In view of Theorem 5.9, we just need to show that

$$\lim_{\deg D\to\infty} \sum_{(E,P,Q)\in\mathcal{X}_D} \frac{|A_{E,P,Q}|\cdot|\operatorname{Aut}(E,P,Q)|^{-1}\cdot|E(K)[2]|^{-1}}{|\mathcal{X}_D|}$$

exists and equals 4. Following the discussion after Theorem 5.3, we see that it is enough to show that the limit

$$\lim_{\deg D\to\infty} \frac{|\{b\in H^0(X,B_D)\cap B^{\text{rs}}(K) \mid \operatorname{im}(\Gamma_K \to W(G,\mathfrak{z}_{\mathfrak{h}}(\kappa_b))) \neq W(G,\mathfrak{z}_{\mathfrak{h}}(\kappa_b))\}|}{|H^0(X,B_D)|}$$

exists and equals 0. This is a consequence of the Hilbert irreducibility theorem. □

Finally, we prove the promised generalization of Theorem 5.9.

Theorem 5.11. *Let $f : \mathcal{Y}_G \to \mathbb{R}$ be a bounded function. Then we have*

$$\lim_{\deg D\to\infty} \sum_{(E,P,Q)\in\mathcal{X}_D} \frac{|\operatorname{Aut}(E,P,Q)|^{-1}\cdot|E(K)[2]|^{-1}\sum_{x\in\mathrm{Sel}_2(E)^{nt}} f(\operatorname{inv} x)}{|\mathcal{X}_D|} = \int_{F\in\mathcal{Y}_G} f(F)\,d\tau_G.$$

Proof. Arguing as in the proof of Theorem 5.9, we get

$$(q-1)\sum_{(E,P,Q)\in\mathcal{X}_D} \frac{|\operatorname{Aut}(E,P,Q)|^{-1}\cdot|E(K)[2]|^{-1}\sum_{x\in\mathrm{Sel}_2(E)^{\mathrm{nt}}} f(\operatorname{inv} x)}{|H^0(X,B_D)^{\mathrm{sf}}|} = \int_{g\in\mathcal{Y}_G} \frac{|H^0(X,\mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X,B_D)^{\mathrm{sf}}|} f(F_g)\,d\nu_G$$

$$= \sum_P \left[\int_{\mathcal{Y}_{G,P}(D)^{>2g_X-2}} f(F_g)\frac{|H^0(X,\mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X,B_D)|}\,d\nu_G \right.$$

$$\left. + \int_{\mathcal{Y}^{\mathrm{sp}}_{G,P}} f(F_g)\frac{|H^0(X,\mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X,B_D)|}\,d\nu_G + \int_{\mathcal{Y}^{<0}_{G,P}} f(F_g)\frac{|H^0(X,\mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(X,B_D)|}\,d\nu_G \right].$$

Since f is bounded, the same arguments as before show that the boundary terms vanish in the limit. On the other hand, the boundedness of f means we can again apply the dominated convergence theorem to deduce that

$$\lim_{\deg D\to\infty} \int_{\mathcal{Y}_P(D)^{>2g_X-2}} f(F_g)\frac{|H^0(X,\mathcal{V}_g(D))^{\mathrm{sf}}|}{|H^0(\mathcal{X},B_D)|}\,d\nu_G = q^{12(1-g_X)}\delta_V \int_{\mathcal{Y}_{G,P}} f(F_g)\,d\nu_G,$$

and these terms can then be regrouped to obtain the statement of the theorem. □

References

[BH04] Indranil Biswas and Yogish I. Holla. Harder-Narasimhan reduction of a principal bundle. *Nagoya Math. J.*, 174:201–223, 2004.

[BPGN97] L. Brambila-Paz, I. Grzegorczyk, and P. E. Newstead. Geography of Brill-Noether loci for small slopes. *J. Algebraic Geom.*, 6(4):645–669, 1997.

[BS15] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math. (2)*, 181(1):191–242, 2015.

[dJ02] A. J. de Jong. Counting elliptic surfaces over finite fields. *Mosc. Math. J.*, 2(2):281–311, 2002. Dedicated to Yuri I. Manin on the occasion of his 65th birthday.

[Gil02] P. Gille. Torseurs sur la droite affine. *Transform. Groups*, 7(3):231–245, 2002.

[HLHN14] Q. P. Hồ, 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.

[Hum95] James E. Humphreys. *Conjugacy classes in semisimple algebraic groups*, volume 43 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1995.

[IMP03] S. Ilangovan, V. B. Mehta, and A. J. Parameswaran. Semistability and semisimplicity in representations of low height in positive characteristic. In *A tribute to C. S. Seshadri (Chennai, 2002)*, Trends Math., pages 271–282. Birkhäuser, Basel, 2003.

[KR71] B. Kostant and S. Rallis. Orbits and representations associated with symmetric spaces. *Amer. J. Math.*, 93:753–809, 1971.

[Lev07] Paul Levy. Involutions of reductive Lie algebras in positive characteristic. *Adv. Math.*, 210(2):505–559, 2007.

[Poo03] Bjorn Poonen. Squarefree values of multivariable polynomials. *Duke Math. J.*, 118(2):353–373, 2003.

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

[RR84] S. Ramanan and A. Ramanathan. Some remarks on the instability flag. *Tohoku Math. J. (2)*, 36(2):269–291, 1984.

[Sch15] Simon Schieder. The Harder-Narasimhan stratification of the moduli stack of G-bundles via Drinfeld's compactifications. *Selecta Math. (N.S.)*, 21(3):763–831, 2015.

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

[SS70] T. A. Springer and R. Steinberg. Conjugacy classes. In *Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69)*, Lecture Notes in Mathematics, Vol. 131, pages 167–266. Springer, Berlin, 1970.

[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.

[Wei95] André Weil. Adèles et groupes algébriques. In *Séminaire Bourbaki, Vol. 5*, pages Exp. No. 186, 249–257. Soc. Math. France, Paris, 1995.