TORSION BOUNDS FOR A FIXED ABELIAN VARIETY AND VARYING NUMBER FIELD

SAMUEL LE FOURN, DAVIDE LOMBARDO, AND DAVID ZYWINA

ABSTRACT. Let A be an abelian variety defined over a number field K. For a finite extension L/K, the cardinality of the group $A(L)_{\text{tors}}$ of torsion points in $A(L)$ can be bounded in terms of the degree $[L : K]$. We study the smallest real number β_A such that for any finite extension L/K and $\varepsilon > 0$, we have $|A(L)_{\text{tors}}| \le C \cdot [L : K]^{\beta_A + \varepsilon}$, where the constant C depends only on A and ε (and not L). Assuming the Mumford–Tate conjecture for A, we will show that β_A agrees with the conjectured value of Hindry and Ratazzi. We also give a similar bound for the maximal order of a torsion point in $A(L)$.

1. INTRODUCTION

Let A be a nonzero abelian variety defined over a number field K. For every finite extension L of K, the group $A(L)_{\text{tors}}$ of torsion points in $A(L)$ is finite. We are interested in finding upper bounds for the cardinality of $A(L)_{\text{tors}}$ that depend only on A and the degree $[L : K]$. A theorem of Masser [Mas] implies that for any real number $\beta > \dim A$ and any finite extension L/K, we have $|A(L)_{\text{tors}}| \le C \cdot [L : K]^\beta$, where C is a constant depending only on A and β. We will see that Masser's bound remains true if $\dim A$ is replaced by some smaller value whenever A is not isogenous over $\overline{K}$ to a power of a CM elliptic curve, cf. §8.

Let β_A be the infimum of the set of real numbers β for which the inequality

$$|A(L)_{\text{tors}}| \le C \cdot [L : K]^\beta$$

holds for all finite extensions L/K, where C is a constant that depends only on A and β (and in particular not L). From Masser, we have $\beta_A \le \dim A$. This is made totally explicit in a recent preprint of Gaudron and Rémond [GR22]: namely, they prove that

$$|A(L)_{\text{tors}}| \le (6g)^{8g} D^g \max(1, h_{\mathcal{F}}(A), \log D)^g,$$

where $g = \dim A$, $D = [L : \mathbb{Q}]$ and $h_{\mathcal{F}}(A)$ is the stable Faltings height of A.

Hindry and Ratazzi have made a precise conjecture for the value of β_A which we now recall. Fix an embedding $K \subseteq \mathbb{C}$. The abelian variety $A_{\mathbb{C}}$, obtained by base extending A to $\mathbb{C}$, is isogenous to a product $\prod_{i=1}^n A_i^{m_i}$, where the A_i are abelian varieties over $\mathbb{C}$ that are simple and pairwise nonisogenous. For each subset $I \subseteq \{1, \dots, n\}$, define the abelian variety $A_I := \prod_{i \in I} A_i^{m_i}$ over $\mathbb{C}$. Associated to each abelian variety B defined over K or $\mathbb{C}$ is a *Mumford–Tate group* G_B whose definition we recall in §2.1; it is a linear algebraic group defined over $\mathbb{Q}$. Define the real number

$$\gamma_A := \max_{\emptyset \ne I \subseteq \{1, \dots, n\}} \frac{2 \dim A_I}{\dim G_{A_I}}.$$

Hindry and Ratazzi have conjectured that $\beta_A = \gamma_A$, cf. [HR12, Conjecture 1.1]; note that A_I and $\prod_{i \in I} A_i$ have isomorphic Mumford–Tate groups. They proved the inequality $\beta_A \ge \gamma_A$ [HR10, Proposition 1.5].

Hindry and Ratazzi have proved their conjecture in various situations where the Mumford–Tate conjecture is known and the Mumford-Tate group G_A is of a very special form [Rat07, HR10, HR12,

HR16]. For example, if G_A is isomorphic to GSp_{2g} (with $g = \dim A$) and the Mumford–Tate conjecture holds for A, then β_A equals $\gamma_A = 2g/(2g^2 + g + 1)$, cf. [HR12]. Cantoral Farfán has proved several additional cases, see [CF19]. A statement of the Mumford–Tate conjecture can be found in §2.3.

The following is our main result; we prove the conjecture of Hindry and Ratazzi assuming the Mumford–Tate conjecture.

Theorem 1.1. *Let A be a nonzero abelian variety defined over a number field K for which the Mumford–Tate conjecture holds. Then $\beta_A = \gamma_A$. Equivalently, γ_A is the smallest real value such that for any finite extension L/K and real number $\varepsilon > 0$, we have*

$$|A(L)_{\mathrm{tors}}| \leq C \cdot [L : K]^{\gamma_A + \varepsilon},$$

where C is a constant that depends only on A and ε.

This result is in fact implied by an unconditional one, namely Theorem 6.2, relating β_A to invariants associated to all the ℓ-adic monodromy groups of A.

Remark 1.2. In addition to recovering all previous results on the Hindry–Ratazzi conjecture, Theorem 1.1 proves many new cases of it: for example, the Mumford-Tate conjecture is known to hold for all geometrically simple abelian varieties of prime dimension [Rib83], while the Hindry–Ratazzi conjecture had not been previously proven for such varieties.

In the case where A is geometrically simple, the following shows that the converse of Theorem 1.1 holds. So the Mumford–Tate conjecture assumption in Theorem 1.1 is reasonable and the value β_A is an interesting arithmetic invariant of A.

Theorem 1.3. *Let A be a geometrically simple abelian variety defined over a number field K. Then the Mumford–Tate conjecture for A holds if and only if $\beta_A = \gamma_A$.*

We also show that the Hindry-Ratazzi conjecture (for all abelian varieties) is in fact equivalent to the Mumford–Tate conjecture (for all abelian varieties).

Theorem 1.4. *The following are equivalent:*

    (a) *the Mumford–Tate conjecture holds for all abelian varieties A defined over a number field,*
    (b) $\beta_A = \gamma_A$ *for all nonzero abelian varieties A defined over a number field,*
    (c) $\beta_A = \gamma_A$ *for all geometrically simple abelian varieties A defined over a number field.*

Remark 1.5. Take any $\varepsilon > 0$ and any torsion point $P \in A(\overline{K})$ whose order we denote by n. A direct consequence of Theorem 1.1 is that, assuming the Mumford–Tate conjecture for A, we have

$$[K(P) : K] \geq C \cdot n^{1/\gamma_A - \varepsilon},$$

where C is a positive constant depending only on A and ε. Here, the constant $1/\gamma_A$ is often not best possible. The next theorem describes an optimal version assuming the Mumford–Tate conjecture for A; an unconditional version can be found in §9.

With a fixed embedding $K \subseteq \mathbb{C}$, the Mumford–Tate group G_A of A comes with a faithful action on the $\mathbb{Q}$-vector space $V_A := H_1(A(\mathbb{C}), \mathbb{Q})$, cf. §2.1.

Theorem 1.6. *Let A be a nonzero abelian variety defined over a number field K for which the Mumford–Tate conjecture holds. Let d be the minimal dimension of the orbits of the action of $G_A(\mathbb{C})$ on the nonzero vectors in $V_A \otimes_{\mathbb{Q}} \mathbb{C}$. Take any real number $\varepsilon > 0$. Then for any integer $n \geq 1$ and any point $P \in A(\overline{K})$ of order n, we have*

$$[K(P) : K] \geq C \cdot n^{d - \varepsilon},$$

where C is a positive constant depending only on A and ε. Moreover, d is the minimal real number that has this property.

Remark 1.7. It is easy to construct examples for which the minimal dimension $d_{\mathbb{Q}}$ of the orbits of the action of G_A on the nonzero vectors in V_A is strictly greater than the quantity d appearing in the previous theorem. The simplest such case arises when A is an elliptic curve with complex multiplication: G_A is then a nonsplit torus of dimension 2, and one sees easily that $d_{\mathbb{Q}} = 2$ while $d = 1$.

1.1. **Notation.**

- ℓ will always denote a rational prime.
- For a scheme X over a commutative ring R and a (commutative) R-algebra S, we will denote by X_S the S-scheme $X \times_{\operatorname{Spec} R} \operatorname{Spec} S$.
- Fix a commutative ring R and a free R-module M of finite rank. We define GL_M to be the group scheme over R such that for each (commutative) R-algebra B, we have $\operatorname{GL}_M(B) = \operatorname{Aut}_B(B \otimes_R M)$ with the obvious functoriality. A choice of basis of the R-module M induces an isomorphism $\operatorname{GL}_M \cong \operatorname{GL}_{d,R}$, where d is the rank of M.
- Let G be an algebraic subgroup of GL_V, where V is a nonzero vector space over a field k. For a subspace W of V, we let G_W be the algebraic subgroup of G that fixes W; more precisely, we have $G_W(B) = \{g \in G(B) : gw = w \text{ for all } w \in B \otimes_k W\}$ for all k-algebras B.
- Let R be a commutative ring, $\mathcal{G}$ be a group subscheme of $\operatorname{GL}_{n,R}$, and $\mathcal{W}$ be a submodule of R^n such that $R^n/\mathcal{W}$ is locally free of rank $n - d$. We define a group subscheme $\operatorname{Fix}_{\mathcal{G}}(\mathcal{W})$ of $\mathcal{G}$ by the functorial property

$$\operatorname{Fix}_{\mathcal{G}}(\mathcal{W})(S) = \{\varphi \in \mathcal{G}(S) \,|\, \varphi_{|\mathcal{W} \otimes_R S} \text{ is the identity on } \mathcal{W} \otimes_R S\}$$

  for every R-algebra S. When $R = k$ is a field and $\mathcal{W} = W$ is a vector subspace of k^n we have $\operatorname{Fix}_{\mathcal{G}}(\mathcal{W}) = \mathcal{G}_W$.
- We define the Mumford–Tate group G_A of an abelian variety A in §2.1.
- We denote by $T_\ell(A)$ the ℓ-adic Tate module of A and set $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. The precise definitions of these objects are recalled in §2.2. We define the ℓ-adic monodromy groups $G_{A,\ell} \subseteq \operatorname{GL}_{V_\ell(A)}$ over $\mathbb{Q}_\ell$ and $\mathcal{G}_{A,\ell} \subseteq \operatorname{GL}_{T_\ell(A)}$ over $\mathbb{Z}_\ell$ in §2.2.
- For a field k, a finite-dimensional k-vector space V and a linear algebraic subgroup G of GL_V, define the slope

$$\gamma_G := \max_{0 \neq W \subseteq V} \frac{\dim W}{\dim G - \dim G_W},$$

  where we vary over the nonzero subspaces W of V. We interpret this as $\gamma_G = +\infty$, when for some nonzero subspace W, the stabilizer G_W has finite index in G. If γ_G is finite, we say that G has finite slope. Note that if γ_G is finite, then $\gamma_G \leq \dim V$.
- For two positive real numbers a and b, by $a \ll b$ (or $b \gg a$), we mean that $a \leq Cb$ for a positive constant C; the dependencies of the constant C will always be indicated by subscripts. For example, Masser's result mentioned above says that for any finite extension L/K and number $\beta > \dim A$, we have $|A(L)_{\text{tors}}| \ll_{A,\beta} [L : K]^\beta$. We will write $a \asymp b$ to denote that $a \ll b$ and $a \gg b$ both hold, where the dependencies in the implicit constants will be indicated by subscripts.

1.2. **Overview.** In §2, we give some background on the ℓ-adic representations associated to an abelian variety, review some of their uniformity properties, and recall the Mumford–Tate conjecture.

The group $G := (G_A)_{\mathbb{C}}$ acts on the complex vector space $V_{\mathbb{C}} := H_1(A(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$. For each subspace W of $V_{\mathbb{C}}$, we have an algebraic subgroup G_W of G as defined in §1.1. In §3, we prove that the inequality

$$(1.1) \qquad\qquad \gamma_A \cdot (\dim G - \dim G_W) \geq \dim W$$

always holds and that γ_A is the smallest real number with this property.

Let ℓ be any prime. In §4 and §5, we prove a version of Theorem 1.1 for the subgroup $A(L)[\ell^\infty]$ consisting of the points of $A(L)$ whose order is a power of ℓ. More precisely, we prove that if the Mumford–Tate conjecture for A holds, then for any finite extension L/K, we have $|A(L)[\ell^\infty]| \ll_{A,\ell} [L : K]^{\gamma_A}$ (this follows from Theorem 5.1 and Lemma 3.9(ii)). Theorem 4.1, proved in §4, further shows that the implicit constant can be taken to be independent of ℓ.

In §6, we obtain upper and lower bounds for β_A, which agree under the assumption of the Mumford–Tate conjecture. This establishes our main theorems. In §7, we make some remarks on a conjectural expression for β_A not involving Mumford–Tate groups. In §8 we show that $\beta_A \leq \dim A$, with equality only for powers of CM elliptic curves. This shows that our results improve on Masser's bound except for those cases. Finally, in §9, we prove Theorem 1.6 and also give an unconditional version.

2. ABELIAN VARIETIES BACKGROUND

In this section, except for §2.1, we fix an abelian variety A of dimension $g \geq 1$ defined over a number field K. We review some of the theory of the ℓ-adic representations associated to A and the Mumford–Tate conjecture.

2.1. **Mumford–Tate groups.**
Let A be a nonzero abelian variety defined over $\mathbb{C}$. We now recall the definition of the Mumford–Tate group G_A of A. If instead A is defined over a number field K, then with a fixed embedding $K \subseteq \mathbb{C}$, we define G_A to be the Mumford–Tate group of $A_\mathbb{C}$. The choice of embedding K into $\mathbb{C}$ does not affect any of the following constructions by [DMOS82, Theorem 2.11].

We view $A(\mathbb{C})$ as a topological space with its usual complex topology. The first homology group $V := H_1(A(\mathbb{C}), \mathbb{Q})$ is a vector space of dimension $2 \dim A$ over $\mathbb{Q}$. It is endowed with a $\mathbb{Q}$-Hodge structure of type $\{(-1, 0), (0, -1)\}$ from the Hodge decomposition, so

$$V \otimes_\mathbb{Q} \mathbb{C} = H_1(A(\mathbb{C}), \mathbb{C}) = V^{-1,0} \oplus V^{0,-1}$$

with $V^{0,-1} = \overline{V^{-1,0}}$. Let $\mu \colon \mathbb{G}_{m,\mathbb{C}} \to \mathrm{GL}_{V \otimes_\mathbb{Q}\mathbb{C}}$ be the cocharacter such that $\mu(z)$ is the automorphism of $V \otimes_\mathbb{Q} \mathbb{C}$ which is multiplication by z on $V^{-1,0}$ and the identity on $V^{0,-1}$ for each $z \in \mathbb{C}^\times = \mathbb{G}_m(\mathbb{C})$. The Mumford–Tate group of A is the smallest algebraic subgroup G_A of GL_V, defined over $\mathbb{Q}$, which contains $\mu(\mathbb{G}_{m,\mathbb{C}})$.

The ring of endomorphisms $\mathrm{End}(A)$ of the abelian variety $A/\mathbb{C}$ acts on V, which induces an injective homomorphism $\mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q} \hookrightarrow \mathrm{End}_\mathbb{Q}(V)$. Denote by $\mathrm{End}_\mathbb{Q}(V)^{G_A}$ the subring of $\mathrm{End}_\mathbb{Q}(V)$ consisting of those elements that commute with G_A.

Lemma 2.1.

  (i) *The group G_A is connected and reductive.*
  (ii) *The image of $\mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q} \hookrightarrow \mathrm{End}_\mathbb{Q}(V)$ is $\mathrm{End}_\mathbb{Q}(V)^{G_A}$.*

Proof. This follows from Propositions 17.3.4 and 17.3.6 of [BL04]; note that the Mumford–Tate group G_A is generated by the *Hodge group* $\mathrm{Hg}(A)$ and the group $\mathbb{G}_m$ of homotheties. $\square$

The abelian variety A is isogenous to a product $\prod_{i=1}^{n} A_i^{m_i}$, where the A_i are simple abelian varieties over $\mathbb{C}$ that are pairwise nonisogenous and the m_i are positive integers. A fixed isogeny induces an isomorphism

$$(2.1) \qquad\qquad V = \bigoplus_{i=1}^{n} V_i$$

of $\mathbb{Q}$-vector spaces, where each $V_i := H_1(A_i^{m_i}(\mathbb{C}), \mathbb{Q})$ is a representation of G_A.

For each subset $I \subseteq \{1, \dots, n\}$, define the subspace $V_I := \bigoplus_{i \in I} V_i$ of V and the abelian variety $A_I := \prod_{i \in I} A_i^{m_i}$. We can identify $H_1(A_I(\mathbb{C}), \mathbb{Q})$ with V_I. The group G_A acts on V_I since it acts on each V_i. The representation $G_A \to \mathrm{GL}_{V_I}$ gives a dominant homomorphism $G_A \to G_{A_I}$ of linear algebraic groups. The kernel of $G_A \to G_{A_I}$ is $(G_A)_{V_I}$ and hence

$$(2.2) \qquad\qquad \dim G_{A_I} = \dim G_A - \dim(G_A)_{V_I}.$$

Lemma 2.2. *The direct sum (2.1) is the decomposition of the representation V of G_A into isotypical components.*

Proof. Take any $i \in \{1, \dots, n\}$ and set $I := \{i\}$. The subspace $V_I = V_i$ of V is a representation of G_A via the homomorphism $G_A \to G_{A_I}$. We thus have

$$\prod_{i=1}^{n} \mathrm{End}(A_i^{m_i}) \otimes_{\mathbb{Z}} \mathbb{Q} = \prod_{i=1}^{n} \mathrm{End}_{\mathbb{Q}}(V_i)^{G_A} \subseteq \mathrm{End}_{\mathbb{Q}}(V)^{G_A} = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} = \prod_{i=1}^{n} \mathrm{End}(A_i^{m_i}) \otimes_{\mathbb{Z}} \mathbb{Q},$$

where the first two equalities follow from Lemma 2.1(ii) and the last equality uses that the simple abelian varieties A_i are pairwise nonisogenous. Therefore, we have $\mathrm{End}_{\mathbb{Q}}(V)^{G_A} = \prod_{i=1}^{n} \mathrm{End}_{\mathbb{Q}}(V_i)^{G_A}$ and each $\mathrm{End}_{\mathbb{Q}}(V_i)^{G_A}$ is isomorphic to $M_{e_i}(D_i)$ for some integer $e_i \geq 1$ and division algebra D_i (the ring $\mathrm{End}(A_i^{m_i}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is of this form since A_i is simple). The lemma is now a consequence of V being a semisimple representation of G_A; this is true since G_A is reductive by Lemma 2.1(i). $\qquad\square$

2.2. **ℓ-adic monodromy groups.** Take any prime ℓ. For each integer $i \geq 1$, let $A[\ell^i]$ be the ℓ^i-torsion subgroup of $A(\overline{K})$, where $\overline{K}$ is a fixed algebraic closure of K. The group $A[\ell^i]$ is a free $\mathbb{Z}/\ell^i\mathbb{Z}$-module of rank $2g$. The ℓ-adic Tate module is

$$T_\ell(A) := \varprojlim_{i} A[\ell^i],$$

where the inverse limit is with respect to the multiplication by ℓ maps $A[\ell^{i+1}] \to A[\ell^i]$. The Tate module $T_\ell(A)$ is a free $\mathbb{Z}_\ell$-module of rank $2g$. Define $V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$; it is a $\mathbb{Q}_\ell$-vector space of dimension $2g$. We can identify $\mathrm{GL}_{V_\ell(A)}$ with the generic fiber of $\mathrm{GL}_{T_\ell(A)}$.

The Galois group $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$ acts on each $A[\ell^i]$ and respects the group structure. This induces an action of Gal_K on $T_\ell(A)$ and $V_\ell(A)$. The action of Gal_K on $V_\ell(A)$ respects the vector space structure and can thus be expressed in terms of a representation

$$\rho_{A,\ell^\infty} \colon \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) = \mathrm{GL}_{T_\ell(A)}(\mathbb{Z}_\ell) \subseteq \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) = \mathrm{GL}_{V_\ell(A)}(\mathbb{Q}_\ell).$$

The ℓ-adic monodromy group of A, which we denote by $G_{A,\ell}$, is the algebraic subgroup of $\mathrm{GL}_{V_\ell(A)}$ obtained by taking the Zariski closure of $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$. The group $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ is open in $G_{A,\ell}(\mathbb{Q}_\ell)$, cf. [Bog80]. Therefore, $G_{A,\ell}$ determines the group $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ up to commensurability.

We define $\mathcal{G}_{A,\ell}$ to be the group subscheme of $\mathrm{GL}_{T_\ell(A)}$ obtained by taking the Zariski closure of $\rho_{A,\ell^\infty}(\mathrm{Gal}_K) \subseteq \mathrm{GL}_{T_\ell(A)}(\mathbb{Z}_\ell)$. We can also describe $\mathcal{G}_{A,\ell}$ as the Zariski closure of $G_{A,\ell}$ in $\mathrm{GL}_{T_\ell(A)}$. The monodromy group $G_{A,\ell}$ is the generic fiber of the $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell}$.

Denote by $G_{A,\ell}^\circ$ the neutral component of $G_{A,\ell}$, i.e., the connected component of $G_{A,\ell}$ containing the identity element; it is an algebraic subgroup of $G_{A,\ell}$. Denote by $K_{A,\ell}$ the finite extension of K

such that the kernel of the homomorphism

$$\mathrm{Gal}_K \xrightarrow{\rho_{A,\ell^\infty}} G_{A,\ell}(\mathbb{Q}_\ell) \to G_{A,\ell}(\mathbb{Q}_\ell)/G_{A,\ell}^\circ(\mathbb{Q}_\ell)$$

is $\mathrm{Gal}(\overline{K}/K_{A,\ell})$, where the second homomorphism is the obvious quotient map. The following proposition was proved by Serre [Ser00, 133]; see also [LP97].

Proposition 2.3. *The extension $K_{A,\ell}/K$ is independent of ℓ. In particular, there is a finite extension K'/K such that $G_{A_{K'},\ell}$ is connected for all ℓ.*

We will make extensive use of the following fundamental results of Faltings.

Proposition 2.4 (Faltings).
  (i) *The representation $V_\ell(A)$ of Gal_K is semisimple.*
  (ii) *The map $\mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q}_\ell \to \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A))$ is an isomorphism of $\mathbb{Q}_\ell$-algebras.*
  (iii) *For any abelian variety B over K, the map $\mathrm{Hom}(A,B) \otimes_\mathbb{Z} \mathbb{Q}_\ell \to \mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A), V_\ell(B))$ is an isomorphism of $\mathbb{Q}_\ell$-vector spaces.*

Proof. These are proven in §5 of [Fal86]. $\qquad\square$

Proposition 2.5. *Assume that the groups $G_{A,\ell}$ are connected for all ℓ.*
  (i) *The algebraic group $G_{A,\ell}$ is reductive for all ℓ.*
  (ii) *For $\ell \gg_A 1$, the $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell}$ is reductive.*

Proof. Part (i) is a direct consequence of Proposition 2.4(i). Part (ii) is proved in [LP95] though also see [Win02, §1.3]. $\qquad\square$

2.3. **The Mumford–Tate conjecture.** After fixing an embedding $\overline{K} \subseteq \mathbb{C}$, the comparison isomorphism $V_\ell(A) \cong V \otimes_\mathbb{Q} \mathbb{Q}_\ell$ induces an isomorphism $\mathrm{GL}_{V_\ell(A)} \cong \mathrm{GL}_{V,\mathbb{Q}_\ell}$. The following conjecture says that $G_{A,\ell}^\circ$ and $(G_A)_{\mathbb{Q}_\ell}$ are the same algebraic group when we use the comparison isomorphism as an identification, cf. [Ser77, §3].

Conjecture 2.6 (Mumford–Tate conjecture for A). *For each prime ℓ, we have $G_{A,\ell}^\circ = (G_A)_{\mathbb{Q}_\ell}$.*

The Mumford–Tate conjecture is still open, however significant progress has been made in showing that several general classes of abelian varieties satisfy the conjecture; we simply refer the reader to [Vas08, §1.4] for a partial list of references.

Proposition 2.7.
  (i) *For each prime ℓ, we have $G_{A,\ell}^\circ \subseteq (G_A)_{\mathbb{Q}_\ell}$.*
  (ii) *The Mumford–Tate conjecture for A holds if and only if the common rank of the groups $G_{A,\ell}^\circ$ equals the rank of G_A; in particular, the conjecture holds for one prime ℓ if and only if it holds for all ℓ.*

Proof. For a proof of (i) see [DMOS82, I, Prop. 6.2]. Part (ii) follows from [LP95, Theorem 4.3]. $\quad\square$

2.4. **Bounded index and independence.** We can identify $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$ with a (compact) subgroup of $G_{A,\ell}(\mathbb{Q}_\ell)$. We thus have a Galois representation

$$\rho_{A,\ell^\infty}\colon \mathrm{Gal}_K \to \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) \subseteq G_{A,\ell}(\mathbb{Q}_\ell).$$

As noted in §2.2, the group $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ is open in $G_{A,\ell}(\mathbb{Q}_\ell)$. So $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ is open, and hence of finite index, in $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$. The following theorem says that this index can in fact be bounded independent of ℓ.

Theorem 2.8. *There is a constant C, depending only on A, such that $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell^\infty}(\mathrm{Gal}_K)] \leq C$ for all primes ℓ.*

Proof. This is proven assuming the Mumford-Tate conjecture for A in [HR16, §10] and uncondi-
tionally in [Zyw19, Theorem 1.2(b) and §6]. $\qquad\square$

Proposition 2.9. *There is a finite extension K'/K such that the representations $\{\rho_{A,\ell^\infty}|_{\mathrm{Gal}_{K'}}\}_\ell$
are* independent*, i.e., we have*

$$\left(\prod_\ell \rho_{A,\ell^\infty}\right)(\mathrm{Gal}_{K'}) = \prod_\ell \rho_{A,\ell^\infty}(\mathrm{Gal}_{K'})$$

in $\prod_\ell G_{A,\ell}(\mathbb{Q}_\ell)$, where the products are over all primes ℓ.

Proof. This was proved by Serre [Ser13]; see also [Ser00, 138]. $\qquad\square$

2.5. **Finiteness after base extension.** Throughout this section, we assume that all the ℓ-adic
monodromy groups $G_{A,\ell}$ are connected. The goal of this section is to prove the following finiteness
result which can often serve as a substitute to assuming the Mumford-Tate conjecture for A.

For a prime ℓ, let $\mathbb{Q}_\ell^{\mathrm{un}}$ be the maximal unramified extension of $\mathbb{Q}_\ell$ in some fixed algebraic closure
$\overline{\mathbb{Q}}_\ell$. Denote by $\mathbb{Z}_\ell^{\mathrm{un}}$ the integral closure of $\mathbb{Z}_\ell$ in $\mathbb{Q}_\ell^{\mathrm{un}}$; it is a DVR with uniformizer ℓ. The residue
field of $\mathbb{Z}_\ell^{\mathrm{un}}$ is an algebraic closure $\overline{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$.

Proposition 2.10. *There is a finite collection $\{\mathcal{G}_i\}_{i\in I}$ of split reductive subgroups of $\mathrm{GL}_{2g,\mathbb{Z}}$ such
that the following hold:*

(a) *For $\ell \gg_A 1$, there is an $i \in I$ such that*

$$(\mathcal{G}_{A,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}} = (\mathcal{G}_i)_{\mathbb{Z}_\ell^{\mathrm{un}}}$$

with respect to an appropriate choice of basis of the free $\mathbb{Z}_\ell^{\mathrm{un}}$-module $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}}$.

(b) *For each $i \in I$, there is a direct sum $\mathbb{Z}^{2g} = \oplus_{j=1}^s W_j$ of representations of $\mathcal{G}_i$ so that if
$F = \mathbb{Q}$ or if $F = \mathbb{F}_\ell$ with $\ell \gg_A 1$, then $F^{2g} = \oplus_{j=1}^s (W_j \otimes_\mathbb{Z} F)$ is the decomposition of the
tautological representations of $(\mathcal{G}_i)_F$ into isotypical components.*

Before starting the proof of the proposition, we need a better understanding of $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}}$ as
a representation of $(\mathcal{G}_{A,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}}$.

Lemma 2.11. *For $\ell \gg_A 1$, there is a direct sum $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}} = \bigoplus_{j=1}^m M_j$ of representations of
$(\mathcal{G}_{A,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}}$ over $\mathbb{Z}_\ell^{\mathrm{un}}$ such that each $M_j \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \overline{\mathbb{Q}}_\ell$ is an irreducible representation of $(\mathcal{G}_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$.*

Proof. To ease notation, we set $\mathcal{G} := (\mathcal{G}_{A,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}}$. The abelian variety A is isogenous to a product
$\prod_{i=1}^s A_i$ of simple abelian varieties over K. A fixed isogeny $A \to \prod_{i=1}^s A_i$ defines an isomor-
phism $T_\ell(A) \cong \oplus_{i=1}^s T_\ell(A_i)$ of $\mathbb{Z}_\ell[\mathrm{Gal}_K]$-modules for all sufficiently large ℓ. Moreover, this is an
isomorphism of representations of $\mathcal{G}_{A,\ell}$ where $\mathcal{G}_{A,\ell}$ acts on $T_\ell(A_i)$ through a dominant morphism
$\mathcal{G}_{A,\ell} \to \mathcal{G}_{A_i,\ell}$. So by taking $\ell \gg_A 1$, we may assume without loss of generality that A is simple.
Define the ring $E := \mathrm{End}(A)$. Since A is simple, the ring $D := E \otimes_\mathbb{Z} \mathbb{Q}$ is a division algebra.

Let R_ℓ be the $\mathbb{Z}_\ell^{\mathrm{un}}$-submodule of $\mathrm{End}_{\mathbb{Z}_\ell^{\mathrm{un}}}(T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}})$ generated by $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$; it is a $\mathbb{Z}_\ell^{\mathrm{un}}$-
algebra. We claim that by taking $\ell \gg_A 1$, every finitely generated and torsion-free R_ℓ-module
is projective. Fix an embedding $\overline{K} \subseteq \mathbb{C}$. The ring E of endomorphisms acts faithfully on $\Lambda :=
H_1(A(\mathbb{C}), \mathbb{Z})$ so we may view E as a subring of $\mathrm{End}_\mathbb{Z}(\Lambda) \cong M_{2g}(\mathbb{Z})$. Let R be the centralizer of E in
$\mathrm{End}_\mathbb{Z}(\Lambda)$. Using the comparison isomorphism $T_\ell(A) = \Lambda \otimes_\mathbb{Z} \mathbb{Z}_\ell$, we may view $R \otimes_\mathbb{Z} \mathbb{Z}_\ell$ as a subalgebra
of $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$. Since the actions of Gal_K and E on $T_\ell(A)$ commute, $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ is a subset
of $R \otimes_\mathbb{Z} \mathbb{Z}_\ell$. After taking ℓ sufficiently large, $R \otimes_\mathbb{Z} \mathbb{Z}_\ell$ will be the $\mathbb{Z}_\ell$-submodule of $\mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(A))$
generated by $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$, see the last remark in [Fal86]. So in $\mathrm{End}_{\mathbb{Z}_\ell^{\mathrm{un}}}(T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}})$, we have
$R_\ell = R \otimes_\mathbb{Z} \mathbb{Z}_\ell^{\mathrm{un}}$. Since $D = E \otimes_\mathbb{Z} \mathbb{Q}$ is a division algebra, $R \otimes_\mathbb{Z} \mathbb{Q}$ is a simple algebra [Stacks, Theorem
074T]. Since R is a $\mathbb{Z}$-order in $R \otimes_\mathbb{Z} \mathbb{Q}$, we find that $R_\ell = R \otimes_\mathbb{Z} \mathbb{Z}_\ell^{\mathrm{un}}$ is a maximal $\mathbb{Z}_\ell^{\mathrm{un}}$-order in

$R \otimes_{\mathbb{Z}} \mathbb{Q}_\ell^{\mathrm{un}}$ after taking ℓ sufficiently large, cf. [CR81, §23] for background on orders. The claim is then a consequence of Theorem 26.12 of [CR81].

Let M be any $\mathbb{Z}_\ell^{\mathrm{un}}$-submodule of $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}}$ that is a representation of $\mathcal{G}$. Since $\mathbb{Z}_\ell^{\mathrm{un}}$ is a DVR, M is a free $\mathbb{Z}_\ell^{\mathrm{un}}$-module of finite rank. We will now show that $M = \oplus_{j=1}^m M_j$ where the M_j are representations of $\mathcal{G}$ over $\mathbb{Z}_\ell^{\mathrm{un}}$ for which the $M_j \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \mathbb{Q}_\ell^{\mathrm{un}}$ are irreducible representations of $\mathcal{G}_{\mathbb{Q}_\ell^{\mathrm{un}}}$. We may assume that M is nonzero since the result is trivial otherwise. Since $\mathcal{G}_{\mathbb{Q}_\ell^{\mathrm{un}}}$ is reductive, there is a direct sum $M \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \mathbb{Q}_\ell^{\mathrm{un}} = \oplus_{i=1}^t V_i$ of irreducible representations of $\mathcal{G}_{\mathbb{Q}_\ell^{\mathrm{un}}}$. Define $M_1 := M \cap V_1$; it is a representation of $\mathcal{G}$ over $\mathbb{Z}_\ell^{\mathrm{un}}$ and $M_1 \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \mathbb{Q}_\ell^{\mathrm{un}} = V_1$. Note that the $\mathbb{Z}_\ell^{\mathrm{un}}$-module M/M_1 is torsion free. Consider the short exact sequence

$$0 \to M_1 \to M \to M/M_1 \to 0$$

of representations of $\mathcal{G}$. This can also be viewed as a short exact sequence of R_ℓ-modules with M/M_1 being finitely generated and torsion-free. The claim we proved above says that M/M_1 is a projective R_ℓ-module. So our short exact sequence splits and we obtain a direct sum $M = M_1 \oplus M'$ of R_ℓ-modules and hence also of representations of $\mathcal{G} = (\mathcal{G}_{A,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}}$ over $\mathbb{Z}_\ell^{\mathrm{un}}$. Now proceeding by induction on the rank over $\mathbb{Z}_\ell^{\mathrm{un}}$, we deduce the existence of the desired direct sum $M = \oplus_{j=1}^m M_j$.

By considering the special case $M = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}}$, we obtain a direct sum $T_\ell(A) = \oplus_{j=1}^m M_j$, where M_j is a representation of $\mathcal{G}$ over $\mathbb{Z}_\ell^{\mathrm{un}}$ such that $M_j \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \mathbb{Q}_\ell^{\mathrm{un}}$ is an irreducible representation of $\mathcal{G}_{\mathbb{Q}_\ell^{\mathrm{un}}}$.

For a fixed $1 \leq j \leq m$, it remains to show that $M_j \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \overline{\mathbb{Q}}_\ell$ is an irreducible representation of $\mathcal{G}_{\overline{\mathbb{Q}}_\ell}$. The ring $D = E \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra whose center L is a number field. Define the integers $d = [L : \mathbb{Q}]$ and $n = [D : L]^{1/2}$. Choose a finite extension L_1 of L that splits D, i.e., $D \otimes_L L_1 \cong M_n(L_1)$. By choosing ℓ large enough, we may assume that ℓ is unramified in the number field L_1. Since ℓ is unramified in L, there are exactly d embeddings $L \hookrightarrow \mathbb{Q}_\ell^{\mathrm{un}}$. Therefore, we have isomorphisms

$$D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell^{\mathrm{un}} = D \otimes_L (L \otimes_{\mathbb{Q}} \mathbb{Q}_\ell^{\mathrm{un}}) = D \otimes_L (\prod_\sigma \mathbb{Q}_\ell^{\mathrm{un}}) = \prod_\sigma (D \otimes_{L,\sigma} \mathbb{Q}_\ell^{\mathrm{un}}),$$

where the σ vary over the embeddings $L \hookrightarrow \mathbb{Q}_\ell^{\mathrm{un}}$. Since ℓ is unramified in L_1, any embedding $\sigma \colon L \hookrightarrow \mathbb{Q}_\ell^{\mathrm{un}}$ extends to an embedding of L_1. So we isomorphisms

$$D \otimes_{L,\sigma} \mathbb{Q}_\ell^{\mathrm{un}} = (D \otimes_L L_1) \otimes_{L_1,\sigma} \mathbb{Q}_\ell^{\mathrm{un}} \cong M_n(L_1) \otimes_{L_1,\sigma} \mathbb{Q}_\ell^{\mathrm{un}} \cong M_n(\mathbb{Q}_\ell^{\mathrm{un}})$$

of $\mathbb{Q}_\ell^{\mathrm{un}}$-algebras. Therefore, $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell^{\mathrm{un}} \cong M_n(\mathbb{Q}_\ell^{\mathrm{un}})^d$.

From Proposition 2.4(ii), the commutant of $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ is isomorphic to $E \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Therefore, the commutant of $\mathcal{G}_{\mathbb{Q}_\ell^{\mathrm{un}}}$ in $\mathrm{End}_{\mathbb{Q}_\ell^{\mathrm{un}}}(V_\ell(A) \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell^{\mathrm{un}})$ is isomorphic to $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell^{\mathrm{un}} \cong M_n(\mathbb{Q}_\ell^{\mathrm{un}})^d$. Since $\mathcal{G}_{\mathbb{Q}_\ell^{\mathrm{un}}}$ is reductive, we can read from this that $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell^{\mathrm{un}} = V_\ell(A) \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell^{\mathrm{un}}$ has d isotypical components with each irreducible representation occuring with multiplicity n. The same holds true for the representation $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell$ since $D \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell \cong M_n(\overline{\mathbb{Q}}_\ell)^d$. So for any irreducible representation $V \subseteq T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell^{\mathrm{un}}$ of $\mathcal{G}_{\mathbb{Q}_\ell^{\mathrm{un}}}$, $V \otimes_{\mathbb{Q}_\ell^{\mathrm{un}}} \overline{\mathbb{Q}}_\ell$ is also an irreducible representation of $(G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$. The lemma is now immediate. $\qquad\square$

Proof of Proposition 2.10. By taking $\ell \gg_A 1$, we may assume by Proposition 2.5(ii) that the $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell} \subseteq \mathrm{GL}_{T_\ell(A)}$ is reductive. By Lemma 2.11 and taking $\ell \gg_A 1$, we may assume that there is a direct sum

$$T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}} = \oplus_{j=1}^m M_j$$

of representations of $(\mathcal{G}_{A,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}}$ over $\mathbb{Z}_\ell^{\mathrm{un}}$ so that each representation M_j is geometrically irreducible.

We claim that the reductive group $(G_{A,\ell})_{\mathbb{Q}_\ell^{\mathrm{un}}}$ is split for all $\ell \gg_A 1$. There is a torus T defined over $\mathbb{Q}$ such that $T_{\mathbb{Q}_\ell}$ is isomorphic to a maximal torus of $G_{A,\ell}$ for all ℓ, cf. [Chi92, §3b]. The torus $T_{\mathbb{Q}_\ell^{\mathrm{un}}}$ is split for all large enough ℓ (for example, it holds for all ℓ that are unramified in some

number field over which T splits). This proves the claim and we may now assume that $(G_{A,\ell})_{\mathbb{Q}_\ell^{\mathrm{un}}}$ is split.

Let $\mathcal{C}_\ell$ and $\mathcal{S}_\ell$ be the central torus and the derived subgroup, respectively, of the reductive $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell}$. The groups $(\mathcal{C}_\ell)_{\mathbb{Z}_\ell^{\mathrm{un}}}$ and $(\mathcal{S}_\ell)_{\mathbb{Z}_\ell^{\mathrm{un}}}$ are both split since $(\mathcal{G}_{A,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}}$ is split. There is a split semisimple group scheme $\mathcal{S}$ over $\mathbb{Z}$ for which there is an isomorphism

$$f_\ell \colon \mathcal{S}_{\mathbb{Z}_\ell^{\mathrm{un}}} \xrightarrow{\sim} (\mathcal{S}_\ell)_{\mathbb{Z}_\ell^{\mathrm{un}}},$$

cf. [SGA3 III, Exposé XXV, Théorème 1.1 for the existence of $\mathcal{S}$ and Exposé XXIII, Corollaire 5.1 for the isomorphism]. We can construct $\mathcal{S}$ directly from the root datum of $(\mathcal{S}_\ell)_{\mathbb{Z}_\ell^{\mathrm{un}}}$. There are only finitely many possibilities for this root datum, up to isomorphism, since our semisimple groups have dimension bounded independent of ℓ. So we may assume that only finitely many $\mathbb{Z}$-group schemes $\mathcal{S}$ arise as we vary ℓ.

Let C be the central torus of the Mumford–Tate group $G_A \subseteq \mathrm{GL}_{V_A}$, where $V_A = H_1(A(\mathbb{C}), \mathbb{Q})$. Fix a minimal field extension L of $\mathbb{Q}$ for which the torus C_L is split and let $X(C_L)$ be the group of characters $C_L \to \mathbb{G}_{m,L}$. Let $\mathcal{C}$ be the split torus over $\mathbb{Z}$ isomorphic to C_L over L for which we can identify its character group $X(\mathcal{C})$ with $X(C_L)$. Let $\Omega \subseteq X(C_L) = X(\mathcal{C})$ be the (finite) set of weights of the action of the torus C_L on $V_A \otimes_{\mathbb{Q}} L$.

We have an inclusion of groups $G_{A,\ell} \subseteq (G_A)_{\mathbb{Q}_\ell}$ by Proposition 2.7(i). By [UY13, Corollary 2.11], their central tori agree, i.e., $(\mathcal{C}_\ell)_{\mathbb{Q}_\ell} = C_{\mathbb{Q}_\ell}$. By taking $\ell \gg_A 1$, we may assume that ℓ is unramified in L and hence there is an embedding $\sigma \colon L \hookrightarrow \mathbb{Q}_\ell^{\mathrm{un}}$. Using the embedding σ, we obtain an isomorphism between $(\mathcal{C}_\ell)_{\mathbb{Q}_\ell^{\mathrm{un}}} = C_{\mathbb{Q}_\ell^{\mathrm{un}}} = (C_L)_{\mathbb{Q}_\ell^{\mathrm{un}}}$ and $(\mathcal{C}_L)_{\mathbb{Q}_\ell^{\mathrm{un}}} = \mathcal{C}_{\mathbb{Q}_\ell^{\mathrm{un}}}$. Since the tori $\mathcal{C}_\ell$ and $\mathcal{C}$ are split over $\mathbb{Z}_\ell^{\mathrm{un}}$, this gives rise to an isomorphism

$$f_\ell' \colon \mathcal{C}_{\mathbb{Z}_\ell^{\mathrm{un}}} \xrightarrow{\sim} (\mathcal{C}_\ell)_{\mathbb{Z}_\ell^{\mathrm{un}}}.$$

Using our isomorphisms f_ℓ and f_ℓ', we may view $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}}$ and each M_j as $\mathbb{Z}_\ell^{\mathrm{un}}$-representations of $\mathcal{S}_{\mathbb{Z}_\ell^{\mathrm{un}}}$ and $\mathcal{C}_{\mathbb{Z}_\ell^{\mathrm{un}}}$. Note that these actions of $\mathcal{S}_{\mathbb{Z}_\ell^{\mathrm{un}}}$ and $\mathcal{C}_{\mathbb{Z}_\ell^{\mathrm{un}}}$ commute with each other.

Now take any $1 \leq j \leq m$. Since $M_j \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \overline{\mathbb{Q}}_\ell$ is an irreducible representation of $(\mathcal{G}_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$, it must also be an irreducible representation of $(\mathcal{S}_\ell)_{\overline{\mathbb{Q}}_\ell}$ with $(\mathcal{C}_\ell)_{\overline{\mathbb{Q}}_\ell}$ acting via a single character $\alpha_j \in X(\mathcal{C})$. The character α_j lies in Ω since with respect to the comparison isomorphism $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell = V_A \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$ it corresponds to a weight of $C_{\overline{\mathbb{Q}}_\ell}$.

Let μ_j be the dominant weight of $\mathcal{S}$ that arises as the highest weight of the irreducible representation $M_j \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \mathbb{Q}_\ell$ of $\mathcal{S}_{\mathbb{Q}_\ell}$ (this lies in the character group of a fixed split maximal torus of $\mathcal{S}$ and is with respect to a choice of a positive system of roots). The minuscule weight conjecture, proved by Pink [Pin98, Corollary 5.11], says that all the weights of $T_\ell(A) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}}_\ell$ as a representation of $(S_\ell)_{\overline{\mathbb{Q}}_\ell}$ are minuscule. Since a semisimple group has only finitely many minuscule weights, we find that for our given $\mathcal{S}$, there are only finitely many possibilities for μ_j.

Following Jantzen [Jan03, II.8.3], there is a $\mathbb{Z}$-representation $V(\mu_j)$ of $\mathcal{S}$ such that for any field F of characteristic 0, $V(\mu_j) \otimes_{\mathbb{Z}} F$ is the unique irreducible representation of $\mathcal{S}_F$, up to isomorphism, with highest weight μ_j. In particular, $M_j \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \mathbb{Q}_\ell^{\mathrm{un}}$ and $V(\mu_j) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell^{\mathrm{un}}$ are isomorphic representations of $\mathcal{S}_{\mathbb{Q}_\ell^{\mathrm{un}}}$.

Since μ_j is a minuscule weight, all the weights of the action of $\mathcal{S}_{\overline{\mathbb{F}}_\ell}$ on $V(\mu_j) \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_\ell$ lie in a single orbit for the Weyl group, and therefore $V(\mu_j) \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_\ell$ is an irreducible representation of $\mathcal{S}_{\overline{\mathbb{F}}_\ell}$, see also [GGN17] (and in particular [GGN17, p. 73, Generalization of Theorem 1.1 to split reductive groups]).

We now claim that M_j and $V(\mu_j) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell^{\mathrm{un}}$ are isomorphic $\mathbb{Z}_\ell^{\mathrm{un}}$-representations of $\mathcal{S}_{\mathbb{Z}_\ell^{\mathrm{un}}}$. We know there is an isomorphism $M_j \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \mathbb{Q}_\ell^{\mathrm{un}} = V(\mu_j) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell^{\mathrm{un}}$ of $\mathcal{S}_{\mathbb{Q}_\ell^{\mathrm{un}}}$ representations that we will view as an identification; this allows us to compare M_j and $\mathcal{V} := V(\mu_j) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell^{\mathrm{un}}$ which are $\mathbb{Z}_\ell^{\mathrm{un}}$-modules

of the same rank. Since $\mathbb{Z}_\ell^{\mathrm{un}}$ is a DVR with uniformizer ℓ, we can scale our isomorphism by an appropriate power of ℓ so that $M_j \subseteq \mathcal{V}$ and $M_j \not\subseteq \ell\mathcal{V}$. To prove that $\mathcal{V} = M_j$, it suffices to show that the quotient map $\varphi \colon M_j \to \mathcal{V}/\ell\mathcal{V}$ is surjective. Define $W := \varphi(M_j)$. Since $\overline{\mathbb{F}}_\ell$ is the residue field of $\mathbb{Z}_\ell^{\mathrm{un}}$, $\mathcal{V}/\ell\mathcal{V}$ is an $\overline{\mathbb{F}}_\ell$-vector space. Moreover, $\mathcal{V}/\ell\mathcal{V}$ is a representation of $\mathcal{S}_{\overline{\mathbb{F}}_\ell}$ that is isomorphic to $\mathcal{V} \otimes_{\mathbb{Z}_\ell^{\mathrm{un}}} \overline{\mathbb{F}}_\ell$. By our previous claim, $\mathcal{V}/\ell\mathcal{V}$ is an irreducible representation of $\mathcal{S}_{\overline{\mathbb{F}}_\ell}$. Since $W \subseteq \mathcal{V}/\ell\mathcal{V}$ is also a representation of $\mathcal{S}_{\overline{\mathbb{F}}_\ell}$, we have $W = 0$ or $W = \mathcal{V}/\ell\mathcal{V}$. We have $W \neq 0$ since $M_j \not\subseteq \ell\mathcal{V}$ and thus φ is surjective.

Define $N_j := V(\mu_j)$; it is a free $\mathbb{Z}$-module of finite rank that has an action of $\mathcal{S}$. We let $\mathcal{C}$ act on N_j via the character α_j. Now define the $\mathbb{Z}$-module $N := \oplus_{j=1}^m N_j$; it is a representation over $\mathbb{Z}$ of $\mathcal{S}$ and $\mathcal{C}$. We have shown above that there is an isomorphism $N_j \otimes_{\mathbb{Z}} \mathbb{Z}_\ell^{\mathrm{un}} = V(\mu_j) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell^{\mathrm{un}} \xrightarrow{\sim} M_j$ of $\mathbb{Z}_\ell^{\mathrm{un}}$-modules that respects the action of $\mathcal{S}_{\mathbb{Z}_\ell^{\mathrm{un}}}$; it also respects the $\mathcal{C}_{\mathbb{Z}_\ell^{\mathrm{un}}}$-action since the torus acts on both by the character α_j. Combining these together, we obtain an isomorphism

$$\psi_\ell \colon N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell^{\mathrm{un}} \xrightarrow{\sim} \oplus_{j=1}^m M_j = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}}$$

of $\mathbb{Z}_\ell^{\mathrm{un}}$-modules that respects the actions of $\mathcal{S}_{\mathbb{Z}_\ell^{\mathrm{un}}}$ and $\mathcal{C}_{\mathbb{Z}_\ell^{\mathrm{un}}}$. Using that $\mathcal{G}_{A,\ell}$ acts faithfully on $T_\ell(A)$, we find that $\mathcal{S}$ and $\mathcal{C}$ act faithfully on N and hence we may view them as subgroups of GL_N. Since $\mathcal{S}$ and $\mathcal{C}$ commute, the subgroup of GL_N generated by $\mathcal{S}$ and $\mathcal{C}$ is a reductive $\mathbb{Z}$-group scheme $\mathcal{G}$. Taking f_ℓ and f'_ℓ into account, the isomorphism

$$\mathrm{GL}_{N \otimes_{\mathbb{Z}} \mathbb{Z}_\ell^{\mathrm{un}}} \xrightarrow{\sim} \mathrm{GL}_{T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell^{\mathrm{un}}}$$

of $\mathbb{Z}_\ell^{\mathrm{un}}$-groups coming from ψ_ℓ gives isomorphisms $\mathcal{S}_{\mathbb{Z}_\ell^{\mathrm{un}}} \xrightarrow{\sim} (\mathcal{S}_\ell)_{\mathbb{Z}_\ell^{\mathrm{un}}}$ and $\mathcal{C}_{\mathbb{Z}_\ell^{\mathrm{un}}} \xrightarrow{\sim} (\mathcal{C}_\ell)_{\mathbb{Z}_\ell^{\mathrm{un}}}$, and hence also an isomorphism $\mathcal{G}_{\mathbb{Z}_\ell^{\mathrm{un}}} \xrightarrow{\sim} (\mathcal{G}_{A,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}}$. After choosing a basis of N over $\mathbb{Z}$, we can view $\mathcal{G}$ as a subgroup of $\mathrm{GL}_{2g,\mathbb{Z}}$. To complete our proof of (a), we need to explain why only finitely many such groups $\mathcal{G}$ need arise as we vary ℓ. In our construction, $\mathcal{C}$ is independent of ℓ and only finitely many $\mathcal{S}$, up to isomorphism, will occur. There are only finitely many representations N_j of $\mathcal{S}$ and $\mathcal{G}$ that will occur since only finitely many dominant weights μ_j show up and there are only finitely many $\alpha_j \in \Omega$. This implies that only a finite number of representations N of $\mathcal{S}$ and $\mathcal{C}$ will occur since the rank of N must be $2g$. Thus our construction gives rise to only finitely many possible groups $\mathcal{G} \subseteq \mathrm{GL}_N$ for $\ell \gg_A 1$.

We now prove (b). We keep notation as in the above construction of $\mathcal{G} \subseteq \mathrm{GL}_N$. Each representation N_j of $\mathcal{G}$ was constructed using the dominant weight μ_j of $\mathcal{S}$ and the character α_j of $\mathcal{C}$. Let F be the field $\mathbb{Q}$ or $\mathbb{F}_\ell$. From the irreducible representation $N_j \otimes_{\mathbb{Z}} F$ of $\mathcal{G}_F$, we can recover μ_j and α_j since we know the central torus acts via a character and the action of the derived subgroup is given by its highest weight (for $F = \mathbb{F}_\ell$, the irreducibility was shown above for $\ell \gg_A 1$ when we proved that $V(\mu_j) \otimes_{\mathbb{Z}} \overline{\mathbb{F}}_\ell$ is an irreducible representation of $\mathcal{S}_{\overline{\mathbb{F}}_\ell}$). Therefore, the isomorphism class of the representation $N_j \otimes_{\mathbb{Z}} F$ of $\mathcal{G}_F$ is determined by (μ_j, α_j). So let $\mathcal{I}$ be the set of pairs (μ_j, α_j) corresponding to the $(\mathcal{S} \times \mathcal{C})$-modules N_j, with $1 \leq j \leq m$. For each $(\mu, \alpha) \in \mathcal{I}$, let $W_{(\mu,\alpha)}$ be the direct sum of the N_j with $1 \leq j \leq m$ for which $(\mu_j, \alpha_j) = (\mu, \alpha)$. Therefore, $N = \oplus_{(\mu,\alpha) \in \mathcal{I}} W_{(\mu,\alpha)}$ and $N \otimes_{\mathbb{Z}} F = \oplus_{(\mu,\alpha) \in \mathcal{I}} (W_{(\mu,\alpha)} \otimes_{\mathbb{Z}} F)$ is the decomposition into isotypical components as a representation of $\mathcal{G}_F$. $\qquad\square$

2.6. Points modulo ℓ.
Throughout this section, we will assume that all the ℓ-adic monodromy groups $G_{A,\ell}$ are connected. Choosing a $\mathbb{Z}_\ell$-basis for $T_\ell(A)$, we can identify $\mathcal{G}_{A,\ell}$ with an algebraic subgroup of $\mathrm{GL}_{2g,\mathbb{Z}_\ell}$ and hence identify the special fiber $G := (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ with an algebraic subgroup of $\mathrm{GL}_{2g,\mathbb{F}_\ell}$. For each subspace $W \subseteq \mathbb{F}_\ell^{2g}$, let G_W be the algebraic subgroup of G as defined in §1.1. The goal of this section is to give bounds on the cardinality of $G_W(\mathbb{F}_\ell)$ that do not depend on W.

For $W \subseteq \mathbb{F}_\ell^{2g}$, let m_W be the number of irreducible components of $(G_W)_{\overline{\mathbb{F}}_\ell}$. Since $(G_W)_{\overline{\mathbb{F}}_\ell}$ is an algebraic group, all its irreducible components are disjoint and have the same dimension. Our next lemma bounds m_W uniformly in ℓ and W; see also [Lom17, Lemma 6] for a closely related result.

Lemma 2.12. *We have $m_W \ll_A 1$ for all primes ℓ and subspaces $W \subseteq \mathbb{F}_\ell^{2g}$.*

Proof. Fix a prime ℓ and a subspace $W \subseteq \mathbb{F}_\ell^{2g}$. In our proof, we can always take ℓ to be sufficiently large since this only excludes a finite number of groups G_W from consideration.

Set $n := 4g^2 + 1$. We can view $\mathrm{GL}_{2g,\mathbb{F}_\ell}$ as a closed subvariety of $\mathbb{A}^n_{\mathbb{F}_\ell}$ by identifying a matrix with its $(2g)^2$ entries and its determinant. Let ι be the embedding given by the inclusions

$$\mathrm{GL}_{2g,\mathbb{F}_\ell} \subset \mathbb{A}^n_{\mathbb{F}_\ell} \subset \mathbb{P}^n_{\mathbb{F}_\ell}.$$

By definition, $G_W = G \cap (\mathrm{GL}_{2g,\mathbb{F}_\ell})_W$ with $(\mathrm{GL}_{2g,\mathbb{F}_\ell})_W$ determined by homogenenous linear equations in the entries of the matrices in $\mathrm{GL}_{2g,\mathbb{F}_\ell}$. So there is a linear subspace L of $\mathbb{P}^n_{\mathbb{F}_\ell}$ such that $\iota(G) \cap L = \iota(G_W)$. We can choose a linear subspace L' in $\mathbb{P}^n_{\mathbb{F}_\ell}$ of codimension $\dim G_W$ that intersects every irreducible component of $\iota(G_W)_{\overline{\mathbb{F}}_\ell}$ and $\iota(G_W)_{\overline{\mathbb{F}}_\ell} \cap L'$ is finite. Let X be the Zariski closure of $\iota(G)$ in $\mathbb{P}^n_{\mathbb{F}_\ell}$. We find that $X_{\overline{\mathbb{F}}_\ell} \cap L_{\overline{\mathbb{F}}_\ell} \cap L'$ is zero dimensional and that the number of its $\overline{\mathbb{F}}_\ell$-points gives an upper bound for m_W. By a suitable version of Bézout's theorem (for example, [Ful98, Example 8.4.6]), we deduce that

$$m_W \leq \deg(X_{\overline{\mathbb{F}}_\ell}) \cdot \deg(L_{\overline{\mathbb{F}}_\ell}) \cdot \deg(L').$$

Therefore, $m_W \leq \deg(X_{\overline{\mathbb{F}}_\ell})$ since linear spaces have degree 1. See [Ful98, §8.4] for background on Bézout's theorem and the degree of a closed subvariety of projective space.

Proposition 2.10 implies that there is a finite collection $\{\mathcal{G}_i\}_{i \in I}$ of reductive subgroups of $\mathrm{GL}_{2g,\mathbb{Z}}$ such that for all sufficiently large ℓ, $G_{\overline{\mathbb{F}}_\ell}$ and $(\mathcal{G}_i)_{\overline{\mathbb{F}}_\ell}$ are conjugate in $\mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell}$ for some $i \in I$. Using that I is finite, this implies that the subvariety $X_{\overline{\mathbb{F}}_\ell}$ of $\mathbb{P}^n_{\overline{\mathbb{F}}_\ell}$ can be defined by a finite set S of homogenous polynomials with $|S|$ and the degree of the $f \in S$ bounded in terms of a constant depending only on A. By Bézout's theorem (for example, [Ful98, Example 8.4.6]), we deduce that $\deg(X_{\overline{\mathbb{F}}_\ell}) \ll_A 1$. Therefore, $m_W \ll_A 1$. $\square$

Proposition 2.13. *Define $G := (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$. We have $|G_W(\mathbb{F}_\ell)| \asymp_A \ell^{\dim G_W}$ for all subspaces $W \subseteq \mathbb{F}_\ell^{2g}$.*

Proof. We have inequalities $|G_W^\circ(\mathbb{F}_\ell)| \leq |G_W(\mathbb{F}_\ell)| \leq m_W \cdot |G_W^\circ(\mathbb{F}_\ell)|$. Since $m_W \ll_A 1$ by Lemma 2.12, it suffices to show that $|G_W^\circ(\mathbb{F}_\ell)| \asymp_A \ell^{\dim G_W}$. So the proposition is a consequence of [Nor87, Lemma 3.5] which shows that $(\ell - 1)^{\dim G_W} \leq |G_W^\circ(\mathbb{F}_\ell)| \leq (\ell + 1)^{\dim G_W}$. $\square$

3. CODIMENSION BOUNDS

3.1. **Lie algebras.** Let V be a nonzero finite-dimensional vector space over a field F. Let $\mathfrak{gl}(V)$ be the Lie algebra consisting of the F-linear endomorphisms of V with the commutator serving as the Lie bracket.

Definition 3.1. Fix a Lie subalgebra $\mathfrak{g}$ of $\mathfrak{gl}(V)$. For each subspace W of V, let $\mathfrak{g}_W$ be the subspace of $\mathfrak{g}$ consisting of $B \in \mathfrak{g}$ such that $Bw = 0$ for all $w \in W$. Observe that $\mathfrak{g}_W$ is a Lie subalgebra of $\mathfrak{g}$. For each nonzero subspace W of V, we define the nonnegative rational number

$$\alpha(\mathfrak{g}, W) := \frac{\dim \mathfrak{g} - \dim \mathfrak{g}_W}{\dim W}.$$

There are only finitely many possibilities for the numerator and denominator of $\alpha(\mathfrak{g}, W)$, so we can define

$$\alpha(\mathfrak{g}) := \min_{W \neq 0} \alpha(\mathfrak{g}, W),$$

where the minimum is over all nonzero subspaces W of V. Note that the notation $\alpha(\mathfrak{g})$ suppresses the dependence on the ambient algebra $\mathfrak{gl}(V)$. We define $\alpha(\mathfrak{g}, 0) = 0$.

The values of $\alpha(\mathfrak{g}, W)$ satisfy the main axiom of "slope theory", which is given in the following lemma.

Lemma 3.2. *For any nonzero subspaces W and W' of V,*

$$\alpha(\mathfrak{g}, W + W') \dim(W + W') + \alpha(\mathfrak{g}, W \cap W') \dim(W \cap W') \leq \alpha(\mathfrak{g}, W) \dim W + \alpha(\mathfrak{g}, W') \dim W'.$$

Proof. The linear map $\mathfrak{g}_W \to \mathfrak{g}_{W \cap W'}/\mathfrak{g}_{W'}$ has kernel $\mathfrak{g}_W \cap \mathfrak{g}_{W'} = \mathfrak{g}_{W+W'}$, so

$$\dim(\mathfrak{g}_W/\mathfrak{g}_{W+W'}) \leq \dim(\mathfrak{g}_{W \cap W'}/\mathfrak{g}_{W'}).$$

Equivalently,

$$\alpha(\mathfrak{g}, W + W') \dim(W + W') - \alpha(\mathfrak{g}, W) \dim W \leq \alpha(\mathfrak{g}, W') \cdot \dim W' - \alpha(\mathfrak{g}, W \cap W') \dim(W \cap W'),$$

which gives the desired inequality. $\qquad\qquad\square$

Lemma 3.3.
   (i) *There exists a unique maximal subspace U of V satisfying $\alpha(\mathfrak{g}, U) = \alpha(\mathfrak{g})$.*
   (ii) *If $\alpha(\mathfrak{g}, W) = \alpha(\mathfrak{g})$ and $\alpha(\mathfrak{g}, W') = \alpha(\mathfrak{g})$ for nonzero subspaces W and W' of V, then $\alpha(\mathfrak{g}, W + W') = \alpha(\mathfrak{g})$.*

Proof. We first prove (ii). By Lemma 3.2 and our assumptions, we have

$$\alpha(\mathfrak{g}, W + W') \dim(W + W') + \alpha(\mathfrak{g}, W \cap W') \dim(W \cap W') \leq \alpha(\mathfrak{g})(\dim W + \dim W').$$

Since $\alpha(\mathfrak{g}) \leq \alpha(\mathfrak{g}, W \cap W')$ when $W \cap W' \neq 0$, we have

$$\alpha(\mathfrak{g}, W + W') \dim(W + W') \leq \alpha(\mathfrak{g})(\dim W + \dim W' - \dim W \cap W') = \alpha(\mathfrak{g}) \dim(W + W')$$

and hence $\alpha(\mathfrak{g}, W + W') \leq \alpha(\mathfrak{g})$. Note that the same inequality also holds if $W \cap W' = 0$, since in this case the term corresponding to $W \cap W'$ in Lemma 3.2 vanishes. By the minimality of $\alpha(\mathfrak{g})$, this implies that $\alpha(\mathfrak{g}, W + W') = \alpha(\mathfrak{g})$. This completes the proof of (ii).

We have $\alpha(\mathfrak{g}, W) = \alpha(\mathfrak{g})$ for some nonzero subspace W of V by the definition of $\alpha(\mathfrak{g})$. By taking U to be the subspace generated by all subspaces W of V with $\alpha(\mathfrak{g}, W) = \alpha(\mathfrak{g})$, we have $\alpha(\mathfrak{g}, U) = \alpha(\mathfrak{g})$ by part (ii). Part (i) is now clear. $\qquad\square$

Fix a finite Galois extension L of F. Then $\mathfrak{g} \otimes_F L$ is a Lie subalgebra of $\mathfrak{gl}(V \otimes_F L)$ and we can define $\alpha(\mathfrak{g} \otimes_F L)$ as before. By Lemma 3.3(i), there are unique subspaces $U \subseteq V$ and $U' \subseteq V \otimes_F L$ that are maximal amongst those subspaces that satisfy $\alpha(\mathfrak{g}, U) = \alpha(\mathfrak{g})$ and $\alpha(\mathfrak{g} \otimes_F L, U') = \alpha(\mathfrak{g} \otimes_F L)$, respectively.

Lemma 3.4. *With notation as above, the inclusion $U \subseteq V$ induces an isomorphism $U \otimes_F L \xrightarrow{\sim} U'$. In particular, we have $\alpha(\mathfrak{g} \otimes_F L) = \alpha(\mathfrak{g})$.*

Proof. We have $\alpha(\mathfrak{g}) = \alpha(\mathfrak{g}, U) = \alpha(\mathfrak{g} \otimes_F L, U \otimes_F L)$ and hence $\alpha(\mathfrak{g} \otimes_F L) \leq \alpha(\mathfrak{g})$.

Take any $\sigma \in \mathrm{Gal}(L/F)$. We have $\sigma((\mathfrak{g} \otimes_F L)_{U'}) = (\mathfrak{g} \otimes_F L)_{\sigma(U')}$. Therefore, $(\mathfrak{g} \otimes_F L)_{U'}$ and $(\mathfrak{g} \otimes_F L)_{\sigma(U')}$ have the same dimension over F and hence also L. Therefore, $\alpha(\mathfrak{g} \otimes_F L, \sigma(U')) = \alpha(\mathfrak{g} \otimes_F L, U') = \alpha(\mathfrak{g} \otimes_F L)$. By the maximality of U', we have $\sigma(U') = U'$ for all $\sigma \in \mathrm{Gal}(L/K)$. By Galois descent for vectors spaces, there is a subspace U_0 of V such that the inclusion $U_0 \subseteq V$ induces an isomorphism $U_0 \otimes_F L \xrightarrow{\sim} U'$. Therefore, $\alpha(\mathfrak{g}, U_0) = \alpha(\mathfrak{g} \otimes_F L, U') = \alpha(\mathfrak{g} \otimes_F L)$. Since $\alpha(\mathfrak{g} \otimes_F L) \leq \alpha(\mathfrak{g})$, this proves that $\alpha(\mathfrak{g}, U_0) = \alpha(\mathfrak{g})$ and hence $U_0 \subseteq U$ by the maximality of U. In particular, $\alpha(\mathfrak{g}) = \alpha(\mathfrak{g} \otimes_F L)$.

We have $U_0 \otimes_F L = U \otimes_F L$ since otherwise $U \otimes_F L$ would be a subspace of $V \otimes_F L$ strictly larger than U' satisfying $\alpha(\mathfrak{g} \otimes_F L, U \otimes_F L) = \alpha(\mathfrak{g} \otimes_F L)$ which would contradict the maximality of U'. Therefore, $U_0 = U$ and the lemma follows. $\qquad\square$

3.2. Reductive groups. Let V be a nonzero finite dimensional vector space over a perfect field F. Consider a reductive group $G \subseteq \mathrm{GL}_V$. Assume that there exists a decomposition

$$V = \bigoplus_{i=1}^{n} V_i$$

of the representation V of G into isotypic components, i.e., $V_i \neq 0$ is a G-invariant subspace of V that is isomorphic to $M_i^{n_i}$ for an irreducible representation M_i of G and the representations M_i are pairwise nonisomorphic. Such a decomposition will always exist when F has characteristic 0.

For each subspace W of V, let G_W be the algebraic subgroup of G that fixes W pointwise. Define

$$\alpha(G) := \min_{W \neq 0} \frac{\dim G - \dim G_W}{\dim W},$$

where the minimum is over all nonzero subspaces $W \subseteq V$. We obviously have $\gamma_G = 1/\alpha(G)$ (the former defined in §1.1).

Let $\mathfrak{g} \subseteq \mathfrak{gl}(V)$ be the Lie algebra of G. For each subspace $W \subseteq V$, the Lie algebra of G_W agrees with the Lie algebra $\mathfrak{g}_W$ (see Definition 3.1); for a proof of the analogous statement in the case of stabilizers, see [Mil80, Proposition 10.31].

The following shows that under certain conditions, $\alpha(G)$ agrees with $\alpha(\mathfrak{g})$ and can be computed using only a finite number of special subspaces W. For each subset $I \subseteq \{1, \dots, n\}$, define $V_I := \oplus_{i \in I} V_i$.

Proposition 3.5. *Assume that the algebraic group G_{V_I} is smooth for all nonempty subsets $I \subseteq \{1, \dots, n\}$; this always holds when F has characteristic 0.*

   (i) *We have $\alpha(G) = \alpha(\mathfrak{g})$.*
   (ii) *We have*

$$\alpha(G) = \min_{\emptyset \neq I \subseteq \{1, \dots, n\}} \frac{\dim G - \dim G_{V_I}}{\dim V_I}.$$

   (iii) *We have $\alpha(G_L) = \alpha(G)$ for all field extensions L/F, where we are using the embedding $G_L \subseteq \mathrm{GL}_{V \otimes_F L}$.*

Proof. First note that the groups G_{V_I} are always smooth when F has characteristic 0 since every affine algebraic group over F is smooth by Cartier's theorem [Mil17, Theorem 3.23].

For any subspace $W \subseteq V$, we have $\dim G_W \leq \dim \mathfrak{g}_W$ since the tangent space of a variety at a point has dimension at least the dimension of the variety. We have $\dim G = \dim \mathfrak{g}$ since G is reductive and hence smooth. From the definitions of $\alpha(G)$ and $\alpha(\mathfrak{g})$, we deduce that $\alpha(\mathfrak{g}) \leq \alpha(G)$. We need to prove the other inequality.

Let U be the maximal subspace of V such that $\alpha(\mathfrak{g}, U) = \alpha(\mathfrak{g})$, see Lemma 3.3(i). We claim that U is a representation of G. Since F is perfect, to prove the claim it suffices to show that $U \otimes_F L$ is stable under the action of $G(L)$ on $V \otimes_F L$ for all finite Galois extensions L/F. Using that $\mathfrak{g} \otimes_F L$ is the Lie algebra of $G_L \subseteq \mathrm{GL}_{V \otimes_F L}$ and Lemma 3.4, we need only consider the case $L = F$, i.e., we need only show that U is stable under the action of $G(F)$. Take any $h \in G(F)$. Using that $h\mathfrak{g}h^{-1} = \mathfrak{g}$, we find that $\mathfrak{g}_{h(U)} = h\mathfrak{g}_U h^{-1}$ and hence $\alpha(\mathfrak{g}, h(U)) = \alpha(\mathfrak{g}, U) = \alpha(\mathfrak{g})$. By the maximality of U, we have $h(U) = U$ and the claim follows.

Let I be the subset of $i \in \{1, \dots, n\}$ for which $U \cap V_i \neq 0$. The set I is nonempty and we have $U = \bigoplus_{i \in I} U \cap V_i$. Note that $U \cap V_i$ is a sum of copies of the irreducible representation of which V_i is a multiple. We have

$$\mathfrak{g}_U = \bigcap_{i \in I} \mathfrak{g}_{U \cap V_i} = \bigcap_{i \in I} \mathfrak{g}_{V_i} = \mathfrak{g}_{V_I}$$

and hence $\alpha(\mathfrak{g}, V_I) = (\dim U)/(\dim V_I)\alpha(\mathfrak{g}, U) \leq \alpha(\mathfrak{g})$. Therefore, $\alpha(\mathfrak{g}, V_I) = \alpha(\mathfrak{g})$ and $V_I = U$ by the maximality of U. Since G_{V_I} is smooth by assumption, we have $\dim G_{V_I} = \dim \mathfrak{g}_{V_I}$ and hence

$$(3.1) \qquad \alpha(\mathfrak{g}) = \alpha(\mathfrak{g}, V_I) = \frac{\dim G - \dim G_{V_I}}{\dim V_I}.$$

Therefore, $\alpha(\mathfrak{g}) \geq \alpha(G)$. We have already proved the other inequality so $\alpha(\mathfrak{g}) = \alpha(G)$. We have thus proved (i), and (ii) then follows from (3.1).

It remains to prove (iii). Take any field extension L/F. For each $1 \leq i \leq n$, define the L-vector space $V_i' := V_i \otimes_F L$. Then $\bigoplus_{i=1}^n V_i'$ is the decomposition of the representation $V \otimes_F L$ of G_L into isotypic components. Take any nonempty subset $I \subseteq \{1, \dots, n\}$. Define $V_I' := \oplus_{i \in I} V_i'$. We have

$$(G_L)_{V_I'} = (G_{V_I})_L.$$

The group $(G_L)_{V_I'}$ is smooth since G_{V_I} is smooth by assumption. In particular, the assumptions of the proposition hold for $G_L \subseteq \mathrm{GL}_{V \otimes_F L}$. We have $\dim(G_L)_{V_I'} = \dim G_{V_I}$, so

$$\frac{\dim G_L - \dim(G_L)_{V_I'}}{\dim V_I'} = \frac{\dim G - \dim G_{V_I}}{\dim V_I}.$$

Since I was an arbitrary nonempty subset of $\{1, \dots, n\}$, we deduce that $\alpha(G_L) = \alpha(G)$ by (ii). $\square$

Remark 3.6. We now give an example where we do not have an equality $\alpha(\mathfrak{g}) = \alpha(G)$ over a field of positive characteristic p. Let G be the algebraic subgroup of $\mathrm{GL}_{2,\mathbb{F}_p}$ given by matrices of the form $\{(\begin{smallmatrix} x^p & 0 \\ 0 & x \end{smallmatrix})\}$. This group G is isomorphic to $\mathbb{G}_{m,\mathbb{F}_p}$ and in particular is smooth. The Lie algebra of G is $\mathfrak{g} = \{(\begin{smallmatrix} 0 & 0 \\ 0 & * \end{smallmatrix})\} \subseteq \mathfrak{gl}(\mathbb{F}_p^2)$. However, for the subspace $W := \mathbb{F}_p \cdot (\begin{smallmatrix} 1 \\ 0 \end{smallmatrix})$ the stabilizer $G_W = \mu_p$ is of dimension 0, whereas $\mathfrak{g}_W = \mathfrak{g}$ is of dimension 1. So in this case we have $\alpha(G) = 1$ while $\alpha(\mathfrak{g}) = 0$.

3.3. **The values γ_A and $\gamma_{A,\ell}$.** Fix a nonzero abelian variety A over a number field K and choose an embedding $\overline{K} \subseteq \mathbb{C}$. Choose a finite extension K' of K in $\overline{K}$ so that the abelian variety $A_{K'}$ is isogenous to a product $\prod_{i=1}^n A_i^{m_i}$, where the A_i are abelian varieties over K' that are simple and pairwise nonisogenous over $\mathbb{C}$. For each subset $I \subseteq \{1, \dots, n\}$, define $A_I := \prod_{i \in I} A_i^{m_i}$.

Define $V = H_1(A(\mathbb{C}), \mathbb{Q})$ and $V_i = H_1(A_i^{m_i}(\mathbb{C}), \mathbb{Q})$. An isogeny between $A_{K'}$ and $\prod_{i=1}^n A_i^{m_i}$ induces an isomorphism

$$(3.2) \qquad V = \bigoplus_{i=1}^n V_i.$$

By Lemma 2.2, the direct sum (3.2) is the decomposition of the representation V of G_A into isotypic components. So Proposition 3.5(ii), applied to $G_A \subseteq \mathrm{GL}_V$, implies that

$$\alpha(G_A) = \min_{\emptyset \neq I \subseteq \{1, \dots, n\}} \frac{\dim G_A - \dim(G_A)_{V_I}}{\dim V_I},$$

where $V_I := \bigoplus_{i \in I} V_i$. By (2.2), we have $\dim G_A - \dim(G_A)_{V_I} = \dim G_{A_I}$. The vector space V_I is isomorphic to $H_1(A_I(\mathbb{C}), \mathbb{Q})$ and hence has dimension $2 \dim A_I$. Therefore,

$$(3.3) \qquad \alpha(G_A) = \min_{\emptyset \neq I \subseteq \{1, \dots, n\}} \frac{\dim G_{A_I}}{2 \dim A_I} = \frac{1}{\gamma_A}.$$

In particular, we have $\gamma_{G_A} = \gamma_A$.

Proposition 3.7. *Take any field extension $F/\mathbb{Q}$ and set $G := (G_A)_F$. For any subspace W of the F-vector space $V \otimes_{\mathbb{Q}} F = H_1(A(\mathbb{C}), F)$, we have*

$$(3.4) \qquad \gamma_A \cdot (\dim G - \dim G_W) \geq \dim W.$$

Moreover, γ_A is the smallest number for which this holds.

Proof. This is just a reformulation of $\alpha((G_A)_F) = \gamma_A^{-1}$ which follows from (3.3) and Proposition 3.5(ii). $\qquad\square$

Remark 3.8. We proved Proposition 3.7 without computing the integers $\dim G_W$. In the work of Hindry and Ratazzi, for example see [HR12, HR16], they explicitly compute $\dim G_W$ to give a direct proof of Proposition 3.7 in various special cases.

Now take any prime ℓ. The ℓ-adic monodromy group $G_{A,\ell}^\circ \subseteq \mathrm{GL}_{V_\ell(A)}$ is reductive, so we can define $\alpha(G_{A,\ell}^\circ)$. We claim that $\alpha(G_{A,\ell}^\circ)$ is nonzero. If $\alpha(G_{A,\ell}^\circ) = 0$, then there would be a finite extension K'/K such that $V_\ell(A)$ has a nonzero subspace fixed pointwise by the action of $\mathrm{Gal}_{K'}$. However, this is impossible since it would imply that $A(K')[\ell^\infty]$ is infinite, contradicting the Mordell–Weil theorem. Therefore, $\alpha(G_{A,\ell}^\circ)$ is nonzero as claimed. We can now define

(3.5) $$\gamma_{A,\ell} := 1/\alpha(G_{A,\ell}^\circ).$$

Note that, by definition, for every prime ℓ we have $\gamma_{G_{A,\ell}^\circ} = \gamma_{A,\ell}$

Lemma 3.9. *Take any prime ℓ.*

(i) *We have inequalities*

$$\gamma_A \leq \max_{\emptyset \neq I \subseteq \{1,\dots,n\}} \frac{2 \dim A_I}{\dim G_{A_I,\ell}^\circ} \leq \gamma_{A,\ell}.$$

(ii) *If the Mumford–Tate conjecture for A holds, then $\gamma_A = \gamma_{A,\ell}$.*

Proof. Recall that there is a finite extension K'/K in $\overline{K}$ for which there is an isogeny $A_{K'} \to \prod_{i=1}^n A_i^{m_i}$, where the A_i are abelian varieties over K' that are simple and pairwise nonisogenous over $\mathbb{C}$. We can assume that K' is chosen large enough so that $G_{A_{K'},\ell}$ is connected.

The isogeny induces an isomorphism

$$V_\ell(A) = \bigoplus_{i=1}^n V_\ell(A_i^{m_i})$$

of $\mathbb{Q}_\ell[\mathrm{Gal}_{K'}]$-modules. In particular, $V_\ell(A)$ is a representation of $G_{A,\ell}^\circ$ and the subspaces $V_\ell(A_i^{m_i})$ are invariant under the action of $G_{A,\ell}^\circ$. Take any distinct $1 \leq i, j \leq n$. We have

(3.6) $$\mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_{K'}]}(V_\ell(A_i^{m_i}), V_\ell(A_j^{m_j})) \cong \mathrm{Hom}(A_i^{m_i}, A_j^{m_j}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$$

by Proposition 2.4(iii). Since A_i and A_j are simple and nonisogenous, we deduce that (3.6) is 0 and hence $V_\ell(A_i^{m_i})$ and $V_\ell(A_j^{m_j})$ contain no isomorphic irreducible representations of $G_{A,\ell}^\circ$. By Proposition 3.5(ii), we have

$$\alpha(G_{A,\ell}^\circ) \leq \min_{\emptyset \neq I \subseteq \{1,\dots,n\}} \frac{\dim G_{A,\ell}^\circ - \dim(G_{A,\ell}^\circ)_{\mathcal{V}_I}}{\dim \mathcal{V}_I},$$

where $\mathcal{V}_I := \bigoplus_{i \in I} V_\ell(A_i^{m_i})$. Note that we only have an inequality here since $V_\ell(A_i^{m_i})$ need not be isotypic for $G_{A,\ell}^\circ$ (though it is a direct sum of isotypic components). Since $(G_{A,\ell})_{\mathcal{V}_I}$ is the kernel of the projection homomorphism $G_{A,\ell}^\circ \to G_{A_I,\ell}$ and $\mathcal{V}_I$ has dimension $2 \dim A_I$, we have

$$\alpha(G_{A,\ell}^\circ) \leq \min_{\emptyset \neq I \subseteq \{1,\dots,n\}} \frac{\dim G_{A_I,\ell}^\circ}{2 \dim A_I},$$

This proves that $\gamma_{A,\ell} \geq \max_{\emptyset \neq I \subseteq \{1,\dots,n\}} 2 \dim A_I/(\dim G_{A_I,\ell}^\circ)$. By Proposition 2.7(i), we deduce that

$$\gamma_{A,\ell} \geq \max_{\emptyset \neq I \subseteq \{1,\dots,n\}} \frac{2 \dim A_I}{\dim G_{A_I}} = \gamma_A.$$

This completes the proof of (i). We now prove (ii). Assuming the Mumford–Tate conjecture for A, we have $\gamma_{A,\ell}^{-1} = \alpha(G_{A,\ell}^\circ) = \alpha((G_A)_{\mathbb{Q}_\ell})$. Therefore, $\gamma_{A,\ell}^{-1} = \alpha((G_A)_{\mathbb{Q}_\ell}) = \alpha(G_A) = \gamma_A^{-1}$ by Proposition 3.5(ii). $\qquad\square$

Proposition 3.10. *Assume that all the ℓ-adic monodromy groups $G_{A,\ell}$ are connected. For $\ell \gg_A 1$ we have $\alpha(G_{A,\ell}) = \alpha((\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}) = \alpha(\mathfrak{g}_{A,\ell})$ where $\mathfrak{g}_{A,\ell}$ is the Lie algebra of $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$.*

Proof. With notation as in Proposition 2.10, we fix an $i \in I$ and set $\mathcal{G} := \mathcal{G}_i$. Let $\mathbb{Z}^{2g} = \oplus_{j=1}^s W_j$ be the direct sum of representations of $\mathcal{G}$ as in Proposition 2.10(b). Since $W_j \otimes_{\mathbb{Z}} \mathbb{Q}$, with $1 \le j \le s$, are the isotypical components of the action of $\mathcal{G}_{\mathbb{Q}}$ on $\mathbb{Q}^{2g}$, Proposition 3.5(ii) implies that

$$\alpha(\mathcal{G}_{\mathbb{Q}}) = \min_{\emptyset \ne J \subseteq \{1,\ldots,s\}} \frac{\dim \mathcal{G}_{\mathbb{Q}} - \dim(\mathcal{G}_{\mathbb{Q}})_{V_J}}{\dim V_J},$$

where $V_J := \oplus_{j \in J}(W_j \otimes_{\mathbb{Z}} \mathbb{Q})$.

For each subset $J \subseteq \{1,\ldots,s\}$, define the $\mathbb{Z}$-submodule $\mathcal{V}_J = \oplus_{j \in J} W_j$ of $\mathbb{Z}^{2g}$. Recall that $\mathrm{Fix}_{\mathcal{G}}(\mathcal{V}_J)$ is a subgroup scheme of $\mathcal{G}$, and hence its generic fibre (which is an algebraic group over a field of characteristic zero) is automatically smooth. So there is a positive constant c, such that the $\mathbb{Z}_\ell$-group scheme $(\mathrm{Fix}_{\mathcal{G}}(\mathcal{V}_J))_{\mathbb{Z}_\ell}$ is smooth for all primes $\ell \ge c$ and all $J \subseteq \{1,\ldots,s\}$.

Take any prime $\ell \ge c$ and any nonempy set $J \subseteq \{1,\ldots,s\}$. Since $(\mathrm{Fix}_{\mathcal{G}}(\mathcal{V}_J))_{\mathbb{Z}_\ell}$ is smooth, its generic fiber $(\mathcal{G}_{\mathbb{Q}})_{\mathcal{V}_J \otimes_{\mathbb{Z}} \mathbb{Q}} = (\mathcal{G}_{\mathbb{Q}})_{V_J}$ and special fiber $(\mathcal{G}_{\mathbb{F}_\ell})_{\mathcal{V}_J \otimes_{\mathbb{Z}} \mathbb{F}_\ell}$ are both smooth of the same dimension. Since $\mathcal{G}_{\mathbb{Z}_\ell}$ is smooth as well, we have

$$\frac{\dim \mathcal{G}_{\mathbb{Q}} - \dim(\mathcal{G}_{\mathbb{Q}})_{V_J}}{\dim \mathcal{V}_J} = \frac{\dim \mathcal{G}_{\mathbb{F}_\ell} - \dim(\mathcal{G}_{\mathbb{F}_\ell})_{\mathcal{V}_J \otimes_{\mathbb{Z}} \mathbb{F}_\ell}}{\dim(\mathcal{V}_J \otimes_{\mathbb{Z}} \mathbb{F}_\ell)}$$

and hence

$$(3.7) \qquad \alpha(\mathcal{G}_{\mathbb{Q}}) = \min_{\emptyset \ne J \subseteq \{1,\ldots,s\}} \frac{\dim \mathcal{G}_{\mathbb{F}_\ell} - \dim(\mathcal{G}_{\mathbb{F}_\ell})_{\mathcal{V}_J \otimes_{\mathbb{Z}} \mathbb{F}_\ell}}{\dim(\mathcal{V}_J \otimes_{\mathbb{Z}} \mathbb{F}_\ell)}.$$

After increasing our constant c appropriately first, Proposition 2.10(b) tells us that the $\mathbb{F}_\ell$-vector spaces $W_j \otimes_{\mathbb{Z}} \mathbb{F}_\ell$, with $1 \le j \le s$, are the isotypical components of $\mathcal{G}_{\mathbb{F}_\ell} \subseteq \mathrm{GL}_{2g,\mathbb{F}_\ell}$. Since $\mathcal{V}_J \otimes_{\mathbb{Z}} \mathbb{F}_\ell = \oplus_{j \in J} W_j \otimes_{\mathbb{Z}} \mathbb{F}_\ell$, we deduce from (3.7) and Proposition 3.5(ii) that $\alpha(\mathcal{G}_{\mathbb{Q}}) = \alpha(\mathcal{G}_{\mathbb{F}_\ell})$; this uses that the groups $(\mathcal{G}_{\mathbb{F}_\ell})_{\mathcal{V}_J \otimes_{\mathbb{Z}} \mathbb{F}_\ell}$ are smooth. By Proposition 3.5(iii), we have $\alpha(\mathcal{G}_{\overline{\mathbb{Q}}_\ell}) = \alpha(\mathcal{G}_{\overline{\mathbb{F}}_\ell})$.

Therefore, for primes $\ell \gg_A 1$ and $i \in I$, we have $\alpha((\mathcal{G}_i)_{\overline{\mathbb{Q}}_\ell}) = \alpha((\mathcal{G}_i)_{\overline{\mathbb{F}}_\ell})$; to get that the bound on ℓ depends only on A, we use that I is finite and that the chosen groups $\mathcal{G}_i$ and the corresponding representations W_j depend only on A. By taking $\ell \gg_A 1$, Proposition 2.10(a) implies that there is an $i \in I$ such that $\alpha((\mathcal{G}_{A,\ell})_{\overline{\mathbb{Q}}_\ell}) = \alpha((\mathcal{G}_i)_{\overline{\mathbb{Q}}_\ell})$ and $\alpha((\mathcal{G}_{A,\ell})_{\overline{\mathbb{F}}_\ell}) = \alpha((\mathcal{G}_i)_{\overline{\mathbb{F}}_\ell})$. Therefore, $\alpha((\mathcal{G}_{A,\ell})_{\overline{\mathbb{Q}}_\ell}) = \alpha((\mathcal{G}_{A,\ell})_{\overline{\mathbb{Q}}_\ell})$ is equal to $\alpha((\mathcal{G}_{A,\ell})_{\overline{\mathbb{F}}_\ell})$ for $\ell \gg_A 1$. By Proposition 3.5(iii) we have $\alpha((\mathcal{G}_{A,\ell})_{\overline{\mathbb{Q}}_\ell}) = \alpha(G_{A,\ell})$ and $\alpha((\mathcal{G}_{A,\ell})_{\overline{\mathbb{F}}_\ell}) = \alpha((\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell})$, hence we obtain $\alpha(G_{A,\ell}) = \alpha((\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell})$.

Note that for $\ell \gg_A 1$, the group $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ satisfies the assumption of Proposition 3.5; it suffices to show this after base extending to $\overline{\mathbb{F}}_\ell$ and we already proved it holds for the groups $(\mathcal{G}_i)_{\overline{\mathbb{F}}_\ell}$ with $i \in I$. We thus have $\alpha((\mathcal{G}_{A,\ell})_{\overline{\mathbb{F}}_\ell}) = \alpha(\mathfrak{g}_{A,\ell})$ for $\ell \gg_A 1$ by Proposition 3.5(i). $\qquad\square$

4. Prime power version: large primes

Fix a nonzero abelian variety A of dimension g defined over a number field K. Take any prime ℓ. In §3.3, we defined a positive rational number $\gamma_{A,\ell}$; it is the smallest number for which

$$\gamma_{A,\ell} \cdot (\dim G_{A,\ell}^\circ - \dim(G_{A,\ell}^\circ)_W) \ge \dim W$$

holds for all nonzero subspaces $W \subseteq V_\ell(A)$. In this section, we prove the following bound for the ℓ-power torsion of $A(L)$ for a finite extension L/K.

Theorem 4.1. *For primes $\ell \gg_A 1$, we have*

$$|A(L)[\ell^\infty]| \ll_A [L:K]^{\gamma_{A,\ell}}$$

for all finite extensions L/K.

The above theorem actually holds for all primes ℓ and we will give a different argument for the finitely many excluded primes in §5. The proofs (both for a single ℓ and the uniform argument) are ineffective, and it would be an interesting problem to obtain explicit estimates in terms of the Faltings height of A and the degree of the field extensions.

4.1. **Lie algebras and filtrations.** For a fixed prime ℓ, set $\mathcal{G} := \mathcal{G}_{A,\ell}$. We shall assume that $G_{A,\ell}$ is connected and that $\mathcal{G}$ is a reductive group scheme over $\mathbb{Z}_\ell$.

By choosing a $\mathbb{Z}_\ell$-basis of $T_\ell(A)$, we may assume that $\mathcal{G} \subseteq \mathrm{GL}_{2g,\mathbb{Z}_\ell}$. Take any commutative $\mathbb{Z}_\ell$-algebra R. Define the ring $R[\varepsilon] := R[x]/(x^2)$, where ε is the image of x and hence satisfies $\varepsilon^2 = 0$. The R-algebra homomorphism $R[\varepsilon] \to R$ mapping ε to 0 induces a homomorphism

$$(4.1) \qquad\qquad\qquad\qquad \mathcal{G}(R[\varepsilon]) \to \mathcal{G}(R).$$

Let $L(R)$ be the set of $B \in M_{2g}(R)$ for which $I + \varepsilon B$ lies in the kernel of (4.1). Observe that $L(R)$ is a *Lie algebra* over R; it is an R-submodule of $M_{2g}(R)$ that is closed under the pairing $[B_1, B_2] = B_1 B_2 - B_2 B_1$.

The Lie algebra of $G_{A,\ell}$ is $L(\mathbb{Q}_\ell)$; its dimension as a $\mathbb{Q}_\ell$-vector space is $\dim G_{A,\ell}$. Since $\mathcal{G}$ is the Zariski closure of $G_{A,\ell}$ in $\mathrm{GL}_{2g,\mathbb{Z}_\ell}$, we find that $L(\mathbb{Z}_\ell) = L(\mathbb{Q}_\ell) \cap M_{2g}(\mathbb{Z}_\ell)$; it is a free $\mathbb{Z}_\ell$-module of rank $\dim G_{A,\ell}$.

Let $\mathfrak{g}_\ell$ be the image of the reduction modulo ℓ homomorphism $L(\mathbb{Z}_\ell) \to L(\mathbb{F}_\ell)$; it is a Lie algebra over $\mathbb{F}_\ell$ of dimension $\dim G_{A,\ell}$ (this uses that $\mathcal{G}$ is smooth over $\mathbb{Z}_\ell$).

Lemma 4.2. *The Lie algebra of $\mathcal{G}_{\mathbb{F}_\ell}$ is $\mathfrak{g}_\ell$.*

Proof. Since $\mathcal{G}$ is smooth over $\mathbb{Z}_\ell$, the Lie algebra of $\mathcal{G}_{\mathbb{F}_\ell}$ is $L(\mathbb{F}_\ell)$ and has dimension equal to $\dim \mathcal{G}_{\mathbb{F}_\ell} = \dim \mathcal{G}_{\mathbb{Q}_\ell} = \dim G_{A,\ell}$. We thus have $L(\mathbb{F}_\ell) = \mathfrak{g}_\ell$ since we have an inclusion $\mathfrak{g}_\ell \subseteq L(\mathbb{F}_\ell)$ of $\mathbb{F}_\ell$-vector spaces of the same dimension. $\qquad\square$

Now consider a closed subgroup H of $\mathcal{G}(\mathbb{Z}_\ell)$. For each integer $i \geq 1$, let $H(\ell^i)$ and H_i be the image and kernel, respectively, of the reduction modulo ℓ^i homomorphism $H \to \mathcal{G}(\mathbb{Z}/\ell^i\mathbb{Z})$. The map

$$\varphi_i \colon H_i \to M_{2g}(\mathbb{F}_\ell), \quad I + \ell^i B \mapsto B \bmod \ell$$

is a group homomorphism with kernel H_{i+1} whose image we will denote by $\mathfrak{h}_i$.

The group $\mathfrak{h}_i$ is an $\mathbb{F}_\ell$-subspace of $M_{2g}(\mathbb{F}_\ell)$ and we have

$$(4.2) \quad |H(\ell^i)| = [H:H_i] = [H:H_1] \cdot \prod_{1 \leq j < i} [H_j : H_{j+1}] = |H(\ell)| \prod_{1 \leq j < i} |\mathfrak{h}_j| = |H(\ell)| \cdot \ell^{\sum_{j=1}^{i-1} \dim \mathfrak{h}_j}$$

Lemma 4.3. *Let H be a closed subgroup of $\mathcal{G}(\mathbb{Z}_\ell)$. Take any $i \geq 1$ with $i \geq 2$ if $\ell = 2$.*

    (i) *We have $\mathfrak{h}_i \subseteq \mathfrak{g}_\ell$.*
    (ii) *If $H = \mathcal{G}(\mathbb{Z}_\ell)$, then $\mathfrak{h}_i = \mathfrak{g}_\ell$.*

Proof. Part (i) follows from (ii), so we may assume that $H = \mathcal{G}(\mathbb{Z}_\ell)$. Fix an $i \geq 1$ and take any $B \in L(\mathbb{Z}_\ell)$. We have a homomorphism $\mathcal{G}(\mathbb{Z}_\ell[\varepsilon]) \to \mathcal{G}(\mathbb{Z}/\ell^{i+1}\mathbb{Z})$ arising from the ring homomorphism $\mathbb{Z}_\ell[\varepsilon] \to \mathbb{Z}/\ell^{i+1}\mathbb{Z}$ that reduces modulo ℓ^{i+1} and sends ε to ℓ^i. In particular, $I + \ell^i B$ modulo ℓ^{i+1} lies in $\mathcal{G}(\mathbb{Z}/\ell^{i+1}\mathbb{Z})$. The reduction map $\mathcal{G}(\mathbb{Z}_\ell) \to \mathcal{G}(\mathbb{Z}/\ell^{i+1}\mathbb{Z})$ is surjective since $\mathcal{G}$ is smooth. So there is an element $I + \ell^i B' \in \mathcal{G}(\mathbb{Z}_\ell)$ such that $B \equiv B' \pmod{\ell}$. Therefore, B modulo ℓ lies in $\mathfrak{h}_i$. Since B was an arbitrary element of $L(\mathbb{Z}_\ell)$, we deduce that $\mathfrak{g}_\ell \subseteq \mathfrak{h}_i$ for all $i \geq 1$.

Now suppose that $\mathfrak{g}_\ell \subsetneq \mathfrak{h}_j$ for some $j \geq 1$ with $j \geq 2$ if $\ell = 2$. There is an element $I + \ell^i B \in H_j$ such that B modulo ℓ does not lie in $\mathfrak{g}_\ell$. Raising $I + \ell^j B$ to the ℓ-th power gives

$$(I + \ell^j B)^\ell = I + \ell^{j+1}B + \sum_{k=2}^{\ell} \binom{\ell}{k} \ell^{jk} B^k.$$

Observe that $\binom{\ell}{k}\ell^{jk} \equiv 0 \pmod{\ell^{j+2}}$ for all $2 \leq k \leq \ell$; this uses that $\binom{\ell}{k} \equiv 0 \pmod{\ell}$ when $2 \leq k < \ell$ (we have also used $j \geq 2$ when $\ell = 2$). Since $(I + \ell^j B)^\ell \in H_{j+1}$, this proves that B modulo ℓ lies in $\mathfrak{h}_{j+1}$ and hence $\mathfrak{g}_\ell \subsetneq \mathfrak{h}_{j+1}$. Therefore, $\mathfrak{g}_\ell \subsetneq \mathfrak{h}_i$ for all sufficiently large i. By (4.2), this implies that $|H(\ell^i)| \gg_{A,\ell} \ell^{i(\dim \mathfrak{g}_\ell + 1)} = \ell^{i(\dim G_{A,\ell} + 1)}$ for all $i \geq 1$. However, we have $|H(\ell^i)| \ll_{A,\ell} \ell^{i \dim G_{A,\ell}}$, see Théorème 8 of [Ser81]. These inequalities contradict for i large enough, so we conclude that $\mathfrak{g}_\ell = \mathfrak{h}_j$ for $j \geq 1$ with $(j, \ell) \neq (1, 2)$. $\square$

Lemma 4.4. *We have* $|\rho_{A,\ell^i}(\mathrm{Gal}_K)| \asymp_A \ell^{i \dim \mathfrak{g}_\ell} = \ell^{i \dim G_{A,\ell}}$.

Proof. Define the group $H = \mathcal{G}(\mathbb{Z}_\ell)$. By Lemma 4.3(ii) and (4.2), we have $|H(\ell^i)| \asymp_A |H(\ell)| \cdot \ell^{(i-1)\dim \mathfrak{g}_\ell}$. Since $\mathcal{G}$ is a smooth group scheme, we have $H(\ell) = \mathcal{G}(\mathbb{F}_\ell)$ by Hensel's lemma. By Proposition 2.13 (with $W = 0$), we have $|H(\ell)| = |\mathcal{G}(\mathbb{F}_\ell)| \asymp_A \ell^{\dim \mathcal{G}_{\mathbb{F}_\ell}}$. We have equalities $\dim \mathfrak{g}_\ell = \dim \mathcal{G}_{\mathbb{F}_\ell} = \dim \mathcal{G}_{\mathbb{Q}_\ell} = \dim G_{A,\ell}$, where we have used the smoothness of $\mathcal{G}$ along with Lemma 4.2. Combining everything together, we find that $|H(\ell^i)| \asymp_A \ell^{i \dim \mathfrak{g}_\ell} = \ell^{i \dim G_{A,\ell}}$.

The image of $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ modulo ℓ^i is the group $\rho_{A,\ell^i}(\mathrm{Gal}_K)$. Therefore,

$$[H(\ell^i) : \rho_{A,\ell^i}(\mathrm{Gal}_K)] \leq [H : \rho_{A,\ell^\infty}(\mathrm{Gal}_K)] \ll_A 1,$$

where the last inequality uses Theorem 2.8. So $|\rho_{A,\ell^i}(\mathrm{Gal}_K)| \asymp_A |H(\ell^i)|$ and the lemma follows from the estimates of $|H(\ell^i)|$ we have computed above. $\square$

4.2. **Proof of Theorem 4.1.** There is no harm in replacing K by a finite extension and A with its base extension by this field. Indeed, suppose that K'/K is a finite extension. For a finite extension L/K, set $L' = L \cdot K'$. We have $|A(L)_{\mathrm{tors}}| \leq |A(L')_{\mathrm{tors}}|$ and

$$[L' : K']^{\gamma_{A,\ell}} \leq [K' : K]^{\gamma_{A,\ell}}[L : K]^{\gamma_{A,\ell}} \leq [K' : K]^{2\dim A}[L : K]^{\gamma_{A,\ell}} \ll_{A,K'} [L : K]^{\gamma_{A,\ell}}.$$

Also $\gamma_{A,\ell} = \gamma_{A_{K'},\ell}$. So Theorem 4.1 for $A_{K'}/K'$ implies the theorem for A/K. So after first replacing K by a finite extension, we may assume by Proposition 2.3 that the algebraic groups $G_{A,\ell}$ are connected for the rest of the section. By taking $\ell \gg_A 1$, we may assume by Proposition 2.5 that the $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell} \subseteq \mathrm{GL}_{T_\ell(A)}$ is reductive and that ℓ is odd.

We now make some identifications that will hold for the rest of the proof. By choosing a basis for $T_\ell(A)$ as a $\mathbb{Z}_\ell$-module, we will identify $\mathcal{G}_{A,\ell}$ with an algebraic subgroup of $\mathrm{GL}_{2g,\mathbb{Z}_\ell}$. In particular, we have $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell} \subseteq \mathrm{GL}_{2g,\mathbb{F}_\ell}$. Define $\mathfrak{g} := \mathfrak{g}_\ell \subseteq M_{2g}(\mathbb{F}_\ell)$ as in §4.1.

Take any finite extension L/K in $\overline{K}$. Define the group $U := A(L)[\ell^\infty]$, i.e., the group of torsion points in $A(L)$ whose order is a power of ℓ. The group U is finite by the Mordell–Weil theorem. For each $i \geq 0$, let $U[\ell^i]$ be the group of $P \in U$ for which $\ell^i P = 0$. For each $i \geq 0$, let

$$\psi_i : A[\ell^{i+1}] \xrightarrow{\sim} (\mathbb{Z}/\ell^{i+1}\mathbb{Z})^{2g}$$

be the isomorphism obtained by our choice of $\mathbb{Z}_\ell$-basis for $T_\ell(A)$. Composing ψ_i with the reduction modulo ℓ map induces an isomorphism $\overline{\psi}_i : A[\ell^{i+1}]/A[\ell^i] \xrightarrow{\sim} \mathbb{F}_\ell^{2g}$. We can identify $U[\ell^{i+1}]/U[\ell^i]$ with a subgroup of $A[\ell^{i+1}]/A[\ell^i]$, so we can define

$$W_i := \overline{\psi}_i(U[\ell^{i+1}]/U[\ell^i]);$$

it is a subspace of $\mathbb{F}_\ell^{2g}$.

Lemma 4.5. *For each $i \geq 1$, we have $|\rho_{A,\ell^i}(\mathrm{Gal}_L)| \ll_A \ell^{\sum_{j=0}^{i-1} \dim \mathfrak{g}_{W_j}}$.*

Proof. Define the group $H := \rho_{A,\ell^\infty}(\mathrm{Gal}_L)$. For each $i \geq 1$, define $H(\ell^i)$, H_i and $\mathfrak{h}_i$ as in §4.1.

We claim that $\mathfrak{h}_i \subseteq \mathfrak{g}_{W_i}$ for all $i \geq 1$. Take any $I + \ell^i B \in H_i$. Since $\mathfrak{h}_i \subseteq \mathfrak{g}$ by Lemma 4.3(i), to prove the claim, we need only show that $Bw = 0$ for all $w \in W_i$. Choose an element $\sigma \in \mathrm{Gal}_L$ for which $\rho_{A,\ell^\infty}(\sigma) = I + \ell^i B$. We have $\sigma(P) = P$ for all $P \in U[\ell^{i+1}]$ since $U \subseteq A(L)$. Therefore, $I + \ell^i B$ fixes each element of $\psi_i(U[\ell^{i+1}])$. So for each $w \in \psi_i(U[\ell^{i+1}])$, we have $(I + \ell^i B)w = w$ and hence $\ell^i Bw = 0$. Therefore, $Bw \equiv 0 \pmod{\ell}$ for all $w \in \psi_i(U[\ell^{i+1}])$. The claim is now immediate since W_i is the image of $\psi_i(U[\ell^{i+1}])$ modulo ℓ.

Take any $i \geq 1$. By (4.2) and the above claim, we have
$$|\rho_{A,\ell^i}(\mathrm{Gal}_L)| = |H(\ell^i)| \ll_A |H(\ell)| \cdot \ell^{\sum_{j=1}^{i-1} \dim \mathfrak{g}_{W_j}}.$$
The group Gal_L fixes $U[\ell] \subseteq A(L)$, so $H(\ell)$ fixes each element of W_0. Therefore, $H(\ell) \subseteq G_{W_0}(\mathbb{F}_\ell)$, where $G := \mathcal{G}_{\mathbb{F}_\ell}$. By Proposition 2.13, we have $|H(\ell)| \leq |G_{W_0}(\mathbb{F}_\ell)| \ll_A \ell^{\dim G_{W_0}}$. Therefore,
$$|\rho_{A,\ell^i}(\mathrm{Gal}_L)| \ll_A \ell^{\dim G_{W_0}} \cdot \ell^{\sum_{j=1}^{i-1} \dim \mathfrak{g}_{W_j}}.$$
Since G has Lie algebra $\mathfrak{g}$ by Lemma 4.2, G_{W_0} will have Lie algebra $\mathfrak{g}_{W_0}$ and hence $\dim G_{W_0} \leq \dim \mathfrak{g}_{W_0}$. Therefore, $|\rho_{A,\ell^i}(\mathrm{Gal}_L)| \ll_A \ell^{\sum_{j=0}^{i-1} \dim \mathfrak{g}_{W_j}}$. $\square$

Take any $i \geq 1$ large enough so that $W_j = 0$ for all $j \geq i$. By Lemmas 4.4 and 4.5, we have
$$[L : K] \geq [\rho_{A,\ell^i}(\mathrm{Gal}_K) : \rho_{A,\ell^i}(\mathrm{Gal}_L)] \gg_A \ell^{\sum_{j=0}^{i-1}(\dim \mathfrak{g} - \dim \mathfrak{g}_{W_j})}.$$
With notation as in §3.1, we have
$$[L : K] \gg_A \ell^{\sum_{j=0}^{i-1} \alpha(\mathfrak{g}) \dim W_j} = \left(\prod_{j=0}^{i-1} |W_j| \right)^{\alpha(\mathfrak{g})} = |U|^{\alpha(\mathfrak{g})}.$$
We have $\alpha(\mathfrak{g}) = \alpha((\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}) = \alpha(G_{A,\ell}) = \gamma_{A,\ell}^{-1}$ for ℓ large enough by Proposition 3.10. The numerator and denominator of $\gamma_{A,\ell}$ can be bounded in terms of the dimension of A, so we have $|A(L)[\ell^\infty]| = |U| \ll_A [L : K]^{\gamma_{A,\ell}}$ for $\ell \gg_A 1$.

5. Prime power version: small primes

In this section, we prove the following version of Theorem 4.1, valid for all primes ℓ.

Theorem 5.1. *For every nonzero abelian variety A of dimension g over a number field K and every prime ℓ, we have*
$$|A(L)[\ell^\infty]| \ll_{A,\ell} [L : K]^{\gamma_{A,\ell}}$$
for all finite extensions L/K.

Since Theorem 4.1 has an implicit constant depending only on A for all sufficiently large primes ℓ, the constant can actually be taken to be independent of ℓ by Theorem 5.1. In fact, the two results are complementary: the proof of Theorem 4.1 relies on remarking that, for ℓ sufficiently large, we only need to consider a finite family of pointwise stabilizers, which are all smooth (again, when ℓ is large), as we see in the proof of Lemma 3.10. On the other hand, for small ℓ the group schemes $\mathcal{G}_{A,\ell}$ can lack several desirable properties (including smoothness or reductivity), which explains why we need to adopt a more general point of view. In fact, as can be seen for example from Proposition 5.7, the proof of Theorem 5.1 has little to do with ℓ-adic monodromy groups and more with general linear group schemes over $\mathbb{Z}_\ell$. We remark that the question of smoothness (or flatness) for stabilizers in reductive group schemes is a current topic of research: see for example [Cot22], where – even under strong assumptions on the fibrewise dimensions of centralizers – the proofs are quite delicate.

Finally, we note that the proof of Theorem 5.1 that we give below can be made uniform in ℓ (at the cost of more technical statements): this can be achieved easily by assuming the Mumford–Tate conjecture, and also unconditionally, with some more work, by relying on the finiteness statement given by Proposition 2.10.

5.1. **Grassmannians and stabilizers.** In order to prove Theorem 5.1 we need to control the behaviour of the subgroups of $\mathcal{G}_{A,\ell}$ that arise as pointwise stabilizers of certain (saturated) submodules $\mathcal{W}$ of $T_\ell A$. As it turns out, the questions we are interested in are more easily studied in families, by letting $\mathcal{W}$ vary among all saturated submodules of a given rank. This can be achieved by considering a suitable universal stabilizer group scheme over the Grassmannian. We now introduce the necessary definitions, starting with the Grassmannian itself; for its basic properties, we refer the reader to [GW20, Section 8.4].

Definition 5.2 (Grassmannian)**.** Let n be a positive integer and fix $d \in \{1, \ldots, n\}$. The Grassmannian of d-dimensional submodules in n-dimensional space, denoted by $\mathrm{Grass}_{d,n}$, is the scheme which represents the contravariant functor in schemes
$$S \mapsto \{\mathcal{O}_S\text{-submodule } \mathcal{U} \subseteq \mathcal{O}_S^n \mid \mathcal{O}_S^n/\mathcal{U} \text{ is a locally free } \mathcal{O}_S\text{-module of rank } n - d\}.$$

Remark 5.3. The scheme $\mathrm{Grass}_{d,n}$ has a finite open covering by schemes isomorphic to $\mathbb{A}^{d(n-d)}$, see [GW20, Corollary 8.15]. Moreover, for every PID R, $\mathrm{Grass}_{d,n}(R)$ is the set of saturated free submodules of R^n of rank d.

We can now define the desired stabilizer scheme over the Grassmannian:

Proposition 5.4. *The functor on algebras*
$$R \mapsto \{(\varphi, \mathcal{W}) \in \mathrm{GL}_n(R) \times \mathrm{Grass}_{d,n}(R) \mid \varphi_{|\mathcal{W}} \text{ is the identity on } \mathcal{W}\}$$
is represented by a subscheme of $\mathrm{GL}_n \times \mathrm{Grass}_{d,n}$.

Proof. Consider the canonical open covering of $\mathrm{Grass}_{d,n}$ by copies of $\mathbb{A}^{d(n-d)}$ given in [GW20, Corollary 8.15]. On each such affine piece, the condition that φ be the identity on $\mathcal{W}$ amounts to a finite number of equations involving the generators of $\mathcal{W}$, which in turn may be expressed in terms of the coordinates of $\mathbb{A}^{d(n-d)}$. These equations glue to give the desired subscheme. $\square$

Definition 5.5. We denote by Fix the scheme representing the functor of Proposition 5.4. Explicitly, Fix is a subgroup scheme of $\mathrm{GL}_{n,\mathrm{Grass}_{d,n}}$ with the following property: for every ring R and every $\mathcal{W} \in \mathrm{Grass}_{d,n}(R)$, the pullback group scheme of Fix by $\mathcal{W} : \mathrm{Spec}\, R \to \mathrm{Grass}_{d,n}$, denoted by $\mathrm{Fix}(\mathcal{W})$, satisfies
$$\mathrm{Fix}(\mathcal{W})(R) = \{\varphi \in \mathrm{GL}_n(R) \mid \varphi_{|\mathcal{W}} \text{ is the identity on } \mathcal{W}\}.$$

Finally, we introduce the following definition for arbitrary linear algebraic groups:

Definition 5.6. Let R_0 be a ring and let $\mathcal{G}$ be a linear algebraic subgroup of GL_{n,R_0}. We denote by $\mathrm{Fix}_\mathcal{G}$ the subgroup scheme of $\mathcal{G}_{\mathrm{Grass}_{d,n,R_0}}$ given by the (scheme-theoretic) intersection of $\mathcal{G}_{\mathrm{Grass}_{d,n,R_0}}$ with Fix_{R_0} inside $\mathrm{GL}_{n,\mathrm{Grass}_{d,n,R_0}}$.

By definition, for every R_0-algebra R and every submodule $\mathcal{W}$ of R^n such that $R^n/\mathcal{W}$ is locally free of rank $n - d$ we have
$$\mathrm{Fix}_\mathcal{G}(\mathcal{W})(R) = \{\varphi \in \mathcal{G}(R) \mid \varphi_{|\mathcal{W}} \text{ is the identity on } \mathcal{W}\}.$$

We thus recover the definition given in §1.1. As already pointed out in that section, when $R_0 = k$ is a field, G is an algebraic subgroup of $\mathrm{GL}_{n,k}$ and W is a subspace of k^n, the group $\mathrm{Fix}_G(W)$ is simply the group G_W. When R is a PID, the condition on $\mathcal{W}$ amounts to saying that $\mathcal{W}$ is a saturated submodule of R^n.

Our main objective in this section is to understand the lack of smoothness of groups of the form $\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})$. Notice that, even when $\mathcal{G}$ is smooth, $\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})$ can easily fail to be smooth (the problem usually being its lack of flatness).

5.2. **Reduction to point-counting on group schemes.** We will deduce Theorem 5.1 from the group-theoretic statement below, whose proof will occupy the rest of the section.

In order to ease the notation, for any scheme X over $\mathbb{Z}_\ell$ we write $X(\ell^i) := X(\mathbb{Z}/\ell^i\mathbb{Z})$. We also write $\pi_i : X(\mathbb{Z}_\ell) \to X(\ell^i)$ and $\pi_{j,i} : X(\ell^j) \to X(\ell^i)$ for the natural reduction maps modulo ℓ^i, for any $0 \le i \le j$. Notice that $X(\ell^i)$ does not have the same meaning here as in §4.

Proposition 5.7. *Let $\mathcal{G} \subseteq \mathrm{GL}_{n,\mathbb{Z}_\ell}$ be a linear group scheme such that $G = \mathcal{G}_{\mathbb{Q}_\ell}$ has finite slope. Then, there is a positive constant $C(\mathcal{G})$ such that for every $m \ge 1$ and every subgroup $H \subseteq (\mathbb{Z}/\ell^m\mathbb{Z})^n = \mathbb{A}^n(\ell^m)$ we have*

$$[\mathcal{G}(\mathbb{Z}_\ell) : \mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H)] \ge \frac{1}{C(\mathcal{G})}|H|^{1/\gamma_G},$$

where

$$\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H) := \{M \in \mathcal{G}(\mathbb{Z}_\ell) \,|\, \pi_m(M) \text{ is the identity on } H\}.$$

Remark 5.8.

(i) It would be better to state the result only in terms of $\mathbb{Z}/\ell^m\mathbb{Z}$-points, but this is not always possible when $\mathcal{G}$ is not smooth, as the proof will make clear, hence this somewhat inelegant inequality. In the smooth case, $\pi_m : \mathcal{G}(\mathbb{Z}_\ell) \to \mathcal{G}(\ell^m)$ is surjective, hence it is enough to prove that

$$[\mathcal{G}(\ell^m) : \{M \in \mathcal{G}(\ell^m) \,|\, M \text{ is the identity on } H\}] \ge \frac{1}{C(\mathcal{G})}|H|^{1/\gamma_G}.$$

(ii) The subgroup "fix" does not have a scheme-theoretic interpretation in itself, as H is not always a direct factor of $(\mathbb{Z}/\ell^m\mathbb{Z})^n$. We will see that when H is a direct factor, it does relate to the definition of Fix as above, and in fact the proof works by reduction to this case.

We begin by showing that Proposition 5.7 implies Theorem 5.1.

Proof of Proposition 5.7 $\Rightarrow$ Theorem 5.1. Up to replacing K by a finite extension we can and do assume that $\mathcal{G}_{A,\ell}$ is connected for all primes ℓ. Let L/K be a finite extension and let ℓ be a prime number. Define $H := A(L)[\ell^\infty]$. By the Mordell-Weil theorem, there is an integer $m \ge 1$ such that $H \subseteq A(L)[\ell^m]$. Every $\sigma \in \mathrm{Gal}(\overline{K}/L)$ fixes H pointwise, and hence

$$\rho_{A,\ell^\infty}(\mathrm{Gal}(\overline{K}/L)) \subseteq \mathrm{fix}_{\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)}(H).$$

We apply Proposition 5.7 to $\mathcal{G}_{A,\ell}$ and obtain the inequality

$$[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \mathrm{fix}_{\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)}(H)] \gg_{A,\ell} |H|^{1/\gamma_{A,\ell}}.$$

Therefore, $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell^\infty}(\mathrm{Gal}(\overline{K}/L))] \gg_{A,\ell} |H|^{1/\gamma_{A,\ell}}$. Since $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ is a finite-index subgroup of $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$ with index bounded independent of ℓ by Theorem 2.8, we have

$$[L : K] \ge [\rho_{A,\ell^\infty}(\mathrm{Gal}_K) : \rho_{A,\ell^\infty}(\mathrm{Gal}(\overline{K}/L))] \gg_{A,\ell} [\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell^\infty}(\mathrm{Gal}(\overline{K}/L))] \gg_{A,\ell} |H|^{1/\gamma_{A,\ell}}.$$

Raising both sides to the power $\gamma_{A,\ell}$ gives $|A(L)[\ell^\infty]| = |H| \ll_{A,\ell} [L : K]^{\gamma_{A,\ell}}$. $\square$

Even though Proposition 5.7 is not explicitly formulated in terms of $\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})$, we now show that it may be deduced from sufficiently strong estimates on the number of $\mathbb{Z}/\ell^n\mathbb{Z}$-points of groups of the form $\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})$. The precise result we need is Proposition 5.9 below. To state it, we introduce

a notion of partial slope. Let V be an n-dimensional vector space over a field k and let G be an algebraic subgroup of GL_V. For every $r = 1, \ldots, n$ we define

$$(5.1) \qquad d_r(G) := \max_{\substack{W \subseteq V \\ \dim \overline{W} = r}} \dim \mathrm{Fix}_G(W).$$

If G is of finite slope, we have

$$(5.2) \qquad \dim G - d_r(G) \geq r/\gamma_G.$$

The key auxiliary result is the following.

Proposition 5.9 (Key estimate). *Let ℓ be a prime number, M a free $\mathbb{Z}_\ell$-module of rank n and $\mathcal{G} \subseteq \mathrm{GL}_M$ a linear group scheme whose generic fiber G has finite slope. There exists a constant $C(\mathcal{G})$ such that for every $r = 1, \ldots, n$, every saturated $\mathbb{Z}_\ell$-submodule $\mathcal{W} \subseteq M$ of rank r and all integers $m \geq m' \geq 0$ we have*

$$(5.3) \qquad \left| \ker \left(\pi_{m,m'} : \mathrm{Fix}_{\mathcal{G}}(\mathcal{W})(\ell^m) \to \mathrm{Fix}_{\mathcal{G}}(\mathcal{W})(\ell^{m'}) \right) \right| \leq C(\mathcal{G}) \ell^{d_r(G)(m-m')}.$$

Remark 5.10. Such a result is easy to establish if we replace $C(\mathcal{G})$ by something possibly depending on $\mathcal{G}$ and $\mathcal{W}$, as $d_r(G)$ is found to be an upper bound for the dimension of the generic fiber of $\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})$. The main difficulty is to give bounds that are uniform in $\mathcal{W}$. Furthermore, if $\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})$ is known to be smooth of relative dimension d, the left-hand side of (5.3) becomes exactly $\ell^{d(m-m')}$ (for $m' \geq 1$), so we see that all the complications come from not being able to make this assumption.

Before diving into the technical lemmas required to prove this Proposition, let us first see how it implies Proposition 5.7 (in short: by dévissage).

Proof of Proposition 5.9 $\Rightarrow$ Proposition 5.7. We take the notation of Proposition 5.7. Consider a subgroup H of $(\mathbb{Z}/\ell^m\mathbb{Z})^n$. There exists a basis $(e_1, \ldots, e_n)$ of $\mathbb{Z}_\ell^n$ and integers $m \geq m_1 \geq \ldots \geq m_r$ with $1 \leq r \leq n$ such that

$$H = \bigoplus_{i=1}^{r} \langle \ell^{m-m_i} \pi_m(e_i) \rangle \subseteq (\mathbb{Z}/\ell^m\mathbb{Z})^n.$$

In particular, notice that

$$(5.4) \qquad |H| = \prod_{i=1}^{r} \ell^{m_i}.$$

We define, for every $j = 1, \ldots, r$,

$$\mathcal{W}_j := \bigoplus_{i=1}^{j} \mathbb{Z}_\ell e_i \quad \text{and} \quad \mathcal{G}_j := \mathrm{Fix}_{\mathcal{G}_{\mathbb{Z}_\ell}}(\mathcal{W}_j).$$

For every $M \in \mathcal{G}(\mathbb{Z}_\ell)$,

$$\pi_m(M) \text{ fixes } H \iff \pi_m(M) \text{ fixes } \ell^{m-m_i}\pi_m(e_i) \text{ for all } 1 \leq i \leq r$$
$$\iff \pi_{m_i}(M) \in \mathcal{G}_i(\ell^{m_i}) \text{ for all } 1 \leq i \leq r$$

as the $\mathcal{W}_j$ form a strictly increasing sequence of saturated submodules of $\mathbb{Z}_\ell^n$. Consequently,

$$\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H) = \bigcap_{i=1}^{r} \pi_{m_i}^{-1}(\mathcal{G}_i(\ell^{m_i})).$$

As $m \geq m_1 \geq m_2 \geq \ldots \geq m_r$, the index we want to bound from below is

$$(5.5) \qquad [\mathcal{G}(\mathbb{Z}_\ell) : \mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H)] \geq [\pi_{m_1}(\mathcal{G}(\mathbb{Z}_\ell)) : \pi_{m_1}(\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H))] = \frac{|\pi_{m_1}(\mathcal{G}(\mathbb{Z}_\ell))|}{|\pi_{m_1}(\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H'))|},$$

where we have identified $H \subseteq (\ell^{m-m_1}\mathbb{Z}/\ell^m\mathbb{Z})^n$ to a subgroup $H' \subseteq (\mathbb{Z}/\ell^{m_1}\mathbb{Z})^n \cong (\ell^{m-m_1}\mathbb{Z}/\ell^m\mathbb{Z})^n$. We can now assume $m = m_1$ and $H = H'$, since the right-hand side does not depend on m anymore. We now bound the ratio $|\pi_{m_1}(\mathcal{G}(\mathbb{Z}_\ell))|/|\pi_{m_1}(\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H))|$.

For the numerator, we have a (non-effective) lower bound of the form $C_1(\mathcal{G})\ell^{m\dim G}$ with $C_1(\mathcal{G}) > 0$, see Lemma 5.16 and the comments following it. For the denominator, we have

$$\left|\pi_m(\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H))\right| \leq |\{M \in \mathcal{G}(\ell^m) : M \text{ fixes } H\}| \leq \left|\bigcap_{i=1}^{r} \pi_{m,m_i}^{-1}(\mathcal{G}_i(\ell^{m_i}))\right|.$$

To bound this cardinality we proceed as follows. To obtain an element of this intersection, first we choose a matrix $M_r \in \mathcal{G}_r(\ell^{m_r})$, then we choose a lift M_{r-1} of M_r in $\mathcal{G}_{r-1}(\ell^{m_{r-1}})$, and notice that two different lifts are multiplicatively related by a matrix of $\mathcal{G}_{r-1}(\ell^{m_{r-1}})$ whose reduction modulo m_r is the identity (in particular, there are at most $|\ker \mathcal{G}_{r-1}(\ell^{m_{r-1}}) \to \mathcal{G}_{r-1}(\ell^{m_r})|$ such lifts). The same holds until we have lifted back to $\mathcal{G}(\ell^m)$. Setting by convention $m_{r+1} = 0$, we thus have

$$\left|\bigcap_{i=1}^{r} \pi_{m,m_i}^{-1}(\mathcal{G}_i(\ell^{m_i}))\right| \leq \prod_{i=1}^{r} |\ker(\mathcal{G}_i(\ell^{m_i}) \to \mathcal{G}_i(\ell^{m_{i+1}}))|.$$

Using Proposition 5.9 for every $\mathcal{G}_i$ we then get

$$
\begin{aligned}
\frac{|\pi_{m_1}(\mathcal{G}(\mathbb{Z}_\ell))|}{|\pi_{m_1}(\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H))|} &\geq \frac{C_1(\mathcal{G})\ell^{m\dim G}}{C(\mathcal{G})^r \prod_{i=1}^{r} \ell^{(m_i-m_{i+1})d_i(G)}} \\
&\geq \frac{C_1(\mathcal{G})}{C(\mathcal{G})^r} \prod_{i=1}^{r} \ell^{(m_i-m_{i+1})(\dim G - d_i(G))} \\
&\geq \frac{C_1(\mathcal{G})}{C(\mathcal{G})^r} \prod_{i=1}^{r} \ell^{(m_i-m_{i+1})i/\gamma_G} \\
&= \frac{C_1(\mathcal{G})}{C(\mathcal{G})^r} \left(\ell^{\sum_{i=1}^{r} m_i}\right)^{1/\gamma_G} \\
&= \frac{C_1(\mathcal{G})}{C(\mathcal{G})^r} |H|^{1/\gamma_G}.
\end{aligned}
$$

Here we used the equality $m = m_1 = \sum_{i=1}^{r}(m_i - m_{i+1})$ in the second line, Inequality (5.2) in the third line, and Equation (5.4) in the last line. Combined with (5.5), this implies the proposition. $\square$

Remark 5.11. The last sequence of inequalities is the counterpart in the present setting of Lemma 4.5.

5.3. Uniformizing the behaviour of the pointwise stabilizers.
Although the group schemes $\mathrm{Fix}_\mathcal{G}(\mathcal{W})$ that appear in Proposition 5.9 are not a priori smooth, the use of the pointwise stabilizer scheme on the Grassmannian allows us to obtain the following "uniform" statement, which suffices to prove Proposition 5.9 when combined with the counting lemmas in the next section.

Proposition 5.12. *Let ℓ be a prime number, let M be a free $\mathbb{Z}_\ell$-module of rank n, and let $\mathcal{G} \subseteq \mathrm{GL}_M$ be a linear group scheme whose generic fiber G has finite slope. Denote by $\varepsilon : \mathrm{Spec}\,\mathbb{Z}_\ell \to \mathcal{G}$ the unit section. For every $r = 1,\ldots,n$ there is an integer $e_r \geq 0$ such that for all saturated submodules $\mathcal{W} \subseteq M$ of rank r, the $\mathbb{Z}_\ell$-module $\ell^{e_r} \cdot \varepsilon^*\Omega^1_{\mathrm{Fix}_\mathcal{G}(\mathcal{W})/\mathbb{Z}_\ell}$ can be generated by a set of cardinality at most $d_r(G)$. Equivalently, for $N = \ell^{e_r} \cdot \varepsilon^*\Omega^1_{\mathrm{Fix}_\mathcal{G}(\mathcal{W})/\mathbb{Z}_\ell}$, we have $\dim_{\mathbb{F}_\ell} N/\ell N \leq d_r(G)$.*

Remark 5.13. For any $W \subseteq M \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ of dimension r, by definition of d_r the group scheme $\mathrm{Fix}_G(W)$ has dimension at most $d_r(G)$, and being an affine algebraic group in characteristic 0 it is smooth by Cartier's theorem. It follows that $\varepsilon^*\Omega^1_{\mathrm{Fix}_G(W)/\mathbb{Q}_\ell}$ is a vector space of dimension at most $d_r(G)$.

The difficulty lies in extending this statement to $\mathbb{Z}_\ell$, up to allowing multiplication by a nonzero element ℓ^{e_r}.

Proof. As explained in Section 5.1, for every $r = 1, \dots, n$, we can view $\mathrm{Fix}_{\mathcal{G}}$ as a subgroup scheme of $\mathcal{G}_{\mathrm{Grass}_{r,n,\mathbb{Z}_\ell}}$, with unit section again denoted by ε. We now define the sheaf

$$\mathcal{F} := \bigwedge^{d_r(G)+1} \varepsilon^* \Omega^1_{\mathrm{Fix}_{\mathcal{G}} \,/\, \mathrm{Grass}_{r,n,\mathbb{Z}_\ell}}.$$

It is a coherent sheaf over $\mathrm{Grass}_{r,n,\mathbb{Z}_\ell}$, and for every $x \in \mathrm{Grass}_{r,n}(\mathbb{Z}_\ell)$, corresponding to a saturated submodule $\mathcal{W}$ of M of rank r, compatibility of pullbacks and exterior powers with base change gives

$$\bigwedge^{d_r(G)+1} \varepsilon^* \Omega^1_{\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})/\mathbb{Z}_\ell} = x^* \mathcal{F}.$$

In particular, for the $\mathbb{Q}_\ell$-points $x \in \mathrm{Grass}_{r,n}(\mathbb{Q}_\ell)$, by definition of $d_r(G)$ we have $x^* \mathcal{F} \cong \mathcal{F}_x = 0$ (see Remark 5.13). By Corollary 5.15 below, there exists an integer $e_r \geq 0$ such that $\ell^{e_r} \cdot x^* \mathcal{F} = 0$ for all $x \in \mathrm{Grass}_{r,n,\mathbb{Z}_\ell}(\mathbb{Z}_\ell)$. This finally gives

$$\bigwedge^{d_r(G)+1} (\ell^{e_r} \varepsilon^* \Omega^1_{\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})/\mathbb{Z}_\ell}) = \ell^{e_r(d_r(G)+1)} x^* \mathcal{F} = 0,$$

which proves that $\ell^{e_r} \cdot \varepsilon^* \Omega^1_{\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})/\mathbb{Z}_\ell}$ is generated by a set of cardinality at most $d_r(G)$. $\qquad\square$

It remains to show that, as claimed in the previous proof, we can find an integer e_r such that $\ell^{e_r} \cdot x^* \mathcal{F} = 0$ for all $\mathbb{Z}_\ell$-sections x. This is achieved in the next lemma and corollary.

Lemma 5.14. *Let $\mathcal{F}$ be a coherent sheaf over $\mathbb{A}^d_{\mathbb{Z}_\ell}$. If $x^* \mathcal{F} \cong \mathcal{F}_x$ vanishes at every $\mathbb{Q}_\ell$-point x of $\mathbb{A}^d_{\mathbb{Z}_\ell}$, there exists an integer $e \geq 0$ such that $\ell^e \cdot y^* \mathcal{F} = 0$ for every $\mathbb{Z}_\ell$-point y of $\mathbb{A}^d_{\mathbb{Z}_\ell}$.*

Proof. Write $\mathbb{A}^d_{\mathbb{Z}_\ell} = \mathrm{Spec}\, A$, where $A = \mathbb{Z}_\ell[t_1, \dots, t_d]$, and let M be the A-module corresponding to $\mathcal{F}$. As $\mathcal{F}$ is coherent, M is the cokernel of a certain A-linear map $A^m \to A^k$, so that we can write $M = A^k/RA^m$ for a suitable matrix $R \in \mathrm{M}_{k \times m}(A)$. The condition $\mathcal{F}_x = 0$ for $x \in \mathbb{A}^d_{\mathbb{Z}_\ell}(\mathbb{Q}_\ell) = \mathbb{Q}^d_\ell$ translates to the following. A $\mathbb{Q}_\ell$-point x can be identified with a d-tuple $(x_1, \dots, x_d) \in \mathbb{Q}^d_\ell$. For such a point, denote by $R(x)$ the evaluation of R (which is a matrix of polynomials in the variables $t_1, \dots, t_d$) at $(t_1, \dots, t_d) = (x_1, \dots, x_d)$. Note that $R(x)$ is a $k \times m$ matrix with coefficients in $\mathbb{Q}_\ell$. The stalk of M at x is then $\mathbb{Q}^k_\ell/R(x)\mathbb{Q}^m_\ell$, so it vanishes if and only if $\mathrm{rk}\, R(x) = k$. This is equivalent to the fact that at least one $k \times k$ minor of $R(x)$ is nonzero, and by assumption this holds for all $x \in \mathbb{A}^d_\ell(\mathbb{Q}_\ell)$.

Let I be the set of all $k \times k$ submatrices of R. For each $i \in I$, let $r_i(t_1, \dots, t_d) \in A$ be the minor of R indexed by i. As we already argued, for every $x = (x_1, \dots, x_d) \in \mathbb{Q}^d_\ell$, at least one of the $r_i(t_1, \dots, t_d)$ is nonvanishing at x, so that the function $f(x) := \min_{i \in I} v_\ell(r_i(x))$ is everywhere finite on $\mathbb{Z}^d_\ell$. The function $f(x)$ is also trivially continuous, so $f(\mathbb{Z}^d_\ell) \subseteq \mathbb{Z}$ is compact, and hence bounded. In particular, there exists an integer $e \geq 0$ such that, for each $y \in \mathbb{Z}^d_\ell$, there exists $i \in I$ for which $v_\ell(r_i(y)) \leq e$. This implies that the $\mathbb{Z}_\ell$-span of the columns of the sub-matrix of $R(y)$ indexed by i contains $(\ell^e \mathbb{Z}_\ell)^k$, hence, a fortiori, the same holds for the $\mathbb{Z}_\ell$-span of all the columns of $R(y)$, and we have shown that this holds for all y. Thus, $\mathbb{Z}^k_\ell/R(y)\mathbb{Z}^m_\ell$ is killed by ℓ^e for all $y \in \mathbb{Z}^d_\ell = \mathbb{A}^d_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell)$. As $\mathbb{Z}^k_\ell/R(y)\mathbb{Z}^m_\ell \cong y^* \mathcal{F}$, the claim follows. $\qquad\square$

Corollary 5.15. *Let $\mathcal{F}$ be a coherent sheaf over $\mathrm{Grass}_{r,n,\mathbb{Z}_\ell}$. Suppose that, for each $\mathbb{Q}_\ell$-point $x \in \mathrm{Grass}_{r,n,\mathbb{Z}_\ell}(\mathbb{Q}_\ell)$, we have $x^* \mathcal{F} \cong \mathcal{F}_x = 0$. Then, there exists an integer $e \geq 0$ such that $\ell^e \cdot x^* \mathcal{F} = 0$ for every $x \in \mathrm{Grass}_{r,n,\mathbb{Z}_\ell}(\mathbb{Z}_\ell)$.*

24

Proof. The scheme $\mathrm{Grass}_{r,n,\mathbb{Z}_\ell}$ is a finite union of affine spaces over $\mathbb{Z}_\ell$, see Remark 5.3. For each such affine space S, Lemma 5.14 gives an integer e_S for which $\ell^{e_S} \cdot x^*\mathcal{F} = 0$ for all $\mathbb{Z}_\ell$-points x of S. The corollary follows by taking $e = \max\{e_S\}$. $\qquad\square$

5.4. Counting lemmas.
First, for the lower bound on the numerator of (5.5), we used the following result.

Lemma 5.16. *For any affine subvariety $\mathcal{X} \subseteq \mathbb{A}^N_{\mathbb{Z}_\ell}$ such that $\mathcal{X}(\mathbb{Z}_\ell)$ is a nonempty open subset of $\mathcal{X}(\mathbb{Q}_\ell)$ and $\mathcal{X}_{\mathbb{Q}_\ell}$ is equidimensional of dimension d, there is a positive constant $C(\mathcal{X})$ such that for all $m \geq 1$,*

$$|\pi_m(\mathcal{X}(\mathbb{Z}_\ell))| \geq C(\mathcal{X})\ell^{dm}.$$

Proof. Considering $\mathcal{X}(\mathbb{Z}_\ell)$ as a closed analytic subvariety of dimension d of $\mathbb{Z}_\ell^N$, we can apply [Oes82, Théorème 2]. Note that the set X_m of [Oes82] is exactly our $\pi_m(\mathcal{X}(\mathbb{Z}_\ell))$, and that we use the fact that $\pi_m(\mathcal{X}(\mathbb{Z}_\ell))$ contains at least one element. The measure $\mu_d(\mathcal{X}(\mathbb{Z}_\ell))$ is nonzero because $\mathcal{X}(\mathbb{Z}_\ell)$ is of dimension d. $\qquad\square$

Any group scheme $\mathcal{G} \subseteq \mathrm{GL}_{n,\mathbb{Z}_\ell}$ satisfies the hypotheses of Lemma 5.16 (embedding GL_n in the affine space $\mathbb{A}^{n^2+1}$) because $\mathcal{G}(\mathbb{Z}_\ell) \neq \emptyset$ is open in $\mathcal{G}(\mathbb{Q}_\ell)$ and $\mathcal{G}_{\mathbb{Q}_\ell}$ is equidimensional.

Our next lemma is an ad hoc version of the implicit function theorem for schemes over $\mathbb{Z}_\ell$:

Lemma 5.17. *Let ℓ be a prime number, $0 \leq d \leq n$ and let $A_{d+1}, \ldots, A_n$ be elements of the ring $\mathbb{Z}_\ell[X_1, \ldots, X_n]$ such that for every $d+1 \leq i \leq n$, we have $A_i - X_i \in \ell\mathbb{Z}_\ell[X_1, \ldots, X_n]$. Denote by S' the scheme $\mathrm{Spec}\,\mathbb{Z}_\ell[X_1, \ldots, X_n]/\langle A_{d+1}, \ldots, A_n\rangle$ and by $p\colon S' \to \mathbb{A}^d_{\mathbb{Z}_\ell}$ the projection given by the first d coordinates.*

For all integers $m \geq 1$, the base-change of p to $\mathbb{Z}/\ell^m\mathbb{Z}$ is an isomorphism, hence induces a bijection $p\colon S'(\mathbb{Z}/\ell^m\mathbb{Z}) \to \mathbb{A}^d(\mathbb{Z}/\ell^m\mathbb{Z})$ on $\mathbb{Z}/\ell^m\mathbb{Z}$-points. Consequently, for all integers $m \geq m' \geq 1$, the cardinality of any fiber of the natural map

$$\pi_{m,m'}\colon S'(\ell^m) \to S'(\ell^{m'})$$

is $\ell^{d(m-m')}$, and $\pi_{m'}\colon S'(\mathbb{Z}_\ell) \to S'(\ell^{m'})$ is surjective for all $m' \geq 1$.

Proof. Define $B = \mathbb{Z}/\ell^m\mathbb{Z}[X_1, \ldots, X_d]$ and $C = B[X_{d+1}, \ldots, X_n]/\langle A_{d+1}, \ldots, A_n\rangle$. So $\mathbb{A}^n_{\mathbb{Z}/\ell^m\mathbb{Z}} = \mathrm{Spec}\,B$ and $S'_{\mathbb{Z}/\ell^m\mathbb{Z}} = \mathrm{Spec}\,C$, and $p_{\mathbb{Z}/\ell^m\mathbb{Z}}$ is induced by the natural homomorphism $B \to C$. The hypothesis $A_i - X_i \in \ell\mathbb{Z}_\ell[X_1, \ldots, X_n]$ implies that the determinant of the Jacobian matrix $\left(\frac{\partial A_i}{\partial X_i}\right)_{i,j=d+1,\ldots,n}$ reduces to 1 modulo ℓ. Since every element of C congruent to 1 modulo ℓ is a unit in C, [Mil80, Corollary 3.16], or equivalently [Stacks, Lemma 02GU], yields that the map $\mathrm{Spec}(C) \to \mathrm{Spec}(B)$ is étale. Furthermore, it is of degree 1, because this can be tested after tensoring with $\mathbb{F}_\ell$, and the given extension $B \hookrightarrow C$ induces an isomorphism $B \otimes \mathbb{F}_\ell \cong C \otimes \mathbb{F}_\ell$ since $A_i \bmod \ell = X_i$ for all $i = d+1, \ldots, n$. As an étale map of degree 1 is an isomorphism, this concludes the proof of the first statement in the lemma. The other statements follow immediately from the properties of $\mathbb{A}^d$. $\qquad\square$

Before stating and proving our main counting lemma we need one more fact that links the cardinality of the fibers of certain reduction maps with suitable derivations:

Lemma 5.18. *Let R be a ring, $X = \mathrm{Spec}\,A$ be an R-scheme and $\varepsilon : A \to R$ be a section. Let I be an ideal of R and m, m' be positive integers with $m' < m \leq 2m'$. Let $\pi_{m'} : R \to R/I^{m'}$ be the canonical projection. The set of points of $X(R/I^m)$ above $\pi_{m'} \circ \varepsilon$ is in bijection with $\mathrm{Hom}_R(\Omega^1_{A/R} \otimes_\varepsilon R, I^{m'}/I^m)$.*

Proof. We write ε_m for $\pi_m \circ \varepsilon$ and similarly for $\varepsilon_{m'}$, and denote by $\pi_{m,m'}$ the canonical map $R/I^m \to R/I^{m'}$. A point of $X(R/I^m)$ above $\varepsilon_{m'}$ is a homomorphism of R-algebras $\varphi : A \to R/I^m$ such that $\pi_{m,m'} \circ \varphi = \varepsilon_{m'}$. Consider the morphism of R-modules

$$\theta := \varphi - \varepsilon_m : A \to I^{m'}/I^m.$$

As φ is a ring morphism, for all $a, b \in A$ we have

$$\begin{aligned}
\theta(ab) &= \varphi(ab) - \varepsilon_m(ab) \\
&= \varphi(a)\varphi(b) - \varepsilon_m(a)\varepsilon_m(b) \\
&= (\theta(a) + \varepsilon_m(a))(\theta(b) + \varepsilon_m(b)) - \varepsilon_m(a)\varepsilon_m(b) \\
&= \varepsilon_m(a)\theta(b) + \varepsilon_m(b)\theta(a),
\end{aligned}$$

because $\theta(a)\theta(b)$ belongs to $I^{2m'}/I^m$, so it is 0 in R/I^m by the assumption $2m' \geq m$. In other words, θ is an A-linear derivation (with the A-module structure on $I^{m'}/I^m$ given by ε_m). Conversely, the same computation shows that every A-linear derivation $\theta : A \to I^{m'}/I^m$ provides a point $\varphi \in X(R/I^m)$ above ε_m. By the defining property of the Kähler differentials we have an isomorphism

$$\operatorname{Der}_A(A, I^{m'}/I^m) \cong \operatorname{Hom}_A(\Omega^1_{A/R}, I^{m'}/I^m),$$

but this latter space is isomorphic to

$$\operatorname{Hom}_R(\Omega^1_{A/R} \otimes_\varepsilon R, I^{m'}/I^m),$$

as can be checked directly because $I^{m'}/I^m$ inherits its A-module structure from ε. $\qquad\square$

Lemma 5.19 (Main counting lemma). *Let ℓ be a prime number, S be a closed subscheme of $\mathbb{A}^n_{\mathbb{Z}_\ell}$, and $\varepsilon : \operatorname{Spec}\mathbb{Z}_\ell \to S$ be a section of the structure morphism. For positive integers $m \geq m'$, denote by $\pi_{m'} : S(\mathbb{Z}_\ell) \to S(\mathbb{Z}/\ell^{m'}\mathbb{Z})$ and $\pi_{m,m'} : S(\mathbb{Z}/\ell^m\mathbb{Z}) \to S(\mathbb{Z}/\ell^{m'}\mathbb{Z})$ the canonical reduction maps modulo $\ell^{m'}$, as in the beginning of §5.2. Assume that, for some non-negative integers d and e, the $\mathbb{Z}_\ell$-module $\ell^e \varepsilon^* \Omega^1_{S/\mathbb{Z}_\ell}$ is generated by a set of cardinality at most d.*

(i) *For all integers $m \geq m' > e$,*

$$\left| \pi^{-1}_{m,m'}(\pi_{m'}(\varepsilon)) \right| \leq \ell^{n(e+1)} \ell^{d(m-m')}.$$

(ii) *If $e = 0$ and $0 < m' \leq m \leq 2m'$, then*

$$\left| \pi^{-1}_{m,m'}(\pi_{m'}(\varepsilon)) \right| \leq \ell^{d(m-m')}.$$

Proof. Let $I \subseteq \mathbb{Z}_\ell[X_1, \ldots, X_n]$ be the ideal defining the subscheme S of $\mathbb{A}^n_{\mathbb{Z}_\ell}$.

(i) Assume first that $m > m' + e + 1$. To begin with, ε is a point of $S(\mathbb{Z}_\ell) \subseteq \mathbb{A}^n_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell)$, hence corresponds to a ring morphism $\mathbb{Z}_\ell[X_1, \ldots, X_n] \to \mathbb{Z}_\ell$. Up to translating the subscheme S, one can assume that ε corresponds to the evaluation of all the X_i at 0. In the following, for a polynomial $P \in \mathbb{Z}_\ell[X_1, \ldots, X_n]$, we write $\mathrm{d}P$ for its differential at 0, i.e.

$$\mathrm{d}P = \sum_{i=1}^n \frac{\partial P}{\partial X_i}(0, \ldots, 0)\, \mathrm{d}X_i.$$

If I is generated by polynomials $P_1, \ldots, P_r$, by the fundamental exact sequences of the Kähler differentials we have

$$M := \varepsilon^* \Omega^1_{S/\mathbb{Z}_\ell} \cong \left(\bigoplus_{i=1}^n \mathbb{Z}_\ell \mathrm{d}X_i \right) / \langle \mathrm{d}P_j,\, 1 \leq j \leq r \rangle.$$

26

By the Smith normal form over the DVR $\mathbb{Z}_\ell$, up to a $\mathbb{Z}_\ell$-linear change of variables we can choose $X_1, \ldots, X_n$ in such a way that

$$\langle \mathrm{d}P_1, \ldots, \mathrm{d}P_r \rangle = \bigoplus_{i=1}^n \ell^{e_i} \mathbb{Z}_\ell \, \mathrm{d}X_i$$

for suitable $e_1 \geq \ldots \geq e_n$ (with $e_i \in \mathbb{N} \cup \{+\infty\}$, where we set $\ell^{+\infty} = 0$ by convention). With this choice of coordinates we have

$$M = \bigoplus_{i=1}^n \frac{\mathbb{Z}_\ell}{\ell^{e_i} \mathbb{Z}_\ell} \, \mathrm{d}X_i.$$

As the e_i are decreasing and $\dim_{\mathbb{F}_\ell} \ell^e M / \ell^{e+1} M \leq d$, we have $e \geq e_i$ for $i = d+1, \ldots, n$. Choose polynomials $Q_1, \ldots, Q_n$ in I such that $\mathrm{d}Q_i = \ell^{\max(e_i, e)} \, \mathrm{d}X_i$ for all $i \in \{1, \ldots, n\}$. Recall that ε corresponds to the ring morphism $\mathbb{Z}_\ell[X_1, \ldots, X_n] \to \mathbb{Z}_\ell$ evaluating a polynomial at $(0, \ldots, 0)$. As ε is a $\mathbb{Z}_\ell$-point of $S = \operatorname{Spec} \mathbb{Z}_\ell[X_1, \ldots, X_n]/I$, the kernel of ε must contain I, so every element of I vanishes at $0 = (0, \ldots, 0)$. Thus $Q_i(0) = 0$ and we have $Q_i = \ell^e X_i + R_i$ with R_i a sum of homogeneous polynomials of degree ≥ 2. For every $i \in \{d+1, \ldots, n\}$ we now consider the polynomial

$$\widetilde{Q}_i := \frac{1}{\ell^{2e+1}} Q_i(\ell^{e+1} X_1, \ldots, \ell^{e+1} X_n) \in \mathbb{Z}_\ell[X_1, \ldots, X_n].$$

Writing $Q_i = \ell^e X_i + R_i$ as above, one obtains that $\widetilde{Q}_i$ is of the form

$$\widetilde{Q}_i = X_i + \ell \widetilde{R}_i(X_1, \ldots, X_n), \quad \widetilde{R}_i \in \mathbb{Z}_\ell[X_1, \ldots, X_n].$$

We apply Lemma 5.17 with $A_i = \widetilde{Q}_i$ for every $i \in \{d+1, \ldots, n\}$. In particular, we let S' denote the $\mathbb{Z}_\ell$-scheme defined in $\mathbb{A}_{\mathbb{Z}_\ell}^n$ by the ideal $\langle \widetilde{Q}_{d+1}, \ldots, \widetilde{Q}_n \rangle$.

Let $x = (x_1, \ldots, x_n) \in S(\ell^m) \subseteq \mathbb{A}_{\mathbb{Z}_\ell}^n(\ell^m) = (\mathbb{Z}/\ell^m \mathbb{Z})^n$ be a point which is zero modulo $\ell^{m'}$. Since $m' > e$ by assumption, we can write $x = \ell^{e+1} y$ for some $y \in (\ell^{m'-e-1} \mathbb{Z}/\ell^m \mathbb{Z})^n$, so that for every $i > d$ we have

$$0 \equiv Q_i(x) \equiv Q_i(\ell^{e+1} y) \equiv \ell^{2e+1} \widetilde{Q}_i(y) \pmod{\ell^m}.$$

This implies that $\widetilde{Q}_i(y) \in \ell^{m-2e-1} \mathbb{Z}/\ell^m \mathbb{Z}$ for all $i = d+1, \ldots, n$. Thus, $y' := \pi_{m, m-2e-1}(y) \in (\mathbb{Z}/\ell^{m-2e-1} \mathbb{Z})^n$ gives a point in $S'(\mathbb{Z}/\ell^{m-2e-1}\mathbb{Z})$ which is zero modulo $\ell^{m'-e-1}$. By Lemma 5.17, the cardinality of any fibre of the map

$$\pi'_{m-2e-1, m'-e} : S'(\ell^{m-2e-1}) \to S'(\ell^{m'-e})$$

is $\ell^{d(m-m'-e-1)}$; note that the lemma applies, since $m' - e$ is strictly positive. The image $y'' = \pi'_{m-2e-1, m'-e}(y')$ of y' in $S'(\ell^{m'-e})$ is in particular a point of $\mathbb{A}^n(\ell^{m'-e})$ which is zero modulo $\ell^{m'-e-1}$, so there are at most ℓ^n possibilities for y''. The point y' lies in the fibre of $\pi'_{m-2e-1, m'-e}$ over y'', so for each y'' there are at most $\ell^{d(m-m'-e-1)}$ such y', hence at most $\ell^n \ell^{d(m-m'-e-1)}$ possibilities for y' in total. Finally, given any such $y' \in (\mathbb{Z}/\ell^{m-2e-1} \mathbb{Z})^n$, there are $\ell^{n(2e+1)}$ possible lifts $y \in (\mathbb{Z}/\ell^m \mathbb{Z})^n$ of y'. Since $x = \ell^{e+1} y$, the value of x is determined by $y \bmod \ell^{m-e-1}$, so for each y' there are at most ℓ^{en} possibilities for x. This gives

$$\left| \pi_{m, m'}^{-1}(\varepsilon \bmod m') \right| \leq \ell^{n(e+1)} \ell^{d(m-m'-e-1)},$$

a slightly better bound than claimed in the statement. Finally, for the case $m \leq m' + e + 1$, we simply consider the embedding of S into $\mathbb{A}_{\mathbb{Z}_\ell}^n$. Via this embedding, a point in $S(\ell^m)$ that reduces to $\varepsilon \bmod m'$ in $S(\ell^{m'})$ is in particular a point of $\mathbb{A}^n(\ell^m)$ that reduces to $(0, \ldots, 0)$ in $\mathbb{A}^n(\ell^{m'})$. It is clear that there are at most $\ell^{n(m-m')}$ such points, and $\ell^{n(m-m')} \leq \ell^{(e+1)n}$, which proves the bound in this case.

27

(ii) This is a consequence of Lemma 5.18. Indeed, we have $e = 0$ by assumption, so we know that $\varepsilon^*\Omega^1_{S/\mathbb{Z}_\ell}$ is generated by at most d elements over $\mathbb{Z}_\ell$, and therefore the cardinality of $\mathrm{Hom}_{\mathbb{Z}_\ell}(\varepsilon^*\Omega^1_{S/\mathbb{Z}_\ell}, \ell^{m'}\mathbb{Z}/\ell^m\mathbb{Z})$ is at most $\ell^{d(m-m')}$. $\qquad\square$

We can now establish the following for group schemes over $\mathbb{Z}_\ell$:

Proposition 5.20. *Let ℓ be a prime number, M be a free $\mathbb{Z}_\ell$-module of finite rank n, and $\mathcal{G}$ be a linear subgroup scheme of GL_M with unit section $\varepsilon \in \mathcal{G}(\mathbb{Z}_\ell)$. Suppose that $e, d \in \mathbb{N}$ are such that $\ell^e\varepsilon^*\Omega^1_{\mathcal{G}/\mathbb{Z}_\ell}$ is generated by at most d elements as a $\mathbb{Z}_\ell$-module, with $d \leq n^2$. There is a constant $C(n, d, e, \ell)$ such that for all integers $m \geq m' > 0$ the following holds:*

$$\left|\ker\left(\pi_{m,m'} : \mathcal{G}(\ell^m) \to \mathcal{G}(\ell^{m'})\right)\right| \leq C(n, d, e, \ell)\ell^{d(m-m')}.$$

Moreover, if $e = 0$ (e.g., if $\mathcal{G}$ is smooth), the result holds with $C(n, d, 0, \ell) = 1$.

Proof. Lemma 5.19 directly implies the result for $m \geq m' > e$. In the general case, we use that given two group homomorphisms $f : G_1 \to G_2$ and $g : G_2 \to G_3$ between finite groups we have $|\ker(g \circ f)| \leq |\ker(g)| \cdot |\ker(f)|$. Hence, if $m > e \geq m'$ we have

$$\begin{aligned}
\left|\ker \pi_{m,m'}\right| &\leq \left|\ker \pi_{m,e+1}\right| \cdot \left|\ker \pi_{e+1,m'}\right| \leq C(n, d, e, \ell)\ell^{d(m-e-1)}\ell^{(e+1-m')n^2} \\
&\leq \left(C(n, d, e, \ell)\ell^{(e+1)n^2}\right)\ell^{d(m-m')},
\end{aligned}$$

where we have used the trivial bound

$$\left|\ker \pi_{e+1,m'}\right| \leq \left|\{M \in \mathrm{M}_n(\mathbb{Z}/\ell^{e+1}\mathbb{Z}) : M \equiv I_n \pmod{\ell^{m'}}\}\right| = \ell^{n^2(e+1-m')}$$

and the fact that $d \leq n^2$. Finally, if $m \leq e$, we similarly bound $|\mathcal{G}(\ell^m)|$ by ℓ^{en^2}, which is enough for our purposes.

In the case $e = 0$, the result follows by induction from part (ii) of Lemma 5.19. $\qquad\square$

5.5. Conclusion of the proof of Proposition 5.9.

Let ε be the unit section of $\mathcal{G}$. By Proposition 5.12, there exists an integer $e_r \geq 0$ such that, for every saturated submodule $\mathcal{W}$ of M of rank r, the $\mathbb{Z}_\ell$-module $\ell^{e_r}\varepsilon^*\Omega^1_{\mathcal{G}_{\mathcal{W}}/\mathbb{Z}_\ell}$ is generated by at most $d_r(G) \leq \dim G \leq \dim \mathrm{GL}_n = n^2$ elements. For $m' \geq 1$, Proposition 5.20 immediately implies the desired inequality with constant given by $C(n, d_r(G), e_r, \ell)$. For $m' = 0$ we then have

$$\begin{aligned}
|\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})(\ell^m)| &\leq |\ker(\pi_{m,1} : \mathrm{Fix}_{\mathcal{G}}(\mathcal{W})(\ell^m) \to \mathrm{Fix}_{\mathcal{G}}(\mathcal{W})(\ell))| \cdot |\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})(\ell)| \\
&\leq C(n, d_r(G), e_r, \ell)\ell^{d_r(G)(m-1)} \cdot |\mathcal{G}(\ell)| \\
&\leq C(n, d_r(G), e_r, \ell)\ell^{n^2-d_r(G)} \cdot \ell^{d_r(G)m}.
\end{aligned}$$

6. An expression for β_A

Fix a nonzero abelian variety A over a number field K. Recall that β_A is the infimum of all real numbers β for which there is a constant C, depending only on A and β, such that the inequality $|A(L)_{\mathrm{tors}}| \leq C \cdot [L : K]^\beta$ holds for all finite extensions L/K.

Lemma 6.1. *For any finite extension K'/K, we have $\beta_{A_{K'}} = \beta_A$.*

Proof. The inequality $\beta_{A_{K'}} \leq \beta_A$ is trivial by considering extensions L of K' as extensions of K. We now prove the opposite inequality. For a finite extension L/K, set $L' = L \cdot K'$. For any $\varepsilon > 0$, we have

$$|A(L)_{\mathrm{tors}}| \leq |A(L')_{\mathrm{tors}}| \ll_{A,K'} [L' : K']^{\beta_{A_{K'}}+\varepsilon} \leq [K' : K]^{\beta_{A_{K'}}+\varepsilon}[L : K]^{\beta_{A_{K'}}+\varepsilon} \ll_{A,\varepsilon,K'} [L : K]^{\beta_{A_{K'}}+\varepsilon}.$$

Therefore, $\beta_A \leq \beta_{A_{K'}}$ by the minimality in the definition of β_A. □

The following describes β_A in terms of the ℓ-adic monodromy groups of $G_{A,\ell}$.

Theorem 6.2. *We have*
$$\beta_A = \max_\ell \gamma_{A,\ell},$$
where the maximum is over all primes ℓ.

Proof. Define $\xi_A := \max_\ell \gamma_{A,\ell}$; the maximum exists since the numerators and denominators of the $\gamma_{A,\ell}$ are bounded. From Lemma 6.1, β_A is unchanged if we replace A by a base extension by a finite extension of K. The value ξ_A is also unchanged if we replace A by such a base extension. So by Proposition 2.9, we may assume that the representations $\{\rho_{A,\ell^\infty}\}_\ell$ are independent. We may also assume that the groups $G_{A,\ell}$ are connected by Proposition 2.3.

We first prove $\beta_A \leq \xi_A$. Take any finite extension L/K and let J be the set of primes that divide $|A(L)_{\text{tors}}|$. For each $\ell \in J$, define the field $L_\ell := K(A(L)[\ell^\infty])$. By the independence of the representations ρ_{A,ℓ^∞}, we have $\prod_{\ell \in J}[L_\ell : K] \leq [L : K]$. By Theorems 4.1 and 5.1, there is a constant $C > 0$ depending only on A such that
$$|A(L)[\ell^\infty]| = |A(L_\ell)[\ell^\infty]| \leq C \cdot [L_\ell : K]^{\gamma_{A,\ell}} \leq C \cdot [L_\ell : K]^{\xi_A}$$
for all $\ell \in J$. Taking the product over all $\ell \in J$, we find that

(6.1)
$$|A(L)_{\text{tors}}| = \prod_{\ell \in J} |A(L)[\ell^\infty]| \leq C^{|J|} \Big(\prod_{\ell \in J}[L_\ell : K]\Big)^{\xi_A} \leq C^{|J|}[L : K]^{\xi_A}.$$

Take any $\varepsilon > 0$ and set $\delta := 1 - 1/(1 + \varepsilon/\xi_A)$; we have $0 < \delta < 1$. We have
$$C^{|J|} = \prod_{\ell \in J} C \ll_{A,\varepsilon} \prod_{\ell \in J} \ell^\delta \leq |A(L)_{\text{tors}}|^\delta,$$
where the first inequality uses that $C \leq \ell^\delta$ for all primes $\ell \gg_{A,\varepsilon} 1$. Using (6.1), this implies that $|A(L)_{\text{tors}}| \ll_{A,\varepsilon} |A(L)_{\text{tors}}|^\delta \cdot [L : K]^{\xi_A}$. Therefore,
$$|A(L)_{\text{tors}}| \ll_{A,\varepsilon} [L : K]^{\xi_A/(1-\delta)} = [L : K]^{\xi_A + \varepsilon},$$
where the equality uses our choice of δ. Since L/K and $\varepsilon > 0$ were arbitrary, this implies that $\beta_A \leq \xi_A$.

We now prove $\xi_A \leq \beta_A$. Fix a prime ℓ with $\gamma_{A,\ell} = \xi_A$ and set $G := G_{A,\ell}$. There is a nonzero subspace $W \subseteq V_\ell(A)$ such that $\gamma_{A,\ell} \cdot (\dim G - \dim G_W) = \dim W$. By choosing a $\mathbb{Z}_\ell$-basis of $T_\ell(A)$, we can view $\mathcal{G}_{A,\ell}$ as a subgroup of $\mathrm{GL}_{2g,\mathbb{Z}_\ell}$ and W as a subspace of $\mathbb{Q}_\ell^{2g}$. Define the groups $\mathcal{H}_0 := G(\mathbb{Q}_\ell) \cap \mathrm{GL}_{2g}(\mathbb{Z}_\ell) = \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$ and $\mathcal{H} := G_W(\mathbb{Q}_\ell) \cap \mathrm{GL}_{2g}(\mathbb{Z}_\ell) \subseteq \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$.

Take any integer $i \geq 1$. By Théorème 9 of [Ser81], we have $|\mathcal{H}_0(\ell^i)| \asymp_{A,\ell} \ell^{i \dim G}$ and $|\mathcal{H}(\ell^i)| \asymp_{A,W,\ell} \ell^{i \dim G_W}$ with notation as in §4.1. Let L_i be the subfield of $\overline{K}$ fixed by the $\sigma \in \mathrm{Gal}_K$ for which $\rho_{A,\ell^i}(\sigma)$ lies in $\mathcal{H}(\ell^i)$. Using Theorem 2.8, we find that $[L_i : K] \asymp_{A,W,\ell} \ell^{i(\dim G - \dim G_W)} = \ell^{i \dim W \cdot \gamma_{A,\ell}^{-1}}$.

Define $\mathcal{W} := W \cap \mathbb{Z}_\ell^{2g}$. The $\mathbb{Z}_\ell$-module $\mathcal{W}$ has rank equal to the dimension of W. The group $\mathcal{W}/\ell^i\mathcal{W} \subseteq (\mathbb{Z}/\ell^i\mathbb{Z})^{2g}$ is fixed by $\mathcal{H}(\ell^i)$. Therefore, $A(L_i)$ has a subgroup of order $|\mathcal{W}/\ell^i\mathcal{W}| = \ell^{i \dim W}$.

Take any $\varepsilon > 0$. By the definition of β_A, we have $|A(L_i)_{\text{tors}}| \ll_{A,\varepsilon} [L_i : K]^{\beta_A + \varepsilon}$ and hence
$$\ell^{i \dim W} \ll_{A,\varepsilon} [L_i : K]^{\beta_A + \varepsilon} \ll_{A,W,\ell} \ell^{i \dim W \cdot \gamma_{A,\ell}^{-1} \cdot (\beta_A + \varepsilon)}.$$

Since this holds for all $i \geq 1$, we must have $\gamma_{A,\ell}^{-1} \cdot (\beta_A + \varepsilon) \geq 1$. Since $\varepsilon > 0$ was arbitrary, we have $\beta_A \geq \gamma_{A,\ell} = \xi_A$. □

6.1. **Proof of Theorem 1.1.** Since we are assuming the Mumford–Tate conjecture for A, the theorem follows from Theorem 6.2 and Lemma 3.9(ii).

6.2. **Proof of Theorem 1.3.** We have $\operatorname{End}(V)^{G_A} \cong \operatorname{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ by Lemma 2.1(ii). Since A is geometrically simple, the ring $\operatorname{End}(V)^{G_A}$ is a division algebra. Therefore, V is an irreducible representation of G_A and hence $\gamma_A = 2 \dim A / \dim G_A$. By Theorem 6.2 and Lemma 3.9(i), we have inequalities

$$\beta_A \geq \max_{\ell} \frac{2 \dim A}{\dim G_{A,\ell}^{\circ}} \geq \gamma_A = \frac{2 \dim A}{\dim G_A}.$$

Suppose that $\beta_A = \gamma_A$. By the above inequalities, we must have $\dim G_{A,\ell}^{\circ} = \dim G_A$ for some prime ℓ. By Proposition 2.7(i) and the equality of dimensions, we deduce that $G_{A,\ell}^{\circ} = (G_A)_{\mathbb{Q}_\ell}$. The Mumford–Tate conjecture for A then follows from Proposition 2.7(ii).

The other implication follows directly from Theorem 1.1.

6.3. **Proof of Theorem 1.4.** Theorem 1.1 shows that (a) implies (b). We trivially have that (b) implies (c). So it remains to show that (c) implies (a).

Assume that (c) holds and let A be a nonzero abelian variety defined over a number field K. Due to the invariance of the Mumford–Tate conjecture under finite extensions of the ground field and under isogeny, enlarging K if needed, we may assume that A is isomorphic over K to a product $B_1^{n_1} \times \cdots \times B_r^{n_r}$, where each B_i is defined over K and is geometrically simple. By assumption, the equality $\beta_{B_i} = \gamma_{B_i}$ holds for each $i = 1, \ldots, r$, hence by Theorem 1.3 the Mumford–Tate conjecture holds for each B_i. By [Com19], this implies that the Mumford–Tate conjecture holds for $A = B_1^{n_1} \times \ldots \times B_r^{n_r}$.

7. SOME REMARKS ON A VERSION WITHOUT MUMFORD–TATE GROUPS

Let A be a nonzero abelian variety defined over a number field K. In this section, we will formulate a conjectural expression for β_A that does not involve the Mumford–Tate group. By Lemma 6.1, we may assume (after extending the number field and replacing by an isogenous abelian variety) that A is of the form $\prod_{i=1}^n A_i^{m_i}$ such that the abelian varieties A_i/K are geometrically simple, pairwise geometrically nonisogenous, and have all their endomorphisms defined over K. For each subset $I \subseteq \{1, \ldots, n\}$, define the abelian variety $A_I := \prod_{i \in I} A_i^{m_i}$ over K. For each prime ℓ, let $\gamma_{A,\ell}$ be the constant defined in §4.

Conjecture 7.1. *For each prime ℓ, we have*

$$\gamma_{A,\ell} = \max_{\emptyset \neq I \subseteq \{1, \ldots, n\}} \frac{2 \dim A_I}{\dim G_{A_I,\ell}}.$$

Note that both sides in Conjecture 7.1 equal γ_A when the Mumford–Tate conjecture for A holds; this uses Lemma 3.9.

Theorem 7.2. *If Conjecture 7.1 holds for A, then*

$$\beta_A = \max_{\substack{\ell \ prime \\ \emptyset \neq I \subseteq \{1, \ldots, n\}}} \frac{2 \dim A_I}{\dim G_{A_I,\ell}}$$

Proof. This is an immediate consequence of Theorem 6.2 and Conjecture 7.1 for A. $\qquad\square$

Proposition 7.3. *Fix a prime ℓ. Suppose there is an algebraic subgroup $H \subseteq G_A$ such that $H_{\mathbb{Q}_\ell}$ and $G_{A,\ell}^{\circ}$ are conjugate in $(G_A)_{\mathbb{Q}_\ell}$. Then Conjecture 7.1 holds for the prime ℓ.*

Proof. By Proposition 2.7(i), we have $G_{A,\ell}^\circ \subseteq (G_A)_{\mathbb{Q}_\ell}$ and hence our assumption that $H_{\mathbb{Q}_\ell}$ and $G_{A,\ell}^\circ$ are conjugate in $(G_A)_{\mathbb{Q}_\ell}$ makes sense. Therefore, $\alpha(G_{A,\ell}^\circ) = \alpha(H_{\mathbb{Q}_\ell}) = \alpha(H)$, where the last equality uses Proposition 3.5(iii).

With notation as in §2.1, the isotypic decomposition of V as a representation of G_A is given by $V = \bigoplus_{i=1}^n V_i$, see Lemma 2.2. For a nonempty subset $I \subseteq \{1, \ldots, n\}$, define $V_I := \bigoplus_{i \in I} V_i$. For any nonempty subset $I \subseteq \{1, \ldots, n\}$, we find that $(H_{V_I})_{\mathbb{Q}_\ell} = (H_{\mathbb{Q}_\ell})_{V_I \otimes_{\mathbb{Q}} \mathbb{Q}_\ell}$ is conjugate in $(G_A)_{\mathbb{Q}_\ell}$ to $(G_{A,\ell}^\circ)_{V_I \otimes_{\mathbb{Q}} \mathbb{Q}_\ell} = (G_{A,\ell}^\circ)_{V_\ell(A_I)}$. So

$$\frac{\dim H - \dim H_{V_I}}{\dim V_I} = \frac{\dim G_{A,\ell}^\circ - \dim (G_{A,\ell}^\circ)_{V_\ell(A_I)}}{\dim V_\ell(A_I)} = \frac{\dim G_{A_I,\ell}^\circ}{2 \dim A_I},$$

where the last equality uses that the kernel of the projection $G_{A,\ell} \to G_{A_I,\ell}$ is $(G_{A,\ell})_{V_\ell(A_I)}$. In particular,

$$(7.1) \qquad \min_{\emptyset \neq I \subseteq \{1, \ldots, n\}} \frac{\dim H - \dim H_{V_I}}{\dim V_I} = \min_{\emptyset \neq I \subseteq \{1, \ldots, n\}} \frac{\dim G_{A_I,\ell}}{2 \dim A_I}.$$

We claim that $V = \bigoplus_{i=1}^n V_i$ is also the isotypic decomposition of V as a representation of H. If the claim holds, then $\alpha(H) = \min_I \dim G_{A_I,\ell}/(2 \dim A_I)$, where I varies over the nonempty subsets of $\{1, \ldots, n\}$, by Proposition 3.5(ii) and (7.1). Thus the proposition will follow from the claim since $\alpha(H) = \alpha(G_{A,\ell}^\circ) = \gamma_{A,\ell}^{-1}$.

The group H is connected and reductive since $G_{A,\ell}^\circ$ has these properties and $H_{\mathbb{Q}_\ell} \cong G_{A,\ell}^\circ$. Since $V = \bigoplus_{i=1}^n V_i$ is the isotypic decomposition as a representation of G_A and $H \subseteq G_A$, to prove the claim it suffices to show that $\operatorname{End}_{\mathbb{Q}}(V)^{G_A} = \operatorname{End}_{\mathbb{Q}}(V)^H$. We have $\operatorname{End}_{\mathbb{Q}}(V)^{G_A} \subseteq \operatorname{End}_{\mathbb{Q}}(V)^H$ since $H \subseteq G_A$, so it suffices to show that they have the same dimension as $\mathbb{Q}$-vector spaces.

By Lemma 2.1(ii), we have $\operatorname{End}_{\mathbb{Q}}(V)^{G_A} = \operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, where we are using that all the endomorphisms of $A_{\overline{K}}$ are defined over K. By Proposition 2.4(ii) and our assumption that all the endomorphisms of $A_{\overline{K}}$ are defined over K, we have $\operatorname{End}_{\mathbb{Q}_\ell}(V_\ell(A))^{G_{A,\ell}^\circ} = \operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. Therefore,

$$\operatorname{End}_{\mathbb{Q}}(V)^H \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \operatorname{End}_{\mathbb{Q}_\ell}(V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^{H_{\mathbb{Q}_\ell}} \cong \operatorname{End}_{\mathbb{Q}_\ell}(V_\ell(A))^{G_{A,\ell}^\circ} = \operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell.$$

So $\operatorname{End}_{\mathbb{Q}}(V)^{G_A}$ and $\operatorname{End}_{\mathbb{Q}}(V)^H$ both have the same dimension as $\operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ as a $\mathbb{Q}$-vector space and thus are equal. This completes the proof of the claim and the proposition. $\square$

We now prove Conjecture 7.1 for several abelian varieties. In particular, Conjecture 7.1 will hold whenever $\operatorname{End}(A_{\overline{K}}) = \mathbb{Z}$; this includes many cases for which the Mumford–Tate conjecture is unknown.

Proposition 7.4. *Suppose that A is geometrically simple and that the center of the ring $\operatorname{End}(A_{\overline{K}})$ is isomorphic to $\mathbb{Z}$. Then Conjecture 7.1 holds, i.e., $\gamma_{A,\ell} = 2 \dim A/\dim G_{A,\ell}$.*

Proof. Take any prime ℓ. After suitably increasing the field K, we may assume that $\operatorname{End}(A_{\overline{K}}) = \operatorname{End}(A)$ and that the group $G_{A,\ell}$ is connected. The ring $D := \operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra since A is geometrically simple. From our assumption on $\operatorname{End}(A_{\overline{K}})$, we find that the division algebra D has center $\mathbb{Q}$. Therefore, $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is a central simple algebra over $\mathbb{Q}_\ell$.

By Proposition 2.4(ii), the natural map $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to \operatorname{End}_{\mathbb{Q}_\ell[\operatorname{Gal}_K]}(V_\ell(A))$ is an isomorphism of $\mathbb{Q}_\ell$-algebras. Therefore, $\operatorname{End}_{\mathbb{Q}_\ell[\operatorname{Gal}_K]}(V_\ell(A))$ is a central simple algebra over $\mathbb{Q}_\ell$.

Denote by $V_\ell(A) = \bigoplus_{i=1}^n V_i$ the decomposition of the representation $V_\ell(A)$ of $G_{A,\ell}$ into isotypical components. We have $\operatorname{End}_{\mathbb{Q}_\ell[\operatorname{Gal}_K]}(V_\ell(A)) = \prod_{i=1}^n \operatorname{End}_{\mathbb{Q}_\ell[\operatorname{Gal}_K]}(V_i)$. Since $\operatorname{End}_{\mathbb{Q}_\ell[\operatorname{Gal}_K]}(V_\ell(A))$ is a simple $\mathbb{Q}_\ell$-algebra, we deduce that $n = 1$. Since there is only one isotypic component, by Proposition 3.5(ii) we find that

$$\gamma_{A,\ell} = \frac{\dim V_\ell(A)}{\dim G_{A,\ell} - \dim (G_{A,\ell})_{V_\ell(A)}} = \frac{2 \dim A}{\dim G_{A,\ell}}. \qquad \square$$

Remark 7.5. Let us briefly sketch why we are currently unable to extend the proof of Proposition 7.4 to arbitrary A. For simplicity, assume that A is geometrically simple, that $\operatorname{End}(A_{\overline{K}}) = \operatorname{End}(A)$ and that $G_{A,\ell}$ is connected for all ℓ.

Denote the center of $\operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ by E; it is a number field. We have $E_\ell := E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \prod_{\lambda | \ell} E_\lambda$, where λ runs over the places of E that divide ℓ. The natural actions of Gal_K and E_ℓ on $V_\ell(A)$ commute. Therefore, $V_\lambda := V_\ell(A) \otimes_{E_\ell} E_\lambda$ is a $\mathbb{Q}_\ell[\operatorname{Gal}_K]$-module that we can identify with a submodule of $V_\ell(A)$. We have $V_\ell(A) = \bigoplus_{\lambda | \ell} V_\lambda$ and using the work of Faltings, one can show that this is the isotypic decomposition of $V_\ell(A)$ as a representation of $G_{A,\ell}$ and that $G_{A,\ell}$ is reductive. Using Proposition 3.5(ii), we have

$$(7.2) \qquad \gamma_{A,\ell} = \max_{\mathcal{L} \neq \emptyset} \frac{\dim V_{\mathcal{L}}}{\dim G_{A,\ell} - \dim(G_{A,\ell})_{V_{\mathcal{L}}}},$$

where $V_{\mathcal{L}} := \bigoplus_{\lambda \in \mathcal{L}} V_\lambda$ and $\mathcal{L}$ runs over the nonempty sets of places λ of E that divide ℓ. Conjecture 7.1 is equivalent to showing that the maximum in (7.2) is obtained with $\mathcal{L} = \{\lambda : \lambda | \ell\}$; this is obvious in the case of Proposition 7.4 where $E = \mathbb{Q}$.

8. IMPROVEMENTS ON MASSER'S BOUND

Consider a nonzero abelian variety A defined over a number field K. From Masser [Mas], we always have the bound $\beta_A \leq \dim A$. The goal of this section is to prove the following, which describes when Masser's bound can be improved upon.

Theorem 8.1. *We have $\beta_A \leq \dim A$, with equality holding if and only if A is isogenous over $\overline{K}$ to a power of a CM elliptic curve.*

Before beginning the proof, we will need to prove a few lemmas. Fix any prime ℓ. We first give some equivalent conditions for an abelian variety to have complex multiplication.

Lemma 8.2. *Let A be a nonzero abelian variety over K that is isogenous over $\overline{K}$ to a power of a geometrically simple abelian variety. Then the following are equivalent:*

(a) *A has complex multiplication,*
(b) *G_A is a torus,*
(c) *$G_{A,\ell}^{\circ}$ is a torus for some, equivalently for every, prime ℓ,*
(d) *there is a representation $W \subseteq V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ of $(G_{A,\ell}^{\circ})_{\overline{\mathbb{Q}}_\ell}$ of degree 1 for some, equivalently for every, prime ℓ.*

Proof. There is no harm in replacing A by its base change by a finite extension of K. So we may assume that A is isogenous to a power of a geometrically simple abelian variety A_1/K. Observe that if one of the conditions (a)–(d) holds for A, then the corresponding condition also holds for A_1. So without loss of generality, we may assume that A is geometrically simple. After again replacing the field K by a finite extension, we may further assume that $\operatorname{End}(A) = \operatorname{End}(A_{\overline{K}})$ and that $G_{A,\ell}$ is connected. Define $g := \dim A$.

Define $D := \operatorname{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Since A is geometrically simple, D is a division algebra. Denote the center of D by F and define the natural numbers $d := [F : \mathbb{Q}]$ and $e := [D : F]^{1/2}$. With notation as in §2.1, we have $G_A \subseteq \operatorname{GL}_V$. By Lemma 2.1(ii), D agrees with the subalgebra of $\operatorname{End}_{\mathbb{Q}}(V)$ that commutes with G_A. Since D is a division algebra, V is an irreducible representation of the reductive group G_A.

Set $L := \overline{\mathbb{Q}}_\ell$. We have an isomorphism

$$D \otimes_{\mathbb{Q}} L = D \otimes_F (F \otimes_{\mathbb{Q}} L) \cong D \otimes_F (\prod_{\sigma} L) \cong \prod_{\sigma}(D \otimes_{F,\sigma} L) \cong M_e(L)^d$$

32

of L-algebras, where the products are over the d embeddings $F \hookrightarrow L$. In particular, the L-subalgebra of $\operatorname{End}_L(V \otimes_{\mathbb{Q}} L)$ that commutes with $(G_A)_L$ is isomorphic to $M_e(L)^d$. Since $(G_A)_L$ is reductive, we must have an isomorphism

$$(8.1) \qquad V \otimes_{\mathbb{Q}} L \cong U_1^e \oplus \cdots \oplus U_d^e$$

of representations of $(G_A)_L$, where the U_i are irreducible and pairwise nonisomorphic. Since V is an irreducible representation of G_A, the U_i must all have the same dimension over L. In particular, $\dim_L U_i = (\dim V)/(de) = 2g/(de)$.

From Proposition 2.4(ii), we find that the L-subalgebra of $\operatorname{End}_L(V_\ell(A) \otimes_{\mathbb{Q}_\ell} L)$ that commutes with $(G_{A,\ell})_L$ is isomorphic to $D \otimes_{\mathbb{Q}} L \cong M_e(L)^d$. So we have an isomorphism

$$(8.2) \qquad V_\ell(A) \otimes_{\mathbb{Q}_\ell} L \cong W_1^e \oplus \cdots \oplus W_d^e$$

of representations of the reductive group $(G_{A,\ell})_L$, where the W_i are irreducible and pairwise nonisomorphic. Using the comparison isomorphism $V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = V_\ell(A)$ and the inclusion $G_{A,\ell} \subseteq (G_{A,\ell})_{\mathbb{Q}_\ell}$ from Proposition 2.7(i), we conclude that (8.1) and (8.2) give the same decomposition of $V_\ell(A) \otimes_{\mathbb{Q}_\ell} L$ into irreducible representations of $(G_{A,\ell})_L$.

We first show that (a) and (b) are equivalent. First suppose that A has complex multiplication. Since A is geometrically simple, $D = F$ is a number field of degree $2g$. So $e = 1$ and $d = 2g$, and hence each U_i has dimension $(2g)/de = 1$. Since the representation of $(G_A)_L$ on $U_1 \oplus \cdots \oplus U_d$ is faithful and all the U_i have dimension 1, we deduce that $(G_A)_L$, and hence also G_A, is commutative. Therefore, the reductive group G_A must be a torus which completes the proof that (a) implies (b). Now suppose instead that G_A is a torus. Since V is an irreducible representation of the torus G_A and L is algebraically closed, $V \otimes_{\mathbb{Q}} L$ will be a direct sum of irreducible representations of $(G_A)_L$ each having dimension 1 and multiplicity 1. So in this case, we will have $e = 1$ and $\dim U_i = 1$ for all $1 \le i \le d$. So $2g/d = 2g/(de) = \dim U_i = 1$ and hence $d = 2g$. Therefore, $D = F$ is a number field of degree $2g$ and hence A has complex multiplication. This completes the proof that (a) and (b) are equivalent.

That (b) implies (c) for every prime ℓ is a direct consequence of the inclusion $G_{A,\ell} \subseteq (G_A)_{\mathbb{Q}_\ell}$ from Proposition 2.7(i). That (c) for a given (resp. every) prime ℓ implies (d) for the same (resp. every) prime ℓ is immediate since the irreducible representations of a torus over an algebraically closed field all have degree 1.

Finally assume that (d) holds for some prime ℓ. It suffices to show that (b) holds. From our decomposition (8.1) into irreducibles, one of the irreducible summands U_i must be isomorphic to W as a representation of $(G_{A,\ell})_L$. Since all the U_i have the same dimension, we deduce that $\dim U_i = \dim W = 1$ for all $1 \le i \le d$. The group $(G_A)_L$ must be commutative since it acts faithfully on a direct sum of degree 1 representations. Therefore, the reductive group $(G_A)_L$, and hence also G_A, must be a torus. $\qquad\square$

We now describe when the ℓ-adic monodromy group of a nonzero abelian variety has smallest possible dimension.

Lemma 8.3. *Let B be a nonzero abelian variety over K. Then $\dim G_{B,\ell} \ge 2$, with equality holding if and only if B is isogenous over $\overline{K}$ to a power of a CM elliptic curve.*

Proof. After replacing B by its base extension by some finite extension of K, we may assume that the group $G_{B,\ell}$ is connected.

The group $G_{B,\ell}$ is reductive by Proposition 2.5(i), so the quotient $S := G_{B,\ell}/Z(G_{B,\ell})$ is semisimple, where $Z(G_{B,\ell})$ is the center of $G_{B,\ell}$. If $S \neq 1$, then $\dim S \ge 3$ since the smallest dimension of a non-trivial semisimple group is 3 (realised by forms of SL_2 and $\mathrm{SL}_2/\{\pm I\}$). In particular, we have $\dim G_{B,\ell} \ge 3$ whenever $S \neq 1$. So for the rest of the proof, we may assume that $S = 1$;

equivalently, $G_{B,\ell}$ is a torus. By Lemma 8.2, G_B is also a torus and B has complex multiplication. We have $(G_B)_{\mathbb{Q}_\ell} \cong G_{B,\ell}$ by [UY13, Corollary 2.11]. So it suffices to prove that $\dim G_B \geq 2$, with equality holding if and only if B is isogenous over $\overline{K}$ to a power of a CM elliptic curve.

After replacing B by its base change by some finite extension of K, we may assume that B is isogenous to a product $\prod_{i=1}^{n} B_i^{m_i}$, where the B_i are abelian varieties over K that are geometrically simple and pairwise nonisogenous.

Take any $1 \leq i \leq n$. Since B has complex multiplication, B_i has complex multiplication and G_{B_i} is a torus. Since G_{B_i} is a quotient of G_B, we have

$$\dim G_B \geq \dim G_{B_i} \geq 2 + \log_2 \dim(B_i) \geq 2$$

by [Rib80, Equation (3.5)], where the last inequality is an equality only if B_i is an elliptic curve. So $\dim G_B \geq 3$ if at least one of the B_i is not an elliptic curve. We can thus assume that each B_i is a CM elliptic curve.

Suppose that $n \geq 2$. Since $G_{B_1 \times B_2}$ is a quotient of G_B and B_1 and B_2 are nonisogenous CM elliptic curves, we have

$$\dim G_B \geq \dim G_{B_1 \times B_2} = 3$$

by [MZ99, Corollary 3.9]. Finally, in the case $n = 1$, i.e., B is isogenous (over $\overline{K}$) to a power of a CM elliptic curve B_1, we have $\dim G_B = \dim G_{B_1} = 2$. $\qquad\square$

We now consider bounds for $\gamma_{A,\ell}$ when A has complex multiplication. This case is easy to study because we know that the Mumford–Tate conjecture holds.

Lemma 8.4. *Let A be a nonzero abelian variety over K that has complex multiplication. Then $\gamma_{A,\ell} \leq \dim A$, with equality holding if and only if A is isogenous over $\overline{K}$ to a power of a CM elliptic curve.*

Proof. After replacing A by its base change by a finite extension of K, we may assume A is isogenous to a product $\prod_{i=1}^{n} A_i^{m_i}$, where the A_i are abelian varieties over K that are geometrically simple and are pairwise nonisomorphic. By definition we have

$$\gamma_A = \max_{\emptyset \neq I \subseteq \{1,\ldots,n\}} \frac{2 \dim A_I}{\dim G_{A_I}},$$

where $A_I := \prod_{i \in I} A_i^{m_i}$. Since A has complex multiplication, so do all the A_I. Since the Mumford–Tate conjecture holds for all abelian varieties with complex multiplication [Poh68], Lemma 3.9(ii) implies that

$$\gamma_{A,\ell} = \max_{\emptyset \neq I \subseteq \{1,\ldots,n\}} \frac{2 \dim A_I}{\dim G^\circ_{A_I,\ell}}.$$

Take any nonempty $I \subseteq \{1,\ldots,n\}$. By Lemma 8.3, we have

$$2 \dim A_I / \dim G^\circ_{A_I,\ell} \leq (2 \dim A_I)/2 = \dim A_I \leq \dim A,$$

with $2 \dim A_I / \dim G^\circ_{A_I,\ell} = \dim A$ if and only if $I = \{1,\ldots,n\}$ and A_I is isogenous over $\overline{K}$ to a power of a CM elliptic curve. The lemma is now immediate after taking the maximum over all I. $\qquad\square$

We now consider powers of geometrically simple abelian varieties.

Lemma 8.5. *Let A be a nonzero abelian variety over K that over $\overline{K}$ is isomorphic to a power of a simple abelian variety. We have $\gamma_{A,\ell} \leq \dim A$, with equality holding if and only if A is isogenous over $\overline{K}$ to a power of a CM elliptic curve.*

34

Proof. After replacing A by its base change by a finite extension of K, we may assume that the group $G_{A,\ell}$ is connected and that A is isogenous to a power of a geometrically simple abelian variety A_1/K. By Proposition 3.5(ii), we have

$$\gamma_{A,\ell} = \frac{\dim W}{\dim G_{A,\ell} - \dim(G_{A,\ell})_W}$$

for some nonzero $\mathbb{Q}_\ell$-subspace $W \subseteq V_\ell(A)$ that is the direct sum of isotypic components of $V_\ell(A)$ as a representation of $G_{A,\ell}$. Define $\delta := \dim G_{A,\ell} - \dim(G_{A,\ell})_W$. If $\delta \geq 3$, then $\gamma_{A,\ell} = (\dim W)/\delta \leq (2 \dim A)/3 < \dim A$. So it remains to consider the cases where δ is 1 or 2.

Suppose that $\delta = 2$. We have $\gamma_{A,\ell} = (\dim W)/\delta = (\dim W)/2 \leq (2 \dim A)/2 = \dim A$. Now suppose we have an equality $\gamma_{A,\ell} = \dim A$ and hence $\dim W = 2 \dim A$. Therefore, $W = V_\ell(A)$ and we then have $(G_{A,\ell})_W = 1$. So $\dim A = \gamma_{A,\ell} = (2 \dim A)/(\dim G_{A,\ell} - 0)$ and hence $\dim G_{A,\ell} = 2$. By Lemma 8.3, we deduce that A is isogenous over $\overline{K}$ to a power of a CM elliptic curve.

Suppose that $\delta = 1$. We know that $G_{A,\ell}$ contains the group $\mathbb{G}_m$ of homotheties of $V_\ell(A)$. Since $G_{A,\ell}$ is connected and $\delta = 1$, we have $G_{A,\ell} = \mathbb{G}_m \cdot (G_{A,\ell})_W$. In particular, $G_{A,\ell}$ acts on W via homotheties. Therefore, any 1-dimensional subspace of W is a representation of $G_{A,\ell}$. By the equivalence of (a) and (d) in Lemma 8.2, we deduce that A has complex multiplication. The lemma now follows from Lemma 8.4. $\qquad\square$

We can now consider upper bounds of $\gamma_{A,\ell}$ for an arbitrary abelian variety.

Theorem 8.6. *Let A be a nonzero abelian variety over K. We have $\gamma_{A,\ell} \leq \dim A$, with equality holding if and only if A is isogenous over $\overline{K}$ to a power of a CM elliptic curve.*

Proof. After replacing A by its base change by a finite extension of K, we may assume that there is an isogeny $\varphi \colon A \to \prod_{i=1}^n A_i$, where each A_i is a power of a geometrically simple abelian variety B_i over K and the B_i are pairwise nonisogenous over $\overline{K}$. We further assume that the group $G_{A,\ell}$, and hence all the groups $G_{A_i,\ell}$, are connected. By Proposition 3.5(ii), we have

$$\gamma_{A,\ell} = \frac{\dim W}{\dim G_{A,\ell} - \dim(G_{A,\ell})_W}$$

for some nonzero $\mathbb{Q}_\ell$-subspace $W \subseteq V_\ell(A)$ that is the direct sum of isotypic components of $V_\ell(A)$ as a representation of $G_{A,\ell}$. Our fixed isogeny φ induces an isomorphism $V_\ell(A) = \oplus_{i=1}^n V_\ell(A_i)$ of representations of $G_{A,\ell}$. We have $\mathrm{Hom}_{G_{A,\ell}}(V_\ell(A_i), V_\ell(A_j)) = \mathrm{Hom}(A_i, A_j) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = 0$ for all distinct $1 \leq i, j \leq n$ by Proposition 2.4(iii). Therefore, $W = \oplus_{i=1}^n W_i$, where W_i is a direct sum of isotypic components of $V_\ell(A_i)$ as a representation of $G_{A_i,\ell}$.

Let I be the set of $i \in \{1, \ldots, n\}$ with $W_i \neq 0$. For each $i \in I$, we have a natural homomorphism of groups $G_{A,\ell}/(G_{A,\ell})_W \twoheadrightarrow G_{A_i,\ell}/(G_{A_i,\ell})_{W_i}$ (we have used that W_i and W are direct sum of isotypic components to guarantee that we are taking a quotient by a normal subgroup). In particular,

$$\dim G_{A,\ell} - \dim(G_{A,\ell})_W \geq \dim G_{A_i,\ell} - \dim(G_{A_i,\ell})_{W_i}.$$

Therefore,

$$\gamma_{A,\ell} = \sum_{i \in I} \frac{\dim W_i}{\dim G_{A,\ell} - \dim(G_{A,\ell})_W} \leq \sum_{i \in I} \frac{\dim W_i}{\dim G_{A_i,\ell} - \dim(G_{A_i,\ell})_W} \leq \sum_{i \in I} \gamma_{A_i,\ell}.$$

By Lemma 8.5, we have

$$\sum_{i \in I} \gamma_{A_i,\ell} \leq \sum_{i \in I} \dim A_i \leq \dim A,$$

with equalities holding if and only if $I = \{1, \ldots, n\}$ and A_i is isogenous over $\overline{K}$ to a power of a CM elliptic curve for all $1 \leq i \leq n$. In particular, we have show that $\gamma_{A,\ell} < \dim A$ whenever A does not

have complex multiplication. The case where A has complex multiplication has already been dealt with in Lemma 8.4. $\square$

Proof of Theorem 8.1. By Theorem 6.2, we have $\beta_A = \gamma_{A,\ell}$ for some prime ℓ. The theorem is then an immediate consequence of Theorem 8.6. $\square$

9. The extension generated by a single torsion point

In this section we prove the following result concerning the degrees of the extensions generated by a single torsion point. In §9.4, we will use it to prove Theorem 1.6. We make use of the notation d_1 from §5.2.

Theorem 9.1. *Let A be a nonzero abelian variety defined over a number field K. Define δ to be the minimum value of $\dim G^\circ_{A,\ell} - d_1(G^\circ_{A,\ell})$ as we vary over all primes ℓ. Take any real number $\varepsilon > 0$. Then for any integer $n \geq 1$ and any point $P \in A(\overline{K})$ of order n, we have*

$$[K(P) : K] \gg_{A,\varepsilon} n^{\delta-\varepsilon}.$$

Moreover, δ is the largest real number with this property.

The structure of the proof is similar to that of Theorem 1.1: we reduce to the case when the order of P is the power of a single prime ℓ and we establish the required inequality separately for each prime, with a constant which is independent of ℓ for $\ell \gg_A 1$.

9.1. Some lemmas.

Lemma 9.2. *Fix a Noetherian integral domain R and let F be its fraction field. Let G be a reductive subgroup of $\mathrm{GL}_{n,R}$. Take any integer $m \geq 0$. Then there is a unique reduced closed subscheme Z_m of $\mathbb{A}^n_R$ such that for any field k that is an R-algebra and any $w \in k^n$, we have $w \in Z_m(k)$ if and only if $\dim(G_k)_W \geq m$ where $W := k \cdot w \subseteq k^n$.*

Proof. The group G is a smooth group scheme over $S := \mathrm{Spec}\, R$. There is a natural left action of G on the S-scheme $X := \mathbb{A}^n_R$. Define the morphisms $f : G \times_S X \to X \times_S X$ and $\Delta : X \to X \times_S X$ by $(g,x) \mapsto (g \cdot x, x)$ and $x \mapsto (x,x)$, respectively. We define Y to be the X-scheme given by the cartesian product

$$
\begin{array}{ccc}
Y & \longrightarrow & X \\
\downarrow & & \downarrow{\scriptstyle\Delta} \\
G \times_S X & \xrightarrow{\;f\;} & X \times_S X.
\end{array}
$$

This defines an X-group scheme Y that we may view as a closed X-group subscheme of $G \times_S X$, and Y is of finite type over X; for details see [SGA3 I, V.10.2]. The function

$$X \to \mathbb{Z}, \quad x \mapsto \dim Y_x,$$

where Y_x is the fiber of Y over x, is upper semicontinuous as a consequence of Chevalley's semicontinuity theorem, cf. [SGA3 I, VIB.4.1]. Equivalently, for each integer $m \geq 0$, the set Z_m of points $x \in X$ that satisfy $\dim Y_x \geq m$ can be viewed as a reduced closed subscheme of X.

Now consider any field k that is an R-algebra. Take any nonzero $w \in k^n = X(k^n)$ and define the subspace $W := k \cdot w \subseteq k^n$. The fiber Y_w is group scheme over k that is isomorphic to the algebraic subgroup of G_k that fixes w. In particular, $Y_w \cong (G_k)_W$ and hence $\dim Y_w = \dim(G_k)_W$. Therefore, $w \in Z_m(k)$ if and only if $\dim(G_k)_W \geq m$.

Finally, Z_m as given in the statement of the lemma is unique since it is a reduced closed subscheme of $\mathbb{A}^n_R$ for which we know the set $Z_m(k)$ for all fields k that are R-algebras. $\square$

We now give some basic properties of $d_1(G)$ when G is defined over a field.

Lemma 9.3. *Let F be a field and fix an algebraic closure $\overline{F}$. Let G be a reductive subgroup of GL_V where V is a finite dimensional vector space over F.*

    (i) *For any field extension L of F, we have $d_1(G_L) \leq d_1(G_{\overline{F}})$.*

    (ii) *For any algebraically closed field L containing F, we have $d_1(G_L) = d_1(G_{\overline{F}})$.*

Proof. After choosing a basis for V, we may assume that G is a subgroup of $\mathrm{GL}_{n,F}$. Fix notation as in Lemma 9.2 with $R := F$. Let $m_1 \geq 0$ be the maximal integer for which the F-variety $Z_{m_1} - \{0\}$ is nonempty (note that Z_m is empty whenever $m > \dim G$). For any field extension L/F, the set $Z_m(L) - \{0\}$ is empty for all $m > m_1$. Therefore, $d_1(G_L) \leq m_1$ by the description of the sets $Z_m(L)$ in Lemma 9.2.

Now take any algebraic closed field L containing F. Then $m_1 \geq 0$ is also the minimal integer for which the set $Z_{m_1}(L) - \{0\}$ is nonempty. From our description of the sets $Z_m(L)$ in Lemma 9.2, we deduce that $d_1(G_L) = m_1$. In particular, when $L = \overline{F}$ we have $d_1(G_{\overline{F}}) = m_1$. The lemma is now immediate. $\qquad\square$

The following shows that for ℓ large enough, d_1 of the special and generic fibers of the $\mathbb{Z}_\ell$-scheme $\mathcal{G}_{A,\ell}$ will agree.

Lemma 9.4. *Let A be a nonzero abelian variety defined over a number field K. Assume that the groups $G_{A,\ell}$ are connected for all ℓ. Then $d_1((\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}) = d_1(G_{A,\ell})$ for all sufficiently large primes ℓ.*

Proof. By taking ℓ large enough, we may assume that $\mathcal{G}_{A,\ell}$ is reductive by Proposition 2.5(ii). After choosing a basis for the ℓ-adic Tate module, we shall view $\mathcal{G}_{A,\ell}$ as a closed subgroup of $\mathrm{GL}_{2g,\mathbb{Z}_\ell}$. Also by taking ℓ sufficiently large, we may assume that $(\mathcal{G}_{A,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}}$ is conjugate in $\mathrm{GL}_{2g,\mathbb{Z}_\ell^{\mathrm{un}}}$ to $\mathcal{G}_{\mathbb{Z}_\ell^{\mathrm{un}}}$ for one of the finitely many reductive groups $\mathcal{G} \subseteq \mathrm{GL}_{2g,\mathbb{Z}}$ from Proposition 2.10. Take any integer $0 \leq m \leq (2g)^2$.

With $R = \mathbb{Z}$ and $G = \mathcal{G}$, let Z_m be the subscheme of $\mathbb{A}^{2g}_{\mathbb{Z}}$ from Lemma 9.2. Define $C_0 := Z_m$. For $i \geq 0$, we recursively define C_{i+1} to be the singular locus of C_i. Note that the C_i are reduced closed subschemes of $\mathbb{A}^{2g}_{\mathbb{Z}}$. Let $r \geq 0$ be the minimal integer for which the generic fiber of the $\mathbb{Z}$-scheme C_r is empty. There is a positive integer N so that $(C_r)_{\mathbb{Z}[1/N]}$ is empty. By taking ℓ large enough, we may assume that $\ell \nmid N$ (this uses that there are only finitely many m and $\mathcal{G}$ we are considering).

For each $0 \leq i < r$, define the $\mathbb{Z}$-scheme $U_i := C_i - C_{i+1}$; it is clearly a regular scheme. The generic fiber of U_i is a variety over $\mathbb{Q}$ that is regular and hence is smooth. So there is a positive integer N such that $(U_i)_{\mathbb{Z}[1/N]}$ is a smooth scheme over $\mathbb{Z}[1/N]$. By taking ℓ large enough, we may assume that $(U_i)_{\mathbb{Z}_\ell}$ is smooth for all $0 \leq i < r$.

With $R = \mathbb{Z}_\ell$ and $G = \mathcal{G}_{A,\ell}$, let $Z_{m,\ell}$ be the reduced closed subscheme Z_m of $\mathbb{A}^{2g}_{\mathbb{Z}_\ell}$ from Lemma 9.2. Define $C_{0,\ell} := Z_{m,\ell}$. For $i \geq 0$, we recursively define $C_{i+1,\ell}$ to be the singular locus of $C_{i,\ell}$; they are closed subschemes of $\mathbb{A}^{2g}_{\mathbb{Z}_\ell}$. Using that singular loci and the construction of the scheme from Lemma 9.2 are both stable under base change, we deduce that $(C_{i,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}}$ and $(C_i)_{\mathbb{Z}_\ell^{\mathrm{un}}}$ are isomorphic $\mathbb{Z}_\ell^{\mathrm{un}}$-schemes. Since $(C_{r,\ell})_{\mathbb{Z}_\ell^{\mathrm{un}}} \cong (C_r)_{\mathbb{Z}_\ell^{\mathrm{un}}}$ is empty and the inclusion $\mathbb{Z}_\ell \subseteq \mathbb{Z}_\ell^{\mathrm{un}}$ is a faithfully flat ring map, we find that $C_{r,\ell}$ is also empty. For $0 \leq i < r$, define the $\mathbb{Z}_\ell$-scheme $U_{i,\ell} := C_{i,\ell} - C_{i+1,\ell}$. We have $U_{i,\ell} \cong (U_i)_{\mathbb{Z}_\ell}$ and hence $U_{i,\ell}$ is smooth. By Hensel's lemma and the smoothness of $U_{i,\ell}$, the reduction modulo ℓ map $U_{i,\ell}(\mathbb{Z}_\ell) \to U_{i,\ell}(\mathbb{F}_\ell)$ is surjective for all $1 \leq i < r$. Since $C_{r,\ell}$ is empty, we find that $Z_{m,\ell}(\mathbb{F}_\ell) = \cup_{0 \leq i < r} U_{i,\ell}(\mathbb{F}_\ell)$ and hence $Z_{m,\ell}(\mathbb{Z}_\ell) \to Z_{m,\ell}(\mathbb{F}_\ell)$ is surjective.

So after taking ℓ sufficiently large, we have shown that for all integers $m \geq 0$, the reduction modulo ℓ map $Z_{m,\ell}(\mathbb{Z}_\ell) \to Z_{m,\ell}(\mathbb{F}_\ell)$ is surjective; this is trivial for the excluded integers $m > (2g)^2$ since $Z_{m,\ell}$ will be empty. In particular, if $Z_{m,\ell}(\mathbb{F}_\ell) - \{0\}$ is nonempty, then $Z_{m,\ell}(\mathbb{Q}_\ell) - \{0\}$ is nonempty as well. Now suppose that $Z_{m,\ell}(\mathbb{Q}_\ell)$ contains a nonzero element w. We can scale w by any nonzero element of $\mathbb{Q}_\ell$ and it will still lie in $Z_{m,\ell}(\mathbb{Q}_\ell)$. So without loss of generality, we

may assume that $w \in \mathbb{Z}_\ell^{2g} - \ell\mathbb{Z}_\ell^{2g}$. We have $w \in Z_m(\mathbb{Z}_\ell)$ and its reduction modulo ℓ gives a nonzero element of $Z_m(\mathbb{F}_\ell)$. So by taking ℓ sufficiently large, we have shown that for all $m \geq 0$, $Z_{m,\ell}(\mathbb{F}_\ell) - \{0\}$ is nonempty if and only if $Z_{m,\ell}(\mathbb{Q}_\ell) - \{0\}$ is nonempty. The lemma is now an immediate consequence of Lemma 9.2. $\qquad\square$

Lemma 9.5. *Let G be a reductive subgroup of $\mathrm{GL}_{n,\mathbb{Z}[1/N]}$ for some positive integer N. Then for all sufficiently large primes $\ell \nmid N$ and all one-dimensional subspaces W of $\overline{\mathbb{F}}_\ell^n$, the group $(G_{\overline{\mathbb{F}}_\ell})_W$ is smooth.*

Proof. Fix a generator w of W. The group $(G_{\overline{\mathbb{F}}_\ell})_W$ is defined inside $\mathrm{GL}_{n,\overline{\mathbb{F}}_\ell}$ by the equations of $G_{\overline{\mathbb{F}}_\ell}$ (whose number and degrees are bounded uniformly in ℓ), together with the n linear equations that encode the condition $g \cdot w = w$. In particular, the number of equations defining $(G_{\overline{\mathbb{F}}_\ell})_W$ and their degrees are bounded uniformly in ℓ. The result then follows immediately from [Lom17, Proposition 1] (notice that this result is stated for finite fields of characteristic ℓ, but the proof makes it clear that it also applies to $\overline{\mathbb{F}}_\ell$). $\qquad\square$

9.2. Prime power case.
Throughout this section, we let A be a nonzero abelian variety defined over a number field K for which the groups $G_{A,\ell}$ are connected for all ℓ. We shall prove that Theorem 9.1 holds when we restrict to the case where n is a power of a prime ℓ. We first give an argument that will work for all sufficiently large ℓ and then one that will work for any remaining ℓ.

Proposition 9.6. *For any prime $\ell \gg_A 1$, if $P \in A(\overline{K})$ is a point of order ℓ^e, then*
$$[K(P) : K] \gg_A (\ell^e)^{\dim G_{A,\ell} - d_1(G_{A,\ell})}.$$

Proof. By taking $\ell \gg_A 1$, we may assume by Proposition 2.5 that the $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell} \subseteq \mathrm{GL}_{T_\ell(A)}$ is reductive and that ℓ is odd. By choosing a basis for $T_\ell(A)$ as a $\mathbb{Z}_\ell$-module, we identify $\mathcal{G}_{A,\ell}$ with an algebraic subgroup of $\mathrm{GL}_{2g,\mathbb{Z}_\ell}$. In particular, we have $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell} \subseteq \mathrm{GL}_{2g,\mathbb{F}_\ell}$. Define $\mathfrak{g} := \mathfrak{g}_\ell \subseteq M_{2g}(\mathbb{F}_\ell)$ as in §4.1; it is the Lie algebra of $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ by Lemma 4.2.

Define the number field $L := K(P)$ and the group $U := A(L)[\ell^\infty]$. Following the proof of Theorem 4.1 given in §4.2, we find that
$$[L : K] \gg_A \ell^{\sum_{j=0}^\infty (\dim \mathfrak{g} - \dim \mathfrak{g}_{W_j})},$$
where W_j is a certain subspace of $\mathbb{F}_\ell^{2g}$ that satisfies $W_j \cong U[\ell^{i+1}]/U[\ell^i]$. Note that the sum occuring in the exponent is actually finite since for j large enough we have $W_j = 0$ and hence $\mathfrak{g}_{W_j} = \mathfrak{g}$.

Since U contains the point P of order ℓ^e, we have subspaces $W_j' \subseteq W_j$ satisfying $\dim W_j' = 1$ for $0 \leq j < e$ and $W_j' = 0$ for $j \geq e$. Since clearly $\dim \mathfrak{g}_{W_j'} \geq \dim \mathfrak{g}_{W_j}$, we obtain
$$[K(P) : K] = [L : K] \gg_A \ell^{\sum_{j=0}^{e-1} (\dim \mathfrak{g} - \dim \mathfrak{g}_{W_j'})}.$$

Set $G := (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$. We claim that for $\ell \gg_A 1$, the group variety G_W is smooth for all one-dimensional subspaces $W \subseteq \mathbb{F}_\ell^{2g}$. It suffices to show that $(G_{\overline{\mathbb{F}}_\ell})_W$ is smooth for all one-dimensional subspaces $W \subseteq \overline{\mathbb{F}}_\ell^{2g}$. Let $\{\mathcal{G}_i\}_{i \in I}$ be the finite collection of reductive subgroups of $\mathrm{GL}_{2g,\mathbb{Z}}$ from Proposition 2.10. By taking $\ell \gg_A 1$, Proposition 2.10 implies that $G_{\overline{\mathbb{F}}_\ell}$ and $\mathcal{G}_{\overline{\mathbb{F}}_\ell}$ are conjugate subgroups of $\mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell}$, where $\mathcal{G} = \mathcal{G}_i$ for some $i \in I$. The claim then follows from Lemma 9.5 and the finiteness of I.

By taking $\ell \gg_A 1$, the above claim proves that $G_{W_j'}$ is smooth for all j. We thus have $\dim \mathfrak{g}_{W_j'} = \dim G_{W_j'}$ since $\mathfrak{g}_{W_j'}$ is the Lie algebra of the smooth group variety $G_{W_j'}$. Therefore, $\dim \mathfrak{g}_{W_j'} \leq d_1(G)$ for all j. We have $\dim \mathfrak{g} = \dim G$ since G is reductive and hence smooth. So we obtain the inequality
$$[K(P) : K] \gg_A (\ell^e)^{\dim G - d_1(G)}.$$

38

We have $\dim G = \dim G_{A,\ell}$ since $\mathcal{G}_{A,\ell}$ is reductive. We have $d_1(G) = d_1(G_{A,\ell})$ for $\ell \gg_A 1$ by Lemma 9.4. The proposition is now immediate. $\qquad\square$

Proposition 9.7. *For every prime ℓ and every point $P \in A(\overline{K})$ of order ℓ^e, we have*

$$[K(P) : K] \gg_{A,\ell} (\ell^e)^{\dim G_{A,\ell} - d_1(G_{A,\ell})}.$$

Proof. Set $G = G_{A,\ell}$. We begin by showing the following analogue of Proposition 5.7. Let $\mathcal{G} \subseteq \mathrm{GL}_{n,\mathbb{Z}_\ell}$ be a linear group scheme such that $G = \mathcal{G}_{\mathbb{Q}_\ell}$ has finite slope. There is a positive constant $C(\mathcal{G})$ such that for every $m \geq 1$ and every *cyclic* subgroup $H \subseteq (\mathbb{Z}/\ell^m\mathbb{Z})^n = \mathbb{A}^n(\ell^m)$ we have

$$(9.1) \qquad [\mathcal{G}(\mathbb{Z}_\ell) : \mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H)] \geq \frac{1}{C(\mathcal{G})}|H|^{\dim G - d_1(G)},$$

where

$$\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H) := \{M \in \mathcal{G}(\mathbb{Z}_\ell)\,|\,\pi_m(M) \text{ is the identity on } H\}.$$

The proposition can be deduced from this statement (applied to the subgroup H generated by P) exactly as Theorem 5.1 is deduced from Proposition 5.7.

To prove (9.1) we proceed as in the proof of Proposition 5.7, taking in particular the same notation. For the convenience of the reader, we repeat here the main steps, which in the present setting are much simpler than in the general case.

Since H is cyclic, generated by a point of order ℓ^e, we can take $r = 1$ and $m_1 = m = e$. We also set $\mathcal{W}_1 := \mathbb{Z}_\ell e_1$ and $\mathcal{G}_1 := \mathrm{Fix}_{\mathcal{G}_{\mathbb{Z}_\ell}}(\mathcal{W}_1)$, where $e_1 \in \mathbb{Z}_\ell^{2g}$ projects to a generator of H modulo ℓ^m. We then obtain

$$[\mathcal{G}(\mathbb{Z}_\ell) : \mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H)] \geq \frac{|\pi_{m_1}(\mathcal{G}(\mathbb{Z}_\ell))|}{|\pi_{m_1}(\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H))|}.$$

The numerator is lower-bounded by $C_1(\mathcal{G})\ell^{m \dim G}$, see Lemma 5.16. The denominator is at most the cardinality of $\mathcal{G}_1(\ell^m)$, which by Proposition 5.9 (applied to $\mathcal{G}_1$, $r = 1$ and $m' = 0$) is at most $C(\mathcal{G})\ell^{d_1(G)m}$. Hence, the quantity above is lower-bounded by $\frac{C_1(\mathcal{G})}{C(\mathcal{G})}\ell^{m(\dim G - d_1(G))}$, as desired. $\qquad\square$

9.3. **Proof of Theorem 9.1.** After replacing K by a finite extension, and A by its base extension to this field, we may assume that all the groups $G_{A,\ell}$ are connected by Proposition 2.3. This is allowable since it will only increase the degree of $K(P)$ by a uniformly bounded quantity and will not change the groups $G_{A,\ell}^\circ$.

Let $P \in A(\overline{K})$ be any torsion point and denote its order by n. We have a factorization $n = \prod_{\ell|n} \ell^{e_\ell}$ and $P = \sum_{\ell|n} P_\ell$ with $P_\ell \in A(\overline{K})$ a torsion point of order ℓ^{e_ℓ}. By Proposition 2.9 there exists a finite extension K' of K such that the extensions $K'(A[\ell^\infty])/K'$ are all linearly disjoint as ℓ ranges over the prime numbers. Thus, we have

$$(9.2) \qquad [K(P) : K] \gg_A [K'(P) : K'] = \prod_{\ell|n}[K'(P_\ell) : K'].$$

By Propositions 9.6 and 9.7, we obtain the inequality

$$(9.3) \qquad [K'(P_\ell) : K'] \geq C \cdot (\ell^{e_\ell})^{\dim G_{A,\ell} - d_1(G_{A,\ell})} \geq C\ell^\varepsilon \cdot (\ell^{e_\ell})^{\dim G_{A,\ell} - d_1(G_{A,\ell}) - \varepsilon}$$

for all $\ell|n$, where C is a positive constant depending only on A. Combining (9.2) and (9.3), and using that $C\ell^\varepsilon \geq 1$ for all $\ell \gg_{A,\varepsilon} 1$, we obtain

$$[K(P) : K] \gg_{A,\varepsilon} \prod_{\ell|n}(\ell^{e_\ell})^{\dim G_{A,\ell} - d_1(G_{A,\ell}) - \varepsilon}$$

and hence $[K(P) : K] \gg_{A,\varepsilon} n^{\delta - \varepsilon}$.

It remains to show that δ is the maximal value for which $[K(P) : K] \gg_{A,\varepsilon} n^{\delta - \varepsilon}$ holds for all $\varepsilon > 0$, all positive integers n and all torsion points $P \in A(\overline{K})$ of order n. Choose a prime ℓ

for which $\delta = \dim G_{A,\ell} - d_1(G_{A,\ell})$. There is a one-dimensional subspace W of $V_\ell(A)$ for which $d_1(G_{A,\ell}) = \dim(G_{A,\ell})_W$. Define $\mathcal{W} := W \cap T_\ell(A)$; it is a rank one $\mathbb{Z}_\ell$-module. Let w be a $\mathbb{Z}_\ell$-basis of $\mathcal{W}$. For every $e \geq 1$, the image of w in $T_\ell(A)/\ell^e T_\ell(A) = A[\ell^e]$ defines a torsion point P_e of exact order ℓ^e. Arguing as in the proof of Theorem 6.2, we obtain

$$[K(P_e) : K] = \frac{[K(A[\ell^e]) : K]}{[K(A[\ell^e]) : K(P_e)]} \asymp_{A,\ell} (\ell^e)^{\dim G_{A,\ell} - \dim((G_{A,\ell})_W)} = (\ell^e)^\delta.$$

Letting $e \to \infty$, we see that δ in the statement of the theorem cannot be replaced with a larger value.

9.4. **Proof of Theorem 1.6.**

After replacing K by a finite extension, and A by its base extension to this field, we may assume that all the groups $G_{A,\ell}$ are connected by Proposition 2.3. Note that this only changes the degree $[K(P) : K]$ by a uniformly bounded amount. Let δ be the minimal value $\dim G_{A,\ell} - d_1(G_{A,\ell}))$ as we vary over all primes ℓ. The theorem will then be a direct consequence of Theorem 9.1 once we show that $\delta = d$.

We claim that $\delta = \dim G_A - d_1((G_A)_{\overline{\mathbb{Q}}})$. We have $(G_A)_{\mathbb{Q}_\ell} = G_{A,\ell}$ since we are assuming the Mumford–Tate conjecture for A, and hence $\dim G_A = \dim G_{A,\ell}$ and $d_1((G_A)_{\mathbb{Q}_\ell}) = d_1(G_{A,\ell})$. Therefore, $\delta = \dim G_A - \max_\ell d_1((G_A)_{\mathbb{Q}_\ell})$ and we need only prove that $d_1((G_A)_{\overline{\mathbb{Q}}}) = \max_\ell d_1((G_A)_{\mathbb{Q}_\ell})$. For all ℓ, we have $d_1((G_A)_{\overline{\mathbb{Q}}}) \geq d_1((G_A)_{\mathbb{Q}_\ell})$ by Lemma 9.3(i). So it suffices to show that $d_1((G_A)_{\overline{\mathbb{Q}}}) \leq d_1((G_A)_{\mathbb{Q}_\ell})$ for some prime ℓ. Set $m := d_1((G_A)_{\overline{\mathbb{Q}}})$. By choosing a basis, we may assume G_A is a subgroup of $\mathrm{GL}_{2g,\mathbb{Q}}$. With $R = \mathbb{Q}$ and $G = G_A$, let Z_m be the subscheme of $\mathbb{A}_{\mathbb{Q}}^{2g}$ from Lemma 9.2. By our choice of m, there is a nonzero $w \in Z_m(\overline{\mathbb{Q}})$. Let $L \subseteq \overline{\mathbb{Q}}$ be a number field for which $w \in Z_m(L)$. Take any prime ℓ that splits completely in L. There is an embedding $L \hookrightarrow \mathbb{Q}_\ell$ and hence $Z_m(\mathbb{Q}_\ell)$ contains a nonzero element. From our description of the set $Z_m(\mathbb{Q}_\ell)$ from Lemma 9.2, we deduce that $d_1((G_A)_{\mathbb{Q}_\ell}) \geq m$ which completes our proof of the claim.

By the above claim and Lemma 9.3(ii), we have $\delta = \dim G_A - d_1((G_A)_{\mathbb{C}})$. By choosing a basis for V_A, we may view G_A as a subgroup of $\mathrm{GL}_{2g,\mathbb{Q}}$. Take any nonzero $w \in \mathbb{C}^{2g}$. With $W := \mathbb{C}w$, define $H := ((G_A)_{\mathbb{C}})_W$; it is the subgroup of $(G_A)_{\mathbb{C}}$ that fixes w. Let $(G_A)_{\mathbb{C}} \to \mathbb{A}_{\mathbb{C}}^{2g}$ be the morphism $g \mapsto g \cdot w$. This morphism factors through an immersion $(G_A)_{\mathbb{C}}/H \hookrightarrow \mathbb{A}_{\mathbb{C}}^{2g}$, cf. [Mil17, Proposition 7.17]. Therefore, the orbit of w under the action of $(G_A)_{\mathbb{C}}$ has dimension $\dim G_A - \dim((G_A)_{\mathbb{C}})_W$. By varying over all nonzero $w \in \mathbb{C}^{2g}$, we deduce that $d = \dim G_A - d_1((G_A)_{\mathbb{C}})$. Therefore, $\delta = d$.

References

[BL04] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004. MR2062673 ↑2.1

[Bog80] Fedor Alekseivich Bogomolov, *Sur l'algébricité des représentations ℓ-adiques*, C. R. Acad. Sci. Paris Sér. A-B **290** (1980), no. 15, A701–A703 (French, with English summary). MR574307 ↑2.2

[CF19] Victoria Cantoral Farfán, *Torsion for abelian varieties of type III*, J. Number Theory **198** (2019), 346–380, DOI 10.1016/j.jnt.2018.10.017. MR3912942 ↑1

[Chi92] Wên Chên Chi, *l-adic and λ-adic representations associated to abelian varieties defined over number fields*, Amer. J. Math. **114** (1992), no. 2, 315–353, DOI 10.2307/2374706. MR1156568 ↑2.5

[Com19] Johan Commelin, *The Mumford-Tate conjecture for products of abelian varieties*, Algebr. Geom. **6** (2019), no. 6, 650–677. MR4009176 ↑6.3

[Cot22] Sean Cotner, *Centralizers of sections of a reductive group scheme* (2022), available at arXiv:2203.15133. ↑5

[CR81] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. I*, Pure and Applied Mathematics, John Wiley & Sons, Inc., New York, 1981. With applications to finite groups and orders. MR632548 ↑2.5

[DMOS82] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin-New York, 1982. MR654325 ↑2.1, 2.3

[Fal86] Gerd Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 9–27. Translated from the German original [Invent. Math. **73** (1983), no. 3, 349–366; ibid. **7**5 (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz. MR861971 ↑2.2, 2.5

[Ful98] William Fulton, *Intersection theory*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 2, Springer-Verlag, Berlin, 1998. ↑2.6

[GGN17] Skip Garibaldi, Robert M. Guralnick, and Daniel K. Nakano, *Globally irreducible Weyl modules*, J. Algebra **477** (2017), 69–87, DOI 10.1016/j.jalgebra.2016.11.038 (English). ↑2.5

[GR22] Éric Gaudron and Gaël Rémond, *Nombre de petits points sur une variété abélienne* (2022), available at https://lmbp.uca.fr/~gaudron/art21.pdf. ↑1

[GW20] Ulrich Görtz and Torsten Wedhorn, *Algebraic geometry I. Schemes. With examples and exercises*, Wiesbaden: Springer Spektrum, 2020 (English). ↑5.1, 5.3, 5.1

[HR10] Marc Hindry and Nicolas Ratazzi, *Torsion dans un produit de courbes elliptiques*, J. Ramanujan Math. Soc. **25** (2010), no. 1, 81–111 (French, with English and French summaries). MR2643390 ↑1

[HR12] _____, *Points de torsion sur les variétés abéliennes de type GSp*, J. Inst. Math. Jussieu **11** (2012), no. 1, 27–65, DOI 10.1017/S147474801000023X (French, with English and French summaries). MR2862374 ↑1, 3.8

[HR16] _____, *Torsion pour les variétés abéliennes de type I et II*, Algebra Number Theory **10** (2016), no. no. 9, 1845–1891. MR3576113 ↑1, 2.4, 3.8

[Jan03] Jens Carsten Jantzen, *Representations of algebraic groups.*, 2nd ed., Math. Surv. Monogr., vol. 107, Providence, RI: American Mathematical Society (AMS), 2003 (English). ↑2.5

[LP95] Michael Larsen and Richard Pink, *Abelian varieties, ℓ-adic representations, and ℓ-independence*, Math. Ann. **302** (1995), no. 3, 561–579. MR1339927 (97e:14057) ↑2.2, 2.3

[LP97] _____, *A connectedness criterion for l-adic Galois representations*, Israel J. Math. **97** (1997), 1–10. MR1441234 (98k:11066) ↑2.2

[Lom17] Davide Lombardo, *Roots of unity and torsion points of abelian varieties*, Ramanujan J. **43(2)** (2017), 383–403. ↑2.6, 9.1

[Mas] David W. Masser, *Lettre à Daniel Bertrand du 10 novembre 1986*. ↑1, 8

[MW95] David W. Masser and Gisbert Wüstholz, *Refinements of the Tate conjecture for abelian varieties*, Abelian varieties (Egloffstein, 1993), de Gruyter, Berlin, 1995, pp. 211–223. MR1336608 ↑

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, No. 33, Princeton University Press, Princeton, N.J., 1980. ↑3.2, 5.4

[Mil17] _____, *Algebraic groups. The theory of group schemes of finite type over a field*, Camb. Stud. Adv. Math., vol. 170, Cambridge: Cambridge University Press, 2017 (English). ↑3.2, 9.4

[MZ99] B. J. J. Moonen and Yu. G. Zarhin, *Hodge classes on abelian varieties of low dimension*, Math. Ann. **315** (1999), no. 4, 711–733, DOI 10.1007/s002080050333. MR1731466 ↑8

[Nor87] Madhav V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Invent. Math. **88** (1987), no. 2, 257–275, DOI 10.1007/BF01388909. MR880952 ↑2.6

[Oes82] Joseph Oesterlé, *Reduction modulo p^n des sous-ensembles analytiques fermés de $\mathbb{Z}_p^N$.*, Invent. Math. **66** (1982), 325–341, DOI 10.1007/BF01389398 (French). ↑5.4

[Pin98] Richard Pink, *l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture*, J. Reine Angew. Math. **495** (1998), 187–237, DOI 10.1515/crll.1998.018. MR1603865 ↑2.5

[Poh68] Henry Pohlmann, *Algebraic cycles on abelian varieties of complex multiplication type*, Ann. of Math. (2) **88** (1968), 161–180, DOI 10.2307/1970570. MR228500 ↑8

[Rat07] Nicolas Ratazzi, *Borne sur la torsion dans les variétés abéliennes de type CM*, Ann. Sci. École Norm. Sup. (4) **40** (2007), no. 6, 951–983, DOI 10.1016/j.ansens.2007.10.002 (French, with English and French summaries). MR2419854 ↑1

[Rib80] Kenneth A. Ribet, *Division fields of abelian varieties with complex multiplication*, Mém. Soc. Math. France (N.S.) **2** (1980/81), 75–94. MR608640 ↑8

[Rib83] _____, *Hodge classes on certain types of abelian varieties*, Amer. J. Math. **105** (1983), no. 2, 523–538, DOI 10.2307/2374267. MR701568 ↑1.2

[Ser77] Jean-Pierre Serre, *Représentations ℓ-adiques*, Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), Japan Soc. Promotion Sci., Tokyo, 1977, pp. 177–193 (French). MR0476753 ↑2.3

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. MR644559 (83k:12011) ↑4.1, 6

[Ser00] ———, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000. 1985–1998.   MR1730973 (2001e:01037) ↑2.2, 2.4

[Ser13] ———, *Un critère d'indépendance pour une famille de représentations ℓ-adiques*, Comment. Math. Helv. **88** (2013), no. 3, 541–554, DOI 10.4171/CMH/295 (French, with English summary). MR3093502 ↑2.4

[SGA3 I] Michel Demazure, Alexandre Grothendieck, Michael Artin, Jean-Étienne Bertin, Peter Gabriel, Michel Raynaud, and Jean-Pierre Serre (eds.), *Séminaire de géométrie algébrique du Bois Marie 1962-64. Schémas en groupes (SGA 3). Tome I: Propriétés générales des schémas en groupes*, New annotated edition of the 1970 original published by Springer, Doc. Math. (SMF), vol. 7, Paris: Société Mathématique de France, 2011 (French). ↑9.1

[SGA3 III] ——— (ed.), *Séminaire de géométrie algébrique du Bois Marie 1962-64. Schémas en groupes (SGA 3). Tome III: Structure des schémas en groupes réductifs*, New annotated edition of the 1970 original published by Springer, Doc. Math. (SMF), vol. 8, Paris: Société Mathématique de France, 2011 (French). ↑2.5

[Stacks] The Stacks Project Authors, *Stacks Project* (2022), available at https://stacks.math.columbia.edu. ↑2.5, 5.4

[UY13] Emmanuel Ullmo and Andrei Yafaev, *Mumford-Tate and generalised Shafarevich conjectures*, Ann. Math. Qué. **37** (2013), no. 2, 255–284, DOI 10.1007/s40316-013-0009-4 (English, with English and French summaries). ↑2.5, 8

[Vas08] Adrian Vasiu, *Some cases of the Mumford-Tate conjecture and Shimura varieties*, Indiana Univ. Math. J. **57** (2008), no. 1, 1–75, DOI 10.1512/iumj.2008.57.3513. MR2400251 ↑2.3

[Win02] Jean-Pierre Wintenberger, *Démonstration d'une conjecture de Lang dans des cas particuliers*, J. Reine Angew. Math. **553** (2002), 1–16. MR1944805 (2003i:11075) ↑2.2

[Zyw19] David Zywina, *An effective open image theorem for abelian varieties* (2019), available at arXiv:1910. 14171. ↑2.4

Institut Fourier, Université Grenoble Alpes, 38610 Gières, France
Email address: Samuel.Le-Fourn@univ-grenoble-alpes.fr

Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo 5, 56127 Pisa, Italy
Email address: davide.lombardo@unipi.it

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
Email address: zywina@math.cornell.edu