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

1. Introduction

Let A be a nonzero abelian variety defined over a number field K. For every finite extension L of K, the group $A(L)_{\mathrm{tors}}$ of torsion points in $A(L)$ is finite. We are interested in finding upper bounds for the cardinality of $A(L)_{\mathrm{tors}}$ 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 $|A(L)_{\mathrm{tors}}| \leq C \cdot [L:K]^{\beta}$, where C is a constant depending only on A and β. Usually, one expects that Masser's bound remains true if $\dim A$ is replaced with some smaller value.

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

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

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 $\beta_A \leq \dim A$.

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 $I \subseteq \{1,\ldots,n\}$, 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

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

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 $\beta_A \geq \gamma_A$ [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]. Cantoral Farfán has proved several additional cases, see [CF19]. 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]. 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.

2020 *Mathematics Subject Classification.* Primary 11G10; Secondary 14K15.

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.

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

Theorem 1.2. *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 1.3. *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.*

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 $\mathrm{GL}_M(B) = \mathrm{Aut}_B(B \otimes_R M)$. A choice of basis of the R-module M induces an isomorphism $\mathrm{GL}_M \cong \mathrm{GL}_{d,R}$, 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 F. For a subspace W of V, we let G_W be the algebraic subgroup of G that fixes W; more precisely, we have $G_W(B) = \{g \in G(B) : gw = w \text{ for all } w \in B \otimes_F V\}$ for all F-algebras B.
- We define the Mumford-Tate group G_A of an abelian variety A in §2.1.
- The ℓ-adic Tate module of A is denoted by $T_\ell(A)$ and $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. We define the ℓ-adic monodromy groups $G_{A,\ell} \subseteq \mathrm{GL}_{V_\ell(A)}$ over $\mathbb{Q}_\ell$ and $\mathcal{G}_{A,\ell} \subseteq \mathrm{GL}_{T_\ell(A)}$ 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

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

  which can be $+\infty$ if, 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 $|A(L)_{\mathrm{tors}}| \ll_{A,\beta} [L:K]^\beta$. 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

$$\gamma_A \cdot (\dim G - \dim G_W) \geq \dim W \tag{1.1}$$

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 3.7(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. Finally in §7, we make some remarks on a conjectural expression for β_A not involving Mumford–Tate groups.

1.3. **Acknowledgments.** The first author is suuported by the IRS grant QUAD (Labex Persyval), a PEPS JCJC grant 2022 and the ANR project JINVARIANT. The second author gratefully acknowledges funding from MIUR (Italy, grant PRIN 2017 "Geometric, algebraic and analytic methods in arithmetic") and from the University of Pisa (grant PRA 2018-19 "Spazi di moduli, rappresentazioni e strutture combinatorie"). The first two authors thank Gaël Rémond for many inspiring discussions and for his insightful comments and ideas, which greatly helped them with writing parts of this paper.

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 embedding $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \hookrightarrow \mathrm{End}_{\mathbb{Q}}(V)$. 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* $\operatorname{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}\hookrightarrow \operatorname{End}_{\mathbb{Q}}(V)$ *is* $\operatorname{End}_{\mathbb{Q}}(V)^{G_A}$.

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

$$V=\oplus_{i=1}^n V_i \tag{2.1}$$

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

For each subset $I\subseteq\{1,\dots,n\}$, define the subspace $V_I:=\oplus_{i\in I}V_i$ 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. For the projection map $V\to V_I$, arising from (2.1), the induced homomorphism $\operatorname{GL}_V\to\operatorname{GL}_{V_I}$ gives rise to 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

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

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

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

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 $\operatorname{End}_{\mathbb{Q}}(V)^{G_A}=\prod_{i=1}^n\operatorname{End}_{\mathbb{Q}}(V_i)^{G_A}$ and each $\operatorname{End}_{\mathbb{Q}}(V_i)^{G_A}$ is isomorphic to $M_{e_i}(D_i)$ for some integer $e_i\geq 1$ and division algebra D_i (the ring $\operatorname{End}(A_i^{m_i})\otimes_{\mathbb{Z}}\mathbb{Q}$ 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). $\square$

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 $\operatorname{GL}_{V_\ell(A)}$ with the generic fiber of $\operatorname{GL}_{T_\ell(A)}$.

The Galois group $\operatorname{Gal}_K:=\operatorname{Gal}(\overline{K}/K)$ 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

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

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

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

Denote by $G^\circ_{A,\ell}$ 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

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

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.*

Proposition 2.4. *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 and the action of $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ on $A[\ell]$ is semisimple.*

Proof. From Faltings [Fal86], we know that Gal_K acts semisimply on $V_\ell(A)$. Part (i) is then a direct consequence. Part (ii) is proved in [LP95] though also see [Win02, §1.3]: the main ingredient is that for $\ell \gg_A 1$, the action of Gal_K is semisimple on $A[\ell]$ by a theorem of Faltings (see Corollary 2 of [MW95]). ☐

2.3. **The Mumford–Tate conjecture.** 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 $G^\circ_{A,\ell}$ and $(G_A)_{\mathbb{Q}_\ell}$ are the same algebraic group when we use the comparison isomorphism as an identification, cf. [Ser77, §3].

Conjecture 2.5 (Mumford–Tate conjecture for A)**.** *For each prime ℓ, we have $G^\circ_{A,\ell} = (G_A)_{\mathbb{Q}_\ell}$.*

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 2.6.

- (i) *For each prime ℓ, we have $G^\circ_{A,\ell} \subseteq (G_A)_{\mathbb{Q}_\ell}$.*
- (ii) *The Mumford–Tate conjecture for A holds if and only if the common rank of the groups $G^\circ_{A,\ell}$ 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]. ☐

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 (see also the proof of Theorem 10.1 of [HR16]).

Theorem 2.7. *There is a constant C, depending only on A, such that $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell^\infty}(\mathrm{Gal}_K)] \le C$ for all primes ℓ.*

Proof. After replacing A by its base extension by an appropriate finite extension of K, we may assume that all the groups $G_{A,\ell}$ are connected, cf. Proposition 2.3. By taking $\ell \gg_A 1$, we may assume by Proposition 2.4 that $\mathcal{G}_{A,\ell}$ is a reductive group scheme over $\mathbb{Z}_\ell$. The theorem for the finite number of excluded primes follows by taking the implicit constant large enough and using the openness of $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ in $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$.

Denote by $\mathcal{S}_{A,\ell}$ and $\mathcal{C}_{A,\ell}$ the derived subgroup and central torus, respectively, of $\mathcal{G}_{A,\ell}$. To prove the theorem, it suffices to show that the indices $[\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell) : \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell) \cap \rho_{A,\ell^\infty}(\mathrm{Gal}_K)]$ and $[\mathcal{C}_{A,\ell}(\mathbb{Z}_\ell) : \mathcal{C}_{A,\ell}(\mathbb{Z}_\ell) \cap \rho_{A,\ell^\infty}(\mathrm{Gal}_K)]$ can be bounded independent of ℓ. That the index involving $\mathcal{C}_{A,\ell}$ can be bounded independently of ℓ was observed by Serre, cf. [Ser00, 138 p.60].

The group $\mathcal{S}_{A,\ell}$ is a semisimple group scheme over $\mathbb{Z}_\ell$. Denote by $\pi_\ell \colon \mathcal{S}^{sc}_{A,\ell} \to \mathcal{S}_{A,\ell}$ the simply connected cover of the semisimple group scheme. Define $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)_u := \pi_\ell(\mathcal{S}^{sc}_{A,\ell}(\mathbb{Z}_\ell))$; it is an open subgroup of $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)$. Wintenberger has proved that $\rho_{A,\ell^\infty}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)_u$ for all primes $\ell \gg_A 1$, cf. [Win02, Théorème 2]. So it suffices to prove that the index $[\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell) : \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)_u]$ can be bounded independent of ℓ. By [Win02, Proposition 1], it thus suffices to prove that $[\mathcal{S}_{A,\ell}(\mathbb{F}_\ell) : \pi_\ell(\mathcal{S}^{sc}_{A,\ell}(\mathbb{F}_\ell))]$ can be bounded independent of ℓ. The algebraic groups $(\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$ and $(\mathcal{S}^{sc}_{A,\ell})_{\mathbb{F}_\ell}$ are connected of the same dimension (which can be bounded in terms of g), so it suffices to prove that the degree of π_ℓ can be bounded independent of ℓ. The degree of π_ℓ can be read off the Lie type of $(\mathcal{S}_{A,\ell})_{\overline{\mathbb{F}}_\ell}$. Finally, note that there are only finitely many possible Lie types since the rank of $(\mathcal{S}_{A,\ell})_{\overline{\mathbb{F}}_\ell}$ can be bounded in terms of g. ☐

Proposition 2.8. *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]. ☐

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.

Proposition 2.9. *There is a finite collection $\{\varrho_i \colon \mathcal{G}_i \to \mathrm{GL}_{2g,\mathbb{Z}}\}_{i\in I}$ of representations of split reductive groups over $\mathbb{Z}$ such that for any sufficiently large prime ℓ there is an $i \in I$ so that the following hold:*

(a) *$G_{A,\ell} \to \mathrm{GL}_{V_\ell(A)}$ and ϱ_i are isomorphic after base-change to $\overline{\mathbb{Q}}_\ell$,*
(b) *$(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell} \to \mathrm{GL}_{A[\ell]}$ and ϱ_i are isomorphic after base-change to $\overline{\mathbb{F}}_\ell$.*

Proof. The Mumford–Tate group $G_A \subseteq \mathrm{GL}_{V_A}$, with $V_A := H_1(A(\mathbb{C}), \mathbb{Q})$, is reductive by Lemma 2.1(i). Let C be the central torus of G_A, i.e., the neutral component of its center. Let $X(C)$ be the group of characters $C_{\overline{\mathbb{Q}}} \to \mathbb{G}_{m,\overline{\mathbb{Q}}}$. Let $\Omega_0 \subseteq X(C)$ be the set of weights of C acting on V_A. In particular, we have

$$V_A \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} = \oplus_{\alpha\in\Omega_0} V_\alpha,$$

where V_α is a nonzero $\overline{\mathbb{Q}}$-vector space consisting of all $v \in V_A \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ that satisfy $t \cdot v = \alpha(t)\, v$ for all $t \in C(\overline{\mathbb{Q}})$. Since C and G_A commute, we deduce that each V_α is a representation of $(G_A)_{\overline{\mathbb{Q}}}$. Let d_α be the dimension of V_α over $\overline{\mathbb{Q}}$.

Take any prime ℓ. Let C_ℓ and S_ℓ be the central torus and derived subgroup, respectively, of the reductive group $G_{A,\ell}$. By Proposition 2.6(i), we have $G_{A,\ell} \subseteq (G_A)_{\mathbb{Q}_\ell}$. By [UY13, Corollary 2.11], we have $C_\ell = C_{\mathbb{Q}_\ell}$ in $(G_A)_{\mathbb{Q}_\ell}$. Now fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. Take any $\alpha \in \Omega_0$ and define $V_{\alpha,\ell} := V_\alpha \otimes_{\overline{\mathbb{Q}}} \overline{\mathbb{Q}}_\ell$. The vector space $V_{\alpha,\ell}$ is a representation of $G := (G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}$ with the central torus $(C_\ell)_{\overline{\mathbb{Q}}_\ell} = C_{\overline{\mathbb{Q}}_\ell}$ acting by homotheties given by α.

There is a split semisimple group scheme $\mathcal{S}$ over $\mathbb{Z}$ such that $\mathcal{S}_{\overline{\mathbb{Q}}_\ell} \cong (S_\ell)_{\overline{\mathbb{Q}}_\ell}$, cf. [SGA3, Exposé XXV §1], and we can construct $\mathcal{S}$ directly from the root datum of $(S_\ell)_{\overline{\mathbb{Q}}_\ell}$. Following Jantzen

[Jan03, II.8.2], for every dominant weight μ of $\mathcal{S}$, we can define a $\mathbb{Z}$-representation $V(\mu)$ of $\mathcal{S}$ which over $\mathbb{Q}$ coincides with the unique irreducible representation of $\mathcal{S}_{\mathbb{Q}}$ with dominant weight μ. By using the dominant weights of the irreducible representations in $V_{\alpha,\ell}$ of $(S_\ell)_{\overline{\mathbb{Q}}_\ell}$ and their multiplicities, we deduce that there is a representation $\rho_\alpha\colon \mathcal{S} \to \mathrm{GL}_{M_\alpha}$, with $M_\alpha := \mathbb{Z}^{d_\alpha}$, so that after base-extending to $\overline{\mathbb{Q}}_\ell$ it is isomorphic to the natural homomorphism $(S_\ell)_{\overline{\mathbb{Q}}_\ell} \to \mathrm{GL}_{V_{\alpha,\ell}}$.

Let $\mathcal{C}$ be the split torus over $\mathbb{Z}$ isomorphic to C over $\overline{\mathbb{Q}}$ for which we can identify the character group of $\mathcal{C}$ with $X(C)$. For $\alpha \in \Omega_0$, we extend ρ_α to a representation

$$\rho_\alpha\colon \mathcal{C} \times \mathcal{S} \to \mathrm{GL}_{M_\alpha},$$

where $\mathcal{C}$ acts on M_α via the character α. Therefore, $\rho_\alpha\colon \mathcal{C} \times \mathcal{S} \to \mathrm{GL}_{M_\alpha}$ base extended to $\overline{\mathbb{Q}}_\ell$ is isomorphic to the natural representation $(C_\ell)_{\overline{\mathbb{Q}}_\ell} \times (S_\ell)_{\overline{\mathbb{Q}}_\ell} \to \mathrm{GL}_{V_{\alpha,\ell}}$ (the actions of $(C_\ell)_{\overline{\mathbb{Q}}}$ and $\mathcal{C}_{\overline{\mathbb{Q}}}$ are both given by the same character α, and since they act via homotheties they both commute with the corresponding semisimple group). Combining the representations ρ_α together, we obtain a single representation

$$\rho\colon \mathcal{C} \times \mathcal{S} \to \mathrm{GL}_M,$$

where $M := \oplus_{\alpha\in\Omega_0} M_\alpha \cong \mathbb{Z}^{2g}$. The representation ρ and the natural representation $C_\ell \times S_\ell \to \mathrm{GL}_{V_\ell(A)}$ are isomorphic after being base extended to $\overline{\mathbb{Q}}_\ell$.

The group $\mathcal{G} := \rho(\mathcal{C} \times \mathcal{S})$ is a split reductive group defined over $\mathbb{Z}$. Let

$$\varrho\colon \mathcal{G} \to \mathrm{GL}_M$$

be the representation given by the inclusion morphism. Since $G_{A,\ell}$ is the image of $C_\ell \times S_\ell \to \mathrm{GL}_{V_\ell(A)}$, we deduce that ϱ and the representation $G_{A,\ell} \hookrightarrow \mathrm{GL}_{V_\ell(A)}$ are isomorphic when base extended to $\overline{\mathbb{Q}}_\ell$. In particular, (a) holds with $\varrho_i := \varrho$.

Now by taking ℓ large enough, we may assume by Proposition 2.4(ii) that the $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell} \subseteq \mathrm{GL}_{T_\ell(A)}$ is reductive and that the action of $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ on $A[\ell]$ is semisimple. The $\mathbb{Z}_\ell$-group schemes $\mathcal{G}_{A,\ell}$ and $\mathcal{G}_{\mathbb{Z}_\ell}$ are reductive and isomorphic over $\overline{\mathbb{Q}}_\ell$ and hence are isomorphic over $\overline{\mathbb{F}}_\ell$ by [Dem65, Theorem 5.1.2], since the base $\operatorname{Spec}\mathbb{Z}_\ell$ is connected and so the type is constant. By base changing $\mathcal{G}_{A,\ell} \hookrightarrow \mathrm{GL}_{T_\ell(A)}$ to $\overline{\mathbb{Q}}_\ell$, we obtain $(G_{A,\ell})_{\overline{\mathbb{Q}}_\ell} \to \mathrm{GL}_{V_\ell(A)\otimes_{\mathbb{Q}_\ell}\overline{\mathbb{Q}}_\ell}$. So by comparing with the representation $\mathcal{G}_{\overline{\mathbb{Q}}_\ell} \to \mathrm{GL}_{M\otimes_{\mathbb{Z}}\overline{\mathbb{Q}}_\ell} \cong \mathrm{GL}_{2g,\overline{\mathbb{Q}}_\ell}$ obtained by base changing ϱ, we find that (b) holds with $\varrho_i := \varrho$ (note that the reductive groups $(\mathcal{G}_{A,\ell})_{\overline{\mathbb{F}}_\ell}$ and $\mathcal{G}_{\overline{\mathbb{F}}_\ell}$ have the same root data and their representations have the same weights and multiplicities since this is true for the corresponding fibers over $\overline{\mathbb{Q}}_\ell$).

For each prime ℓ, we have constructed a representation $\varrho\colon \mathcal{G} \to \mathrm{GL}_M \cong \mathrm{GL}_{2g,\mathbb{Z}}$ of a reductive group scheme over $\mathbb{Z}$ that satisfies (a) with $\varrho_i := \varrho$ and for ℓ sufficiently large also satisfies (b) with $\varrho_i := \varrho$. It remains to show that as we vary ℓ, we obtain only finitely many ϱ up to isomorphism.

There are only finitely many possibilities for the root datum of S_ℓ, up to isomorphism, since S_ℓ is semisimple of bounded dimension. Therefore, up to isomorphism, there are only finitely many semisimple groups $\mathcal{S}$ over $\mathbb{Z}$ that could arise.

We now fix a possible $\mathcal{S}$ and restrict ourselves to primes ℓ for which $\mathcal{S}_{\overline{\mathbb{Q}}_\ell} \cong (S_\ell)_{\overline{\mathbb{Q}}_\ell}$. The minuscule weight conjecture, proved by Pink [Pin98, Corollary 5.11], says that all the weights of $V_{\alpha,\ell}$ as a representation of $(S_\ell)_{\overline{\mathbb{Q}}_\ell}$ are minuscule. So, up to isomorphism, there are only finitely many possibilities for the representations ρ_α, with $\alpha \in \Omega_0$, since a semisimple group has only finitely many minuscule weights and the rank of these representations are bounded. Therefore, up to isomorphism, we have only finitely many possibilities for the representation $\rho\colon \mathcal{S} \to \mathrm{GL}_M$. Finally, since the torus $\mathcal{C}$ and its action on M does not depend on the prime ℓ, we deduce that there are only finitely many possible groups $\mathcal{G}$ and representations $\varrho\colon \mathcal{G} \to \mathrm{GL}_M$ up to isomorphism. $\square$

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 $\mathcal{H} := (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ with an algebraic subgroup of $\mathrm{GL}_{2g,\mathbb{F}_\ell}$. For each subspace $W \subseteq \mathbb{F}_\ell^{2g}$, let $\mathcal{H}_W$ be the algebraic subgroup of $\mathcal{H}$ as defined in §1.1. The goal of this section is to give bounds on the cardinality of $\mathcal{H}_W(\mathbb{F}_\ell)$ that do not depend on W.

For $W \subseteq \mathbb{F}_\ell^{2g}$, let m_W be the number of irreducible components of $(\mathcal{H}_W)_{\overline{\mathbb{F}}_\ell}$. Since $(\mathcal{H}_W)_{\overline{\mathbb{F}}_\ell}$ 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 2.10. *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 $\mathcal{H}_W$ 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, $\mathcal{H}_W = \mathcal{H} \cap (\mathrm{GL}_{2g,\mathbb{F}_\ell})_W$ 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 $\iota(\mathcal{H}) \cap L = \iota(\mathcal{H}_W)$. We can choose a linear subspace L' in $\mathbb{P}^n_{\overline{\mathbb{F}}_\ell}$ of codimension $\dim \mathcal{H}_W$ that intersects every irreducible component of $\iota(\mathcal{H}_W)_{\overline{\mathbb{F}}_\ell}$ and $\iota(\mathcal{H}_W)_{\overline{\mathbb{F}}_\ell} \cap L'$ is finite. Let X be the Zariski closure of $\iota(\mathcal{H})$ 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, $m_W \leq \deg(X)$ since linear spaces have degree 1 and the degree of a variety is stable under extension of fields. See [Ful98, §8.4] for background on Bézout's theorem and the degree of a closed subvariety of projective space.

By taking ℓ large enough, Proposition 2.9 implies that the subvariety X of $\mathbb{P}^n_{\mathbb{F}_\ell}$ 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 $\deg(X) \ll_A 1$. Therefore, $m_W \leq \deg(X) \ll_A 1$. ☐

Proposition 2.11. *For any subspace $W \subseteq \mathbb{F}_\ell^{2g}$, we have $|\mathcal{H}_W(\mathbb{F}_\ell)| \asymp_A \ell^{\dim \mathcal{H}_W}$.*

Proof. We have inequalities $|\mathcal{H}_W^\circ(\mathbb{F}_\ell)| \leq |\mathcal{H}_W(\mathbb{F}_\ell)| \leq m_W \cdot |\mathcal{H}_W^\circ(\mathbb{F}_\ell)|$. Since $m_W \ll_A 1$ by Lemma 2.10, it suffices to show that $|\mathcal{H}_W^\circ(\mathbb{F}_\ell)| \asymp_A \ell^{\dim \mathcal{H}_W}$. So the proposition is a consequence of [Nor87, Lemma 3.5] which shows that $(\ell-1)^{\dim \mathcal{H}_W} \leq |\mathcal{H}_W^\circ(\mathbb{F}_\ell)| \leq (\ell+1)^{\dim \mathcal{H}_W}$. ☐

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.

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 3.1. *For any non-zero 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. □

Lemma 3.2.

(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 3.1 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 3.1 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. □

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 3.2(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 3.3. *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 give a subspace of $V \otimes_F L$ strictly larger than U' such that $\alpha(\mathfrak{g} \otimes_F L, U \otimes_F L) = \alpha(\mathfrak{g} \otimes_F L)$; this contradicts the maximality of U'. Therefore, $U_0 = U$ and the lemma follows. $\square$

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 that 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. Define

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

where the minimum is over all nonzero subspaces $W \subseteq V$. The following shows that to compute $\alpha(G)$, we need only consider a finite number of special subspaces W. 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 of V, the Lie algebra of G_W agrees with the Lie algebra $\mathfrak{g}_W$ (for a proof of the analogous statement in the case of stabilizers, see [Mil80, Proposition 10.31]). In particular, $\dim G_W = \dim \mathfrak{g}_W$. Therefore, $\alpha(G) = \alpha(\mathfrak{g})$.

Proposition 3.4.

(i) *We have*

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

where $V_I := \bigoplus_{i \in I} V_i$.

(ii) *For any field extension F'/F we have $\alpha(G_{F'}) = \alpha(G)$, where we are using the embedding $G_{F'} \subseteq \mathrm{GL}_{V \otimes_F F'}$.*

Proof. Let U be the maximal subspace of V such that $\alpha(\mathfrak{g}, U) = \alpha(\mathfrak{g})$, see Lemma 3.2(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 3.3, 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 $U = \bigoplus_{i \in I} U \cap V_i$. We have $\mathfrak{g}_U = \mathfrak{g}_{V_I}$ 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. We have thus proved that

$$\alpha(\mathfrak{g}) = \min_{\emptyset \neq I \subseteq \{1,\dots,n\}} \alpha(\mathfrak{g}, V_I). \tag{3.1}$$

Part (i) follows since $\alpha(\mathfrak{g}) = \alpha(G)$ and $\alpha(\mathfrak{g}, V_I) = (\dim G - \dim G_{V_I})/\dim V_I$.

We now prove (ii). Since F is perfect, there exists a finite Galois extension L/F over which all irreducible representations of G_L in $V \otimes_F L$ stay irreducible after extending by any field extension of L. Using part (i), we find that $\alpha(G_L) = \alpha(G_{LF'}) \leq \alpha(G_{F'})$. Since $\alpha(G_{F'}) \leq \alpha(G)$, it suffices to prove that $\alpha(G_L) = \alpha(G)$. By Lemma 3.3, we have $\alpha(G_L) = \alpha(\mathfrak{g} \otimes_F L) = \alpha(\mathfrak{g}) = \alpha(G)$. $\square$

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 an 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

$$V = \oplus_{i=1}^n V_i. \tag{3.2}$$

By Lemma 2.2, the direct sum (3.2) is the decomposition of the representation V of G_A into isotypic components. So with $G_A \subseteq \mathrm{GL}_V$, Proposition 3.4(i) 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 $V_I := \oplus_{i\in I} V_i$. 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,

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

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

Proposition 3.5. *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*

$$\gamma_A \cdot (\dim G - \dim G_W) \geq \dim W. \tag{3.4}$$

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 3.4(ii). □

Remark 3.6. We proved Proposition 3.5 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 3.5 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 is a finite extension K'/K such that $V_\ell(A)$ has a nonzero subspace stable under 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

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

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

Lemma 3.7. *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

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

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 $1 \le i, j \le n$. We have

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

by Faltings' proof of the Tate conjecture for abelian varieties, cf. Corollary 1 in §5 of [Fal86]. Since A_i and A_j are simple and nonisogenous, we have $\mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_{K'}]}(V_\ell(A_i^{m_i}), V_\ell(A_j^{m_j})) = 0$ 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 3.4(i), we have

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

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 the 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

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

This proves that $\gamma_{A,\ell} \ge \max_{\emptyset \ne I \subseteq \{1,\dots,n\}} 2 \dim A_I / (\dim G_{A_I,\ell}^\circ)$. By Proposition 2.6(i), we deduce that

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

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 3.4(ii). $\square$

We have $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell} \subseteq \mathrm{GL}_{T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell} = \mathrm{GL}_{A[\ell]}$.

Lemma 3.8. *Let $\mathcal{G}$ be a reductive group subscheme of $\mathrm{GL}_{2g,\mathbb{Z}}$. For all $\ell \gg_{\mathcal{G}} 1$ we have $\alpha(\mathcal{G}_{\mathbb{Q}_\ell}) = \alpha(\mathcal{G}_{\mathbb{F}_\ell})$. If $\rho : \mathcal{G} \to \mathrm{GL}_{2g,\mathbb{Z}}$ is a representation of a reductive group scheme $\mathcal{G}$ over $\mathbb{Z}$, then we have $\alpha((\rho(\mathcal{G}))_{\mathbb{Q}_\ell}) = \alpha((\rho(\mathcal{G}))_{\mathbb{F}_\ell})$ for all $\ell \gg_{\mathcal{G},\rho} 1$.*

Proof. We prove the first statement, which clearly implies the second. Write $\mathbb{Q}^{2g} = \bigoplus_{j=1}^r W_j$, where the W_j are the isotypic components for the action of $\mathcal{G}_{\mathbb{Q}}$, and define $\mathcal{W}_j = W_j \cap \mathbb{Z}^{2g}$ and $\overline{\mathcal{W}_j} := \mathcal{W}_j \otimes_{\mathbb{Z}} \mathbb{F}_\ell$. Assuming ℓ is large enough, we have $\bigoplus_j \mathcal{W}_j \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = \mathbb{Z}_\ell^{2g}$ and the central idempotents of $\mathrm{End}_{\mathcal{G}_{\mathbb{Z}_\ell}}(\mathbb{Z}_\ell^{2g})$ all come from central idempotents of $Z(\mathrm{End}_{\mathcal{G}}(\mathbb{Z}^{2g})) \otimes \mathbb{Z}_\ell$. Furthermore, by [CR06, Lemmas 77.4 and 77.10], the central idempotents of $\mathrm{End}_{\mathcal{G}_{\mathbb{F}_\ell}}(\mathbb{F}_\ell^{2g})$ come from those over $\mathbb{Z}$. This proves that the isotypic components of $\mathcal{G}_{\mathbb{F}_\ell}$ are the $\overline{\mathcal{W}_j}$ for $1 \le j \le r$. For any subset $J \subseteq \{1, \dots, r\}$ write $\mathcal{W}_J := \bigoplus_{j \in J} \mathcal{W}_j$ and $W_J := \bigoplus_{j \in J} W_j$. By Proposition 3.4(i) we have

$$\alpha(\mathcal{G}_{\mathbb{F}_\ell}) = \min_{J \ne \emptyset} \frac{\dim(\mathcal{G}_{\mathbb{F}_\ell}) - \dim \mathrm{Fix}_{\mathcal{G}}(\mathcal{W}_J)_{\mathbb{F}_\ell}}{\dim(\mathcal{W}_J \otimes_{\mathbb{Z}} \mathbb{F}_\ell)}.$$

Now, $\mathrm{Fix}_{\mathcal{G}}(\mathcal{W}_J)$ is a subgroup scheme, so its generic fibre (which is an algebraic group over a field of characteristic zero) is automatically smooth. In particular, $\mathrm{Fix}_{\mathcal{G}}(\mathcal{W}_J)$ is smooth over $\mathbb{Z}_\ell$ for $\ell \gg_{\mathcal{G}} 1$, which implies that $\dim \mathrm{Fix}_{\mathcal{G}}(\mathcal{W}_J)_{\mathbb{F}_\ell} = \dim \mathrm{Fix}_G(W_J)$ for ℓ large enough: indeed, notice that the generic fibre of $\mathrm{Fix}_{\mathcal{G}}(\mathcal{W}_J)$ is $\mathrm{Fix}_G(W_J)$. Assuming ℓ is large enough, the group $\mathcal{G}$ is smooth over $\mathbb{Z}_\ell$, so $\dim(\mathcal{G}_{\mathbb{F}_\ell}) = \dim(\mathcal{G}_{\mathbb{Q}})$. Furthermore, the dimension of $\mathcal{W}_J \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ agrees with the dimension of W_J. Combining these observations with Proposition 3.4(i), applied to $\mathcal{G}_{\mathbb{Q}}$, yields $\alpha(\mathcal{G}_{\mathbb{F}_\ell}) = \alpha(\mathcal{G}_{\mathbb{Q}})$. Finally, we have $\alpha(\mathcal{G}_{\mathbb{Q}}) = \alpha(\mathcal{G}_{\mathbb{Q}_\ell})$ by the invariance of α under extensions of fields (Proposition 3.4(ii)). □

Proposition 3.9. *Assume that all the ℓ-adic monodromy groups $G_{A,\ell}$ are connected. For $\ell \gg_A 1$ we have $\alpha(G_{A,\ell}) = \alpha((\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell})$.*

Proof. Consider the finite family $\{\varrho_i : \mathcal{G}_i \to \mathrm{GL}_{2g,\mathbb{Z}}\}_{i\in I}$ of representations of split reductive groups over $\mathbb{Z}$ from Proposition 2.9. Take $\ell \gg_A 1$ large enough so that the conclusion of Proposition 2.9 holds for some $i \in I$. Therefore, $\alpha((G_{A,\ell})_{\overline{\mathbb{Q}}_\ell}) = \alpha(\varrho_i(\mathcal{G}_i)_{\overline{\mathbb{Q}}_\ell})$ and $\alpha((\mathcal{G}_{A,\ell})_{\overline{\mathbb{F}}_\ell}) = \alpha(\rho_i(\mathcal{G}_i)_{\overline{\mathbb{F}}_\ell})$. By Proposition 3.4(ii), we have $\alpha(G_{A,\ell}) = \alpha(\varrho_i(\mathcal{G}_i)_{\mathbb{Q}_\ell})$ and $\alpha((\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}) = \alpha(\varrho_i(\mathcal{G}_i)_{\mathbb{F}_\ell})$. By assuming ℓ is large enough, depending only on A, we will have $\alpha(\varrho_i(\mathcal{G}_i)_{\mathbb{Q}_\ell}) = \alpha(\varrho_i(\mathcal{G}_i)_{\mathbb{F}_\ell})$ by Lemma 3.8 (this makes use of I being finite). Therefore, $\alpha(G_{A,\ell}) = \alpha((\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell})$. □

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

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

holds for all nonzero subspaces $W \subseteq V_\ell(A)$. In this section, we prove the following bounds 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

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

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 $[B_1, B_2] = B_1B_2 - B_2B_1$.

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 $\dim G_{A,\ell}$.

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. $\square$

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

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

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. Set $H := \rho_{A,\ell^\infty}(\mathrm{Gal}_K)$. We then have $H(\ell^i) = \rho_{A,\ell^i}(\mathrm{Gal}_K)$. By Theorem 2.7, we have $[\mathcal{G}(\mathbb{Z}_\ell) : \rho_{A,\ell^\infty}(\mathrm{Gal}_K)] \ll_A 1$. By Lemma 4.3(i), we then obtain that $\mathfrak{h}_i = \mathfrak{g}_\ell$ for all $i \geq 1$ where $i \gg_A 1$ or $\ell \gg_A 1$. By (4.2), we deduce that

$$|\rho_{A,\ell^i}(\mathrm{Gal}_K)| = |H(\ell^i)| \asymp_A |H(\ell)| \cdot \ell^{(i-1)\dim \mathfrak{g}_\ell} = |H(\ell)| \cdot \ell^{(i-1)\dim G_{A,\ell}}.$$

Since $[\mathcal{G}(\mathbb{F}_\ell) : H(\ell)] \ll_A 1$, it suffices to show that $|\mathcal{G}(\mathbb{F}_\ell)| \asymp_A \ell^{\dim G_{A,\ell}}$. We have $\dim \mathcal{G}_{\mathbb{F}_\ell} = \dim \mathcal{G}_{\mathbb{Q}_\ell} = \dim G_{A,\ell}$. By Proposition 2.11 (with $W = 0$), we have $|\mathcal{G}(\mathbb{F}_\ell)| \asymp_A \ell^{\dim \mathcal{G}_{\mathbb{F}_\ell}} = \ell^{\dim G_{A,\ell}}$. $\square$

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 2.4 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

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

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 $\overline{\psi}_i \colon A[\ell^{i+1}]/A[\ell^i] \xrightarrow{\sim} \mathbb{F}_\ell^{2g}$. 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 $\overline{\psi}_i(W[\ell^{i+1}]/W[\ell^i])$.

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, $H(\ell) \subseteq \mathcal{H}_{W_0}(\mathbb{F}_\ell)$, where $\mathcal{H} := \mathcal{G}_{\mathbb{F}_\ell}$. By Proposition 2.11, we have $|H(\ell)| \leq |\mathcal{H}_{W_0}(\mathbb{F}_\ell)| \ll_A \ell^{\dim \mathcal{H}_{W_0}}$. Therefore,

$$|\rho_{A,\ell^i}(\mathrm{Gal}_L)| \ll_A \ell^{\dim \mathcal{H}_{W_0}} \cdot \ell^{\sum_{j=1}^{i-1} \dim \mathfrak{g}_{W_j}}.$$

Since $\mathcal{H}$ has Lie algebra $\mathfrak{g}$ by Lemma 4.2, $\mathcal{H}_{W_0}$ will have Lie algebra $\mathfrak{g}_{W_0}$ and hence $\dim \mathcal{H}_{W_0} = \dim \mathfrak{g}_{W_0}$. Therefore, $|\rho_{A,\ell^i}(\mathrm{Gal}_L)| \ll_A \ell^{\sum_{j=0}^{i-1} \dim \mathfrak{g}_{W_j}}$. ☐

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

$$[L : K] \gg_A \ell^{\sum_{j=0}^{i-1} \alpha(\mathfrak{g}) \dim W_j} = \Big(\prod_{j=0}^{i-1} |W_j|\Big)^{\alpha(\mathfrak{g})} = |U|^{\alpha(\mathfrak{g})}.$$

We have $\alpha(\mathfrak{g}) = \alpha((\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell})$ since $\mathfrak{g}$ is the Lie algebra of $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$. Therefore, $\alpha(\mathfrak{g}) = \gamma_{A,\ell}^{-1}$ by Lemma 3.9. The numerator and denominator of $\gamma_{A,\ell}$ can be bounded in terms of the dimension of A, so we have $|A(L)[\ell^\infty]| = |U| \ll_A [L : K]^{\gamma_{A,\ell}}$.

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 abelian variety A of dimension g over a number field K and every prime ℓ, there is a constant $C_1(A,\ell)$ such that we have*

$$|A(L)[\ell^\infty]| \leq C_1(A,\ell)[L:K]^{\gamma_{A,\ell}}$$

for all finite extensions L/K.

Since Theorem 4.1 gives a uniform value of $C_1(A,\ell)$ for all sufficiently large primes ℓ, the constant can actually be taken to be independent of ℓ. 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 3.9. 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 2.9.

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 $d \in \{1,\dots,n\}$. 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

$$S \mapsto \{\mathcal{O}_S\text{-submodule } \mathcal{U} \subseteq \mathcal{O}_S^n \;\big|\; \mathcal{O}_S^n/\mathcal{U} \text{ is a locally free } \mathcal{O}_S\text{-module of rank } n-d\}.$$

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].

Remark 5.3. 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*

$$R \mapsto \{(\varphi,\mathcal{W}) \in \mathrm{GL}_n(R) \times \mathrm{Grass}_{d,n}(R) \;\big|\; \varphi_{|\mathcal{W}} \textit{ is the identity on } \mathcal{W}\}$$

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. □

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 $\mathcal{W} : \operatorname{Spec} R \to \mathrm{Grass}_{d,n}$, denoted by $\mathrm{Fix}(\mathcal{W})$, satisfies

$$\mathrm{Fix}(\mathcal{W})(R) = \{\varphi \in \mathrm{GL}_n(R) \;\big|\; \varphi_{|\mathcal{W}} \text{ is the identity on } \mathcal{W}\}.$$

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}.

By definition, for every R_0-algebra R and every submodule $\mathcal{W}$ of R^n of rank d such that $R^n/\mathcal{W}$ is locally free of rank $n-d$ we have

$$\mathrm{Fix}_{\mathcal{G}}(\mathcal{W})(R) = \{\varphi \in \mathcal{G}(R) \,|\, \varphi_{|\mathcal{W}} \text{ is the identity on } \mathcal{W}\}.$$

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 introduced in Section 1.1. 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 $1 \le i \le j$. 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

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

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 ⇒ 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 $m \geq 1$ 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 2.7, we have

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

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

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

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

If G is of finite slope, we have

$$\dim G - d_r(G) \geq r/\gamma_G. \tag{5.1}$$

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*

$$\left|\ker\left(\pi_{m,m'} : \mathrm{Fix}_{\mathcal{G}}(\mathcal{W})(\ell^m) \to \mathrm{Fix}_{\mathcal{G}}(\mathcal{W})(\ell^{m'})\right)\right| \leq C(\mathcal{G})\ell^{d_r(G)(m-m')}. \tag{5.2}$$

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 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 (5.2) 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 ⇒ Proposition 5.7. We take the notation of Proposition 5.7. Consider a subgroup H of $(\mathbb{Z}/\ell^m\mathbb{Z})^n$, which we can assume to be nontrivial. 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

$$|H| = \prod_{i=1}^{r} \ell^{m_i}. \tag{5.3}$$

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

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

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

$$[\mathcal{G}(\mathbb{Z}_\ell) : \mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H)] \geq [\pi_{m_1}(\mathcal{G}(\mathbb{Z}_\ell)) : \pi_{m_1}(\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H))] = \frac{|\pi_{m_1}(\mathcal{G}(\mathbb{Z}_\ell))|}{|\pi_{m_1}(\mathrm{fix}_{\mathcal{G}(\mathbb{Z}_\ell)}(H'))|}, \tag{5.4}$$

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 5.14 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 backed to $\mathcal{G}(\ell^m)$. Setting by convention $m_{r+1} = 0$, we thus have

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

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, Equation (5.1) in the third line, and Equation (5.3) in the last line. Combined with (5.4), this implies the proposition. □

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 $\varepsilon : \operatorname{Spec}\mathbb{Z}_\ell \to \mathcal{G}$ 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 $r = 1, \ldots, n$, 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). Now, as $\mathbb{Q}_\ell$-points are dense in $\mathrm{Grass}_{r,n,\mathbb{Q}_\ell}$ (the $\mathbb{Q}$-points are already dense in

$\mathrm{Grass}_{r,n,\mathbb{Q}}$), this implies that the support of $\mathcal{F}$ is contained in the special fibre. As $\mathcal{F}$ is coherent, this implies that $\ell^{e_r}\mathcal{F} = 0$ for e_r sufficiently large. 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 $d_r(G)$. □

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

Lemma 5.14. *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. □

Any group scheme $\mathcal{G} \subseteq \mathrm{GL}_{n,\mathbb{Z}_\ell}$ satisfies the hypotheses of Lemma 5.14 (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 5.15. *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 $p : S'(\mathbb{Z}/\ell^m\mathbb{Z}) \to \mathbb{A}^d(\mathbb{Z}/\ell^m\mathbb{Z})$ 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

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

is $\ell^{d(m-m')}$, and $\pi_{m'} : S'(\mathbb{Z}_\ell) \to S'(\ell^{m'})$ 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 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 $\mathbb{A}^d$. □

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 5.16. *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

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

but this latter space is isomorphic to

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

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

Lemma 5.17 (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 $P_1, \dots, P_r$, by the fundamental exact sequences of the Kähler differentials we have

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

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

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

for suitable $e_1 \ge \ldots \ge e_n$ (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 $\dim_{\mathbb{F}_\ell} \ell^e M / \ell^{e+1} M \le d$, we have $e \ge e_i$ for $i = d+1, \dots, n$. Choose polynomials $Q_1, \dots, Q_n$ in I such that $\mathrm{d}Q_i = \ell^{\max(e_i, e)} \, \mathrm{d}X_i$ for all $i \in \{1, \dots, n\}$. Recall that ε corresponds to the ring morphism $\mathbb{Z}_\ell[X_1, \dots, X_n] \to \mathbb{Z}_\ell$ evaluating a polynomial at $(0, \dots, 0)$. As ε is a $\mathbb{Z}_\ell$-point of $S = \operatorname{Spec} \mathbb{Z}_\ell[X_1, \dots, X_n]/I$, the kernel of ε must contain I, so every element of I vanishes at $0 = (0, \dots, 0)$. 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 $i \in \{d+1, \dots, n\}$ we now consider the polynomial

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

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

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

We apply Lemma 5.15 with $A_i = \widetilde{Q}_i$ for every $i \in \{d+1, \dots, n\}$. In particular, we let S' denote the $\mathbb{Z}_\ell$-scheme defined in $\mathbb{A}^n_{\mathbb{Z}_\ell}$ by the ideal $\langle \widetilde{Q}_{d+1}, \dots, \widetilde{Q}_n \rangle$.

Let $x = (x_1, \dots, x_n) \in S(\ell^m) \subseteq \mathbb{A}^n_{\mathbb{Z}_\ell}(\ell^m) = (\mathbb{Z}/\ell^m\mathbb{Z})^n$ 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 $i = d+1, \dots, n$. 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 5.15, 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

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

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 $\mathbb{A}^n_{\mathbb{Z}_\ell}$. Via this embedding, a point in $S(\ell^m)$ that reduces to ε mod m' in $S(\ell^{m'})$ is in particular a point of $\mathbb{A}^n(\ell^m)$ that reduces to $(0, \dots, 0)$ 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.

(ii) This is a consequence of Lemma 5.16. 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 $\ell^{d(m-m')}$. □

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

Proposition 5.18. *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 5.17 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

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

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 5.17.

□

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 5.18 immediately implies the desired inequality with constant given by $C(n, d_r(G), e, \ell)$. For $m' = 0$ we then have

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

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 $\beta_{A_{K'}} \le \beta_A$ is trivial by considering extensions L 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

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

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

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 2.8, 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 $\beta_A \le \xi_A$. Take any finite extension L/K and let J be the set of primes that divide $|A(L)_{\mathrm{tors}}|$. 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 $\prod_{\ell\in J}[L_\ell : K] \le [L : K]$. By Theorems 4.1 and 5.1, there is a constant $C > 0$ depending only on A such that

$$|A(L)[\ell^\infty]| = |A(L_\ell)[\ell^\infty]| \le C \cdot [L_\ell : K]^{\gamma_{A,\ell}} \le C \cdot [L_\ell : K]^{\xi_A}$$

for all $\ell \in J$. Taking the product over all $\ell \in J$, we find that

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

Take any $\varepsilon > 0$ and set $\delta := 1 - 1/(1 + \varepsilon/\xi_A)$; we have $0 < \delta < 1$. We have

$$C^{|J|} = \prod_{\ell\in J} C \ll_{A,\varepsilon} \prod_{\ell\in J} \ell^\delta \le |A(L)_{\mathrm{tors}}|^\delta,$$

where the first inequality uses that $C \le \ell^\delta$ for all primes $\ell \gg_{A,\varepsilon} 1$. Using (6.1), this implies that $|A(L)_{\mathrm{tors}}| \ll_{A,\varepsilon} |A(L)_{\mathrm{tors}}|^\delta \cdot [L : K]^{\xi_A}$. Therefore,

$$|A(L)_{\mathrm{tors}}| \ll_{A,\varepsilon} [L : K]^{\xi_A/(1-\delta)} = [L : K]^{\xi_A+\varepsilon},$$

where the equality uses our choice of δ. Since L/K and $\varepsilon > 0$ were arbitrary, this implies that $\beta_A \le \xi_A$.

We now prove $\xi_A \le \beta_A$. 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 $i \ge 1$. 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 2.7, 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 $|A(L_i)_{\mathrm{tors}}| \ll_{A,\varepsilon} [L_i : K]^{\beta_A+\varepsilon}$ 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 $\beta_A \geq \gamma_{A,\ell} = \xi_A$. $\square$

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 3.7(ii).

6.2. **Proof of Theorem 1.2.** We have $\mathrm{End}(V)^{G_A} \cong \mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ by Lemma 2.1(ii). Since A is geometrically simple, the ring $\mathrm{End}(V)^{G_A}$ 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 3.7(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 2.6(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 2.6(ii).

The other implication follows directly from Theorem 1.1.

6.3. **Proof of Theorem 1.3.** 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 any 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 1.2 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 3.7.

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

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

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

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 2.6(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 3.4(ii).

With notation as in §2.1, we have $V = \oplus_{i=1}^{n} V_i$ which is the isotypic decomposition of V as a representation of G_A by Lemma 2.2. For a nonempty subset $I \subseteq \{1,\ldots,n\}$, define $V_I := \oplus_{i\in I} V_i$. 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,

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

We claim that $V = \oplus_{i=1}^{n} V_i$ 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 3.4(i) 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 $V = \oplus_{i=1}^{n} V_i$ is the isotypic decomposition as a representation of G_A and $H \subseteq G_A$, to prove the claim it suffices to show that $\mathrm{End}_{\mathbb{Q}}(V)^{G_A} = \mathrm{End}_{\mathbb{Q}}(V)^{H}$. We have $\mathrm{End}_{\mathbb{Q}}(V)^{G_A} \subseteq \mathrm{End}_{\mathbb{Q}}(V)^{H}$ 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 $\mathrm{End}_{\mathbb{Q}}(V)^{G_A} = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, where we are using that all the endomorphisms of $A_{\overline{K}}$ are defined over K. By Faltings [Fal86] and our assumption that all the endomorphisms of $A_{\overline{K}}$ are defined over K, we have $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))^{G_{A,\ell}^{\circ}} = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. Therefore,

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

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

We now prove Conjecture 7.1 for several abelian varieties. In particular, Conjecture 7.1 will hold whenever $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$; 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 $\mathrm{End}(A_{\overline{K}})$ 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 $\mathrm{End}(A_{\overline{K}}) = \mathrm{End}(A)$ and that the group $G_{A,\ell}$ is connected. The ring $D := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra since A is geometrically simple. From our assumption on $\mathrm{End}(A_{\overline{K}})$, 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 $\mathbb{Q}_\ell$.

From Faltings [Fal86, §5], we know that $V_\ell(A)$ is a semisimple $\mathbb{Q}_\ell[\mathrm{Gal}_K]$-module and that the natural map

$$D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A))$$

is an isomorphism. Therefore, $G_{A,\ell}$ is reductive and $\mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A))$ is a central simple algebra over $\mathbb{Q}_\ell$.

Denote by $V_\ell(A) = \oplus_{i=1}^{n} V_i$ the decomposition of the representation $V_\ell(A)$ of $G_{A,\ell}$ into isotypical components. We have $\mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A)) = \prod_{i=1}^{n} \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_i)$. Since $\mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A))$ is a simple $\mathbb{Q}_\ell$-algebra, we deduce that $n = 1$. Since there is only one isotypic component, by Proposition 3.4(i) 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 $\mathrm{End}(A_{\overline{K}}) = \mathrm{End}(A)$ and that $G_{A,\ell}$ is connected for all ℓ.

Denote the center of $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ 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 $\mathbb{Q}_\ell[\mathrm{Gal}_K]$-module that we can identify with a submodule of $V_\ell(A)$. We have $V_\ell(A) = \oplus_{\lambda|\ell} V_\lambda$ 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 3.4(i), we have

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

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 $E = \mathbb{Q}$.

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

[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

[CR06] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras.* (2006) (English). ↑3.3

[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

[Dem65] Michel Demazure, *Schémas en groupes réductifs*, Bull. Soc. Math. Fr. **93** (1965), 369–413, DOI 10.24033/bsmf.1629 (French). ↑2.5

[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. **7**3 (1983), no. 3, 349–366; ibid. **7**5 (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz. MR861971 ↑2.2, 3.3, 7, 7

[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

[GW20] Ulrich Görtz and Torsten Wedhorn, *Algebraic geometry I. Schemes. With examples and exercises*, Wiesbaden: Springer Spektrum, 2020 (English). ↑5.1, 5.2, 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, 3.6

[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, 3.6

[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

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

[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 ↑2.2

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

[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

[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

[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, 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] 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 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. ↑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

[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, 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