TORSION BOUNDS FOR A FIXED ABELIAN VARIETY AND VARYING NUMBER FIELD

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 $|A(L)_{\mathrm{tors}}| \le C \cdot [L:K]^{\beta_A+\varepsilon}$, where the constant C depends only on A and ε (and not L). Assuming the Mumford–Tate conjecture for A, we will show that β_A agrees with the conjectured value of Hindry and Ratazzi.

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

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

holds for all finite extensions L/K, where C is a constant that depends only on A and β (and in particular not L). From Masser, we have $\beta_A \le \dim A$.

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

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

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

Hindry and Ratazzi have proved their conjecture in various situations where the Mumford–Tate conjecture is known and the group G_A is of a very special form [Rat07, HR10, HR12, HR16]. Cantoral Farfán has recently proved several additional cases, see [CF17]. 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

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*

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

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

Date: January 5, 2017.

Remark 1.2.

(i) Our proof of Theorem 1.1 will give the stronger bound $|A(L)_{\mathrm{tors}}| \leq C^{\omega(|A(L)_{\mathrm{tors}}|)}[L:K]^{\gamma_A}$ for all finite extensions L/K, where C is a positive constant that depends only on A and $\omega(|A(L)_{\mathrm{tors}}|)$ is the number of distinct prime divisors of $|A(L)_{\mathrm{tors}}|$.

(ii) In the excluded trivial case $A = 0$, we have $\beta_A = 0$.

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

1.1. **Notations.** For a scheme X over a commutative ring R and an R-algebra S, we will denote by X_S the S-scheme $X_S := X \times_{\operatorname{Spec} R} \operatorname{Spec} S$.

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 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, 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.

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; 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.

We will denote rational primes by ℓ.

1.2. **Overview.** In §2, we give some background on the ℓ-adic representations associated to an abelian variety 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. In §3, we will 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.

Take any prime ℓ. In §4, 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 $|A(L)[\ell^\infty]| \ll_A [L:K]^{\gamma_A}$ (this follows from Proposition 4.1 and Lemma 4.2).

In §5, we prove upper and lower bounds for β_A. We will prove our main theorems in §6; assuming the Mumford–Tate conjecture, the upper and lower bounds for β_A in §5 will agree. Finally in §7, we make some remarks on a conjectural expression for β_A without using Mumford–Tate groups.

2. Abelian variety 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 $A_{\mathbb{C}}$.

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

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

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 $V_i := V_\ell(A_i^{m_i})$.

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 $\mathrm{GL}_V \to \mathrm{GL}_{V_I}$ gives rise to a dominant homomorphism $G_A \to G_{A_I}$ of linear algebraic groups. The kernel of homomorphism $G_A \to G_{A_I}$ 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

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

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

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 $2g$.

Let $\mathrm{GL}_{V_\ell(A)}$ be the group scheme over $\mathbb{Q}_\ell$ such that $\mathrm{GL}_{V_\ell(A)}(R) = \mathrm{Aut}_R(R\otimes_{\mathbb{Q}_\ell} V_\ell(A))$ for each $\mathbb{Q}_\ell$-algebra R. Let $\mathrm{GL}_{T_\ell(A)}$ be the groups scheme over $\mathbb{Z}_\ell$ for which $\mathrm{GL}_{T_\ell(A)}(R) = \mathrm{Aut}_R(R\otimes_{\mathbb{Z}_\ell} T_\ell(A))$ for all $\mathbb{Z}_\ell$-algebras R. We can identify $\mathrm{GL}_{V_\ell(A)}$ with the generic fiber of $\mathrm{GL}_{T_\ell(A)}$.

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

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

The ℓ-adic monodromy group of A, which we denote by $G_{A,\ell}$, is the algebraic subgroup of $\mathrm{GL}_{V_\ell(A)}$ obtained by taking the Zariski closure of $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$.

The group $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ is open in $G_{A,\ell}(\mathbb{Q}_\ell)$, cf. [Bog80]. Therefore, $G_{A,\ell}$ determines the group $\rho_{A,\ell^\infty}(\mathrm{Gal}_K)$ up to commensurability.

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.*

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

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) *The $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell}$ is reductive for $\ell \gg_A 1$.*

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]. □

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 we have $G^\circ_{A,\ell} = (G_A)_{\mathbb{Q}_\ell}$ for a single prime ℓ*

Proof. For a proof of (i), see Deligne's proof in [DMOS82, I, Prop. 6.2]. Part (ii) follows from [LP95, Theorem 4.3]. □

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 [LP95, Theorem 4.3]; in particular, the conjecture holds for one prime ℓ if and only if it holds for all ℓ.

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

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

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

Theorem 2.7. *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 $\mathcal{S}_{A,\ell}$ it 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*

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

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

Proof. This was proved by Serre [Ser00, 138]; see also [Ser13]. □

2.5. **Points modulo ℓ.** Choose a $\mathbb{Z}_\ell$-basis for $T_\ell(A)$, we can then 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. In this section, we sketch the following.

Proposition 2.9. *For any subspace $W \subseteq \mathbb{F}_\ell^{2g}$, we have $|\mathcal{H}_W(\mathbb{F}_\ell)| \asymp_A \ell^{\dim \mathcal{H}_W}$.*

Note that the main content of Proposition 2.9 is that the implicit constants are independent of ℓ. We first state a lemma that can be thought of as bounding the complexity of the neutral component $\mathcal{H}^\circ$ of $\mathcal{H}$ over $\overline{\mathbb{F}}_\ell$.

Lemma 2.10. *Assume that $\mathcal{H}$ is reductive. Let C and S be the central torus and derived subgroup, respectively, of $\mathcal{H}^\circ$. Then the subvarieties $C_{\overline{\mathbb{F}}_\ell}$ and $S_{\overline{\mathbb{F}}_\ell}$ of $\mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell}$ can be both defined by N polynomials in $\overline{\mathbb{F}}_\ell[\{x_{i,j} : 1 \le i,j \le 2g\}]$ with degree at most D, where $N \ll_A 1$ and $D \ll_A 1$.*

Proof. By taking $\ell \gg_A 1$, the group $\mathcal{H}^\circ$ will agree with the reductive group constructed by Serre in [Ser00, 137 p.44] that is denoted $\underline{H}_\ell$; this is proved in [Win02, §3.4.1]. There is a torus $\mathcal{C}$ in $\mathrm{GL}_{2g,\mathbb{Q}}$ for which the central torus of $\underline{H}_\ell$ for $\ell \gg_A 1$ is obtained by reducing $\mathcal{C}$ modulo ℓ, cf. [Ser00, 137 p.43]. This gives the lemma for C.

We may assume that $\ell > 2g$. Define the subgroup $G := \rho_{A,\ell}(\mathrm{Gal}_K)$ of $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$. By Serre's construction, we find that S equals $\widetilde{G}$, where $\widetilde{G}$ is the "exponentially generated" subgroup of $\mathrm{GL}_{2g,\mathbb{F}_\ell}$ generated by G, see [Nor87, Definition 1.3] for a definition of such subgroups. Let G^+ be the subgroup of G generated by its elements of order ℓ; it is a normal subgroup of G with index relatively prime to ℓ. The associated subgroup $\widetilde{G^+}$ of $\mathrm{GL}_{2g,\mathbb{F}_\ell}$ agrees with $\widetilde{G}$.

By taking $\ell \gg_A 1$, the group G acts semisimply on $\mathbb{F}_\ell^{2g}$, cf. [MW95, Corollary 2]. From the proof of Corollary B.4 of [EHK12], the group G^+ also acts semisimply on $\mathbb{F}_\ell^{2g}$. By Theorem B.7 in [EHK12], there is a finite collection $\{\varrho_i \colon \mathbf{G}_i \to \mathrm{GL}_{2g}\}_{i\in I}$ of $\mathbb{Z}$-representations of simply connected Chevalley groups such that for $\ell \gg_A 1$, the subgroup $S_{\overline{\mathbb{F}}_\ell} = \widetilde{G}_{\overline{\mathbb{F}}_\ell}$ of $\mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell}$ is conjugate to the image of ϱ_i over $\overline{\mathbb{F}}_\ell$ for some $i \in I$. The lemma for S is now immediate since the finite collection of representations ϱ_i is independent of ℓ. □

Proof of Proposition 2.9. Let K' be the field $K_{A,\ell}$, which is independent of ℓ, from Proposition 2.3. Replacing A/K be $A_{K'}/K'$ thus changes the index of $\mathcal{H}_W(\mathbb{F}_\ell)$ by at most $[K' : K]$. So without loss of generality, we may assume that the algebraic groups $G_{A,\ell}$ are connected for all ℓ.

By [Nor87, Lemma 3.5], we have $(\ell-1)^{\dim \mathcal{H}_W} \le |\mathcal{H}_W^\circ(\mathbb{F}_\ell)| \le (\ell+1)^{\dim \mathcal{H}_W}$, where $\mathcal{H}_W^\circ$ is the neutral component of $\mathcal{H}_W$. Therefore,

$$(\ell-1)^{\dim \mathcal{H}_W} \le |\mathcal{H}_W^\circ(\mathbb{F}_\ell)| \le m'(\ell+1)^{\dim \mathcal{H}_W},$$

where m' is the number of connected components of $(\mathcal{H}_W)_{\overline{\mathbb{F}}_\ell}$. We have $\dim \mathcal{H}_W \le (2g)^2 \ll_A 1$, so it thus suffices to show that $m' \ll_A 1$.

By Proposition 2.4(ii), we may assume that ℓ is large enough so that $\mathcal{H}$ is connected and reductive. Denote by C and S, the central torus and derived subgroup, respectively, of $\mathcal{H}$. Define the algebraic subgroup $H := C \times S$ of $\mathrm{GL}_{2g,\mathbb{F}_\ell} \times \mathrm{GL}_{2g,\mathbb{F}_\ell}$ and denote by $\varphi \colon H \to \mathcal{H}$ the homomorphism obtained by multiplying matrices. Let H_W be the subvariety of H obtained by taking the inverse image of $\mathcal{H}_W$ under φ. Denote by m the number of irreducible components of $(H_W)_{\overline{\mathbb{F}}_\ell}$. We have $m' \le m$ since φ is dominant. It thus suffices to prove that $m \ll_A 1$.

Fix a prime $p \neq \ell$ and set $d = \dim \mathcal{H}_W$. The connected components $U_1, \dots, U_m$ of $(H_W)_{\overline{\mathbb{F}}_\ell}$ are cosets of $(H_W)^\circ_{\overline{\mathbb{F}}_\ell}$, so they are irreducible, disjoint and all have dimension d. Therefore,

$$H_c^{2d}((H_W)_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_p) = \oplus_{i=1}^m H_c^{2d}(U_i, \mathbb{Q}_p),$$

where we are using étale cohomology with compact support. Each vector space $H_c^{2d}(U_i, \mathbb{Q}_p)$ is 1-dimensional, so m is equal to $h := \dim H_c^{2d}((H_W)_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_p)$. It thus suffices to show that $h \ll_A 1$.

By Lemma 2.10, the subvarieties $C_{\overline{\mathbb{F}}_\ell}$ and $S_{\overline{\mathbb{F}}_\ell}$ of $\mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell}$ can both be defined by N polynomials in $\overline{\mathbb{F}}_\ell[\{x_{i,j} : 1 \le i,j \le 2g\}]$ with degree at most D, where we have $N \ll_A 1$ and $D \ll_A 1$. So there are positive integers $N \ll_A 1$ and $D \ll_A 1$ such that the subvariety $(H_W)_{\overline{\mathbb{F}}_\ell}$ of $\mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell} \times \mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell}$ can be described as the pairs of matrices (X, Y) that are the locus of N particular polynomials in $\overline{\mathbb{F}}_\ell[\{x_{i,j}, y_{i,j} : 1 \le i,j \le 2g\}]$ all of which have degree at most D. By [Kat01, Theorem 1], we find that h can be bounded from above in terms of g, N and D (note that we can identify $\mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell}$ with a closed subvariety of $\mathbb{A}^{4g^2+1}_{\overline{\mathbb{F}}_\ell}$ by identifying a matrix B with a $((2g)^2+1)$-tuple coming from its entries and $\det(B)^{-1}$). In particular, $h \ll_A 1$. □

3. Codimension bounds

Let A be a nonzero abelian variety defined over $\mathbb{C}$. Associated to $A/\mathbb{C}$ is a constant γ_A defined as in §1. The Mumford–Tate group G_A acts on $V := H_1(A(\mathbb{C}), \mathbb{Q})$ and hence $(G_A)_F$ acts on the F-vector space $V \otimes_{\mathbb{Q}} F = H_1(A(\mathbb{C}), F)$ for every extension $F/\mathbb{Q}$. The following theorem will be proved in §3.3 and gives a useful characterization of γ_A.

Theorem 3.1. *Take any 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*

$$\gamma_A \cdot (\dim G - \dim G_W) \ge \dim W. \tag{3.1}$$

Moreover, γ_A is the smallest number for which this holds; equivalently, there is a nonzero subspace $W \subseteq V \otimes_{\mathbb{Q}} F$ for which equality holds in (3.1).

Remark 3.2. We will prove Theorem 3.1 without explicitly computing the integers $\dim G_W$. In the work of Hindry and Ratazzi, for example see [HR12, HR16], they explicitly compute $\dim G_W$ in various cases where the representation of G_A acting on V is of a special form; one can then directly verify Theorem 3.1.

3.1. **Group theory.** Consider a connected reductive group $G \subseteq \mathrm{GL}_V$, where V is a nonzero finite dimensional vector space over a field Q of characteristic 0. Fix an extension F of Q and define the F-vector space $V_F := V \otimes_Q F$. The algebraic group G_F is a connected and reductive subgroup of GL_{V_F}. For each subspace $W \subseteq V_F$, we can define a group $(G_F)_W$ as in §1.1 and a real number

$$\alpha_W := \frac{\dim(G_F) - \dim(G_F)_W}{\dim W}.$$

There are only finitely many possibilities for the numerator and denominator of α_W, so we can define

$$\alpha(F) := \min_{W \neq 0} \alpha_W,$$

where the minimum is over all nonzero subspaces $W \subseteq V_F$.

The following theorem says that $\alpha(F)$ is equal to $\alpha(Q)$ and that $\alpha(Q) = \alpha_W$ for a subspace $W \subseteq V$ of a very special form. Denote by $V = \oplus_{i=1}^n V_i$ the decomposition of the representation V of G into isotypical 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 exists since G is a connected reductive group defined over a field of characteristic 0.

Theorem 3.3. *For each extension F of Q, we have $\alpha(F) = \alpha(Q)$. Moreover,*

$$\alpha(Q) = \min_{\emptyset \neq I \subseteq \{1,\dots,n\}} \alpha_{V_I},$$

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

3.2. **Proof of Theorem 3.3.**

Lemma 3.4. *Let W and W' be nonzero subspaces of V_F that satisfy $\alpha_W = \alpha(F)$ and $\alpha_{W'} = \alpha(F)$. Then $\alpha_{W+W'} = \alpha(F)$.*

Proof. For algebraic groups $H_2 \subseteq H_1$, we define the codimension $\mathrm{codim}_{H_1}(H_2) := \dim H_1 - \dim H_2$.

Let $\mathfrak{g} \subseteq \mathrm{End}(V)$ be the Lie algebra of $G \subseteq \mathrm{GL}_V$. For each subspace W of V, let $\mathfrak{g}_W \subseteq \mathfrak{g}$ be the Lie algebra of G_W; one can verify that $\mathfrak{g}_W$ consists of the $B \in \mathfrak{g}$ for which $Bw = 0$ for all $w \in W$. Of course we have $\dim \mathfrak{g}_W = \dim G_W$.

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

$$\mathrm{codim}_{G_W}(G_{W+W'}) = \dim(\mathfrak{g}_W/\mathfrak{g}_{W+W'}) \leq \dim(\mathfrak{g}_{W\cap W'}/\mathfrak{g}_{W'}) = \mathrm{codim}_{G_{W\cap W'}}(G_{W'}).$$

Therefore,

$$\mathrm{codim}_G(G_{W\cap W'}) + \mathrm{codim}_{G_W}(G_{W+W'}) \leq \mathrm{codim}_G(G_{W\cap W'}) + \mathrm{codim}_{G_{W\cap W'}}(G_{W'}) = \mathrm{codim}_G(G_{W'}). \tag{3.2}$$

We have $\mathrm{codim}_G(G_{W'}) = \alpha_{W'} \dim W' = \alpha(F) \cdot \dim W'$. If $W \cap W' \neq 0$, then $\mathrm{codim}_G(G_{W\cap W'}) = \alpha_{W\cap W'} \dim(W \cap W') \geq \alpha(F) \cdot \dim(W \cap W')$. If $W \cap W' = 0$, then the inequality $\mathrm{codim}_G(G_{W\cap W'}) \geq \alpha(F) \cdot \dim(W \cap W')$ holds trivially. From (3.2), we deduce that

$$\alpha(F) \cdot \dim(W \cap W') + \mathrm{codim}_{G_W}(G_{W+W'}) \leq \alpha(F) \cdot \dim W'$$

and hence $\mathrm{codim}_{G_W}(G_{W+W'}) \leq \alpha(F) \cdot (\dim W' - \dim(W \cap W'))$. We also have $\mathrm{codim}_G G_W = \alpha_W \dim W = \alpha(F) \cdot \dim W$. Therefore,

$$\begin{aligned}
\mathrm{codim}_G(G_{W+W'}) &= \mathrm{codim}_G G_W + \mathrm{codim}_{G_W}(G_{W+W'}) \\
&\leq \alpha(F) \dim W + \alpha(F)(\dim W' - \dim(W \cap W')) \\
&\leq \alpha(F)(\dim W + \dim W' - \dim(W \cap W')) \\
&= \alpha(F) \dim(W + W').
\end{aligned}$$

We have $\mathrm{codim}_G(G_{W+W'}) = \alpha_{W+W'} \dim(W + W')$, so the above inequality implies that $\alpha_{W+W'} \leq \alpha(F)$. By the minimality in the definition of $\alpha(F)$, we must have $\alpha_{W+W'} = \alpha(F)$. □

Lemma 3.5. *For any fields extensions $F \subseteq F'$ of Q, we have $\alpha(Q) \geq \alpha(F) \geq \alpha(F')$.*

Proof. We need only prove $\alpha(F) \geq \alpha(F')$; the other inequality follows by replacing (F, F') by (Q, F). For each nonzero subspace $W \subseteq V_F$, we have $\alpha_W = \alpha_{W \otimes_F F'}$. This implies that $\alpha(F) \geq \alpha(F')$. □

For any extension F' of F, we have $\alpha(Q) \geq \alpha(F) \geq \alpha(F')$ by Lemma 3.5. So to prove that $\alpha(Q) = \alpha(F)$, there is no harm in replacing F by a larger field. We can thus assume that F contains an algebraic closure $\overline{Q}$ of Q.

Let W_0 be a subspace of $V_{\overline{Q}}$ satisfying $\alpha_{W_0} = \alpha(\overline{Q})$ that is maximal with respect to inclusion. By Lemma 3.4, if W is any subspace of $V_{\overline{Q}}$ that satisfies $\alpha_W = \alpha(\overline{Q})$, then $W \subseteq W_0$.

Lemma 3.6.

(i) *We have $\alpha(F) = \alpha(\overline{Q})$.*
(ii) *The subspace W_0 of $V_{\overline{Q}}$ is a representation of $G_{\overline{Q}}$.*

Proof. Let W_1 be a subspace of V_F satisfying $\alpha_{W_1} = \alpha(F)$ that is maximal with respect to inclusion. By Lemma 3.4, if W is a subspace of V_F that satisfies $\alpha_W = \alpha(F)$, then $W \subseteq W_1$.

Take any $g \in G(F)$. We have $G_{gW_1} = gG_{W_1}g^{-1}$, so $\alpha_{gW_1} = \alpha_{W_1} = \alpha(F)$. Since the subspace gW_1 of V_F satisfies $\alpha_{gW_1} = \alpha(F)$, we must have $gW_1 \subseteq W_1$. Therefore, W_1 is stable under the action of $G(F)$ on V_F. The subspace W_1 of V_F is a representation of G_F since $G(\overline{Q}) \subseteq G(F)$ is Zariski dense in G.

Since G is connected and reductive, the action of $G_{\overline{Q}}$ on $V_{\overline{Q}}$ is semisimple and the irreducible representations are geometrically irreducible. Therefore, there is a (nonzero) subspace $W \subseteq V_{\overline{Q}}$ that is a representation of $G_{\overline{Q}}$ and satisfies $W \otimes_{\overline{Q}} F = W_1$. Therefore, $\alpha_W = \alpha_{W \otimes_{\overline{Q}} F} = \alpha_{W_1} = \alpha(F)$. We have

$$\alpha_W \geq \alpha(\overline{Q}) \geq \alpha(F) = \alpha_W,$$

where the second inequality uses Lemma 3.5. Therefore, $\alpha_W = \alpha(\overline{Q}) = \alpha(F)$ which proves (i).

To prove (ii), it suffices to show that $W = W_0$. We have

$$\alpha_{W_0 \otimes_{\overline{Q}} F} = \alpha_{W_0} = \alpha(\overline{Q}) = \alpha(F)$$

and so $W_0 \otimes_{\overline{Q}} F$ is a subspace of $W_1 = W \otimes_{\overline{Q}} F$. In particular, $\dim W_0 \leq \dim W$. We have $W \subseteq W_0$ since W is a subspace of $V_{\overline{Q}}$ satisfying $\alpha_W = \alpha(\overline{Q})$. We deduce that $W = W_0$ since W is a subspace of W_0 and they have the same dimensions. □

The Galois group $\mathrm{Gal}_Q := \mathrm{Gal}(\overline{Q}/Q)$ acts on the group $V_{\overline{Q}} = V \otimes_Q \overline{Q}$ by acting trivially on V and in the usual manner on $\overline{Q}$. With respect to this Galois action, define $\mathcal{W} := W_0^{\mathrm{Gal}_Q}$; it is a subspace of the Q-vector space V.

Lemma 3.7.

(i) *We have $\alpha(\overline{Q}) = \alpha(Q)$.*
(ii) *We have $\alpha_{\mathcal{W}} = \alpha(Q)$. For any nonzero subspace $W \subseteq V$ with $\alpha_W = \alpha(Q)$, we have $W \subseteq \mathcal{W}$.*
(iii) *The space $\mathcal{W}$ is a subrepresentation of the representation V of G.*

Proof. Take any $\sigma \in \mathrm{Gal}_Q$. For each $v \in V_{\overline{Q}}$ and $c \in \overline{Q}$, we have $\sigma(cv) = \sigma(c)\sigma(v)$. We find that $\sigma(W_0)$ and W_0 are $\overline{Q}$-vector spaces of the same dimension; moreover, for a basis $\{v_i\}$ of W_0, $\{\sigma(v_i)\}$ is a basis of $\sigma(W_0)$. Note that a matrix $g \in G(\overline{Q})$ fixes W_0 if and only if $\sigma(g)$ fixes $\sigma(W_0)$. The algebraic groups $(G_{\overline{Q}})_{W_0}$ and $(G_{\overline{Q}})_{\sigma(W_0)}$ over $\overline{Q}$ have the same dimension; moreover, one can be obtained from the other by base changing by the morphism $\mathrm{Spec}\,\overline{Q} \to \mathrm{Spec}\,\overline{Q}$ induced by σ. Therefore, $\alpha_{\sigma(W_0)} = \alpha_{W_0}$ and hence $\alpha_{\sigma(W_0)} = \alpha(\overline{Q})$. By Lemma 3.4, we have $\alpha_{\sigma(W_0)+W_0} = \alpha(\overline{Q})$. By the maximality in the definition of W_0, we find that $\sigma(W_0) \subseteq W_0$ and hence $\sigma(W_0) = W_0$ since they have the same dimension.

Since $\sigma(W_0) = W_0$ for all $\sigma \in \mathrm{Gal}_Q$, we find that $\mathcal{W}$ has the same dimension as W_0 and moreover $W_0 = \mathcal{W} \otimes_Q \overline{Q}$. Therefore, $\alpha_{W_0} = \alpha_{\mathcal{W}}$ and hence $\alpha_{\mathcal{W}} = \alpha(\overline{Q})$. Since $\alpha(Q) \geq \alpha(\overline{Q})$ by Lemma 3.5, we deduce that $\alpha_{\mathcal{W}} = \alpha(\overline{Q}) = \alpha(Q)$. This proves (i).

Now take any nonzero subspace $W \subseteq V$ for which $\alpha_W = \alpha(Q)$. We then have $\alpha_{W \otimes_Q \overline{Q}} = \alpha(Q)$ and hence $W \otimes_Q \overline{Q} \subseteq W_0$ by the maximality in the definition of W_0. Therefore, W is a subspace of $W_0^{\mathrm{Gal}_Q} = \mathcal{W}$.

It remains to show that $\mathcal{W}$ is a subrepresentation of V. It suffices to show that $G(\overline{Q})$ acts on $\mathcal{W} \otimes_Q \overline{Q}$ which is clear by Lemma 3.6 since $W_0 = \mathcal{W} \otimes_Q \overline{Q}$. □

We now finish our proof of Theorem 3.3. We have $\alpha(F) = \alpha(Q)$ by Lemmas 3.6(i) and 3.7(i). It remains to show that $\alpha(Q) = \alpha_{V_I}$ for some nonempty subset $I \subseteq \{1, \dots, n\}$, where $V_I := \oplus_{i \in I} V_i$.

Since G is reductive, Lemma 3.7(iii) implies that $\mathcal{W}$ is a direct sum of irreducible representations of G. In particular, $\mathcal{W} = \oplus_{i=1}^n \mathcal{W}_i$, where $\mathcal{W}_i \subseteq V_i$ is a representation of G. Let I be the set of $1 \le i \le n$ for which $\mathcal{W}_i \neq 0$. The set I is non-empty since $\mathcal{W}$ is non-zero.

Take any $i \in I$. We have $V_i \cong M_i^{n_i}$ and $\mathcal{W}_i \cong M_i^{m_i}$, where M_i is an irreducible representation of G and n_i and m_i are positive integers. Since $G_{\mathcal{W}}$ fixes $\mathcal{W}_i$ (and hence fixes M_i), it must also fix V_i. Therefore, $G_{\mathcal{W}}$ fixes V_I and hence $G_{\mathcal{W}} \subseteq G_{V_I}$. Since $\mathcal{W} \subseteq V_I$, we also have $G_{V_I} \subseteq G_{\mathcal{W}}$ and thus $G_{V_I} = G_{\mathcal{W}}$. From $\mathcal{W} \subseteq V_I$ and $G_{\mathcal{W}} = G_{V_I}$, we have $\alpha_{V_I} \le \alpha_{\mathcal{W}} = \alpha(Q)$. This implies that $\alpha_{V_I} = \alpha(Q)$ by the minimality in the definition of $\alpha(Q)$. This completes our proof of the theorem.

3.3. **Proof of Theorem 3.1.** The representation of G_A on $V = H_1(A(\mathbb{C}), \mathbb{Q})$, up to isomorphism, does not change if we replace A by an isogenous abelian variety. So without loss of generality, we may assume that $A = \prod_{i=1}^n A_i^{m_i}$, where the A_i are simple abelian varieties over $\mathbb{C}$ that are pairwise nonisogenous.

Define $V = H_1(A(\mathbb{C}), \mathbb{Q})$ and $V_i = H_1(A_i^{m_i}(\mathbb{C}), \mathbb{Q})$. We have an isomorphism

$$V = \oplus_{i=1}^n V_i \tag{3.3}$$

of vector spaces. By Lemma 2.2, the direct sum (3.3) is the decomposition of the representation V of G_A into isotypical components. The group G_A is connected and reductive by Lemma 2.1(i). Set $G := (G_A)_F$.

For each nonzero subspace W of V_F, define $\alpha_W := (\dim G - \dim G_W)/\dim W$. Define $\alpha(F) := \min_{W \neq 0} \alpha_W$, where the minimum is over all nonzero subspaces $W \subseteq V_F$.

By Theorem 3.3, we find that

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

where $V_I = \oplus_{i \in I} V_i$. For each subset I of $\{1, \dots, n\}$, define the abelian subvariety $A_I = \prod_{i \in I} A_i^{m_i}$. 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 thus has dimension $2 \dim A_I$. Therefore,

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

So $\alpha(F)$ equals γ_A^{-1} and the theorem is now clear from the definition of $\alpha(F)$.

4. Prime power version

Fix a nonzero abelian variety A of dimension $g \ge 1$ defined over a number field K and fix a prime ℓ.

We claim that $\dim (G_{A,\ell})_W < \dim G_{A,\ell}$ for every nonzero subspaces W of $V_\ell(A)$. On the contrary, suppose that $\dim (G_{A,\ell})_W = \dim G_{A,\ell}$ for some $W \neq 0$. We then have $(G_{A,\ell}^\circ)_W = G_{A,\ell}^\circ$ and hence there is a finite extension K'/K such that $\mathrm{Gal}_{K'}$ acts trivially on W. This in turn would imply that $A(K')[\ell^\infty]$ is infinite which contradicts the Mordell-Weil theorem. So the claim holds.

Define the real number

$$\gamma_{A,\ell} = \min_{W \neq 0} \frac{\dim W}{\dim G_{A,\ell} - \dim (G_{A,\ell})_W}, \tag{4.1}$$

where the minimum is over all nonzero subspaces W of $V_\ell(A)$. We can also characterize $\gamma_{A,\ell}$ as the smallest value for which we have

$$\gamma_{A,\ell} \cdot (\dim G_{A,\ell} - \dim (G_{A,\ell})_W) \ge \dim W \tag{4.2}$$

for all subspaces W of the $\mathbb{Q}_\ell$-vector space $V_\ell(A)$. The goal of this section is to prove the following.

Proposition 4.1. *We have $|A(L)[\ell^\infty]| \le C \cdot [L : K]^{\gamma_{A,\ell}}$ for all finite extensions L/K, where C is a constant that depends only on A.*

For later use, we have stated Proposition 4.1 in an unconditional form. Under the Mumford–Tate conjecture for A, the constant $\gamma_{A,\ell}$ agrees with γ_A and in particular does not depend on ℓ.

Lemma 4.2. *If the Mumford–Tate conjecture holds for A, then $\gamma_{A,\ell} = \gamma_A$.*

Proof. This follows by using the Mumford–Tate conjecture for A (Conjecture 2.5) and Theorem 3.1 with $F = \mathbb{Q}_\ell$. □

We now make some identifications that will hold for the remainder of §4. Choose a basis for $T_\ell(A)$ as a $\mathbb{Z}_\ell$-module; this also gives a basis for $V_\ell(A)$ as a $\mathbb{Q}_\ell$-vector space. We can thus identify $\mathcal{G}_{A,\ell}$ with an algebraic subgroup of $\mathrm{GL}_{2g,\mathbb{Z}_\ell}$ and $G_{A,\ell} = (\mathcal{G}_{A,\ell})_{\mathbb{Q}_\ell}$ with an algebraic subgroup of $\mathrm{GL}_{2g,\mathbb{Q}_\ell}$.

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

$$|A(L)_{\mathrm{tors}}| \le |A(L')_{\mathrm{tors}}| \quad \text{and} \quad [L' : K']^{\gamma_{A,\ell}} \le [K' : K]^{\gamma_{A,\ell}} [L : K]^{\gamma_{A,\ell}} \le [K' : K]^{2\dim A} [L : K]^{\gamma_{A,\ell}} \ll_{A,K'} [L : K]^{\gamma_{A,\ell}}.$$

Also $\gamma_{A,\ell} = \gamma_{A_{K'},\ell}$. So Proposition 4.1 for $A_{K'}/K'$ implies the proposition 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.

4.1. **Filtration.** Let H be a closed subgroup of $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. For each integer $i \ge 1$, let $H(\ell^i)$ and H_i be the image and kernel, respectively, of the reduction modulo ℓ^i homomorphism $H \to \mathrm{GL}_{2g}(\mathbb{Z}/\ell^i\mathbb{Z})$. The map

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

is a 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

$$|H(\ell^i)| = [H : H_i] = [H : H_1] \cdot \prod_{1 \le j < i} [H_j : H_{j+1}] = |H(\ell)| \prod_{1 \le j < i} |\mathfrak{h}_j| = |H(\ell)| \cdot \ell^{\sum_{j=1}^{i-1} \dim \mathfrak{h}_j} \tag{4.3}$$

Lemma 4.3. *Take any integer $i \ge 1$ and suppose that $i \ge 2$ if $\ell = 2$. Then $\mathfrak{h}_i \subseteq \mathfrak{h}_{i+1}$.*

Proof. Take any $I + \ell^i B \in H_i$. It suffices to show that $I + \ell^{i+1} B' \in H_{i+1}$ for some matrix $B' \in M_{2g}(\mathbb{Z}_\ell)$ satisfying $B' \equiv B \pmod{\ell}$. Raising $I + \ell^i B$ to the ℓ-th power gives

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

It suffices to observe that $\binom{\ell}{j} \ell^{ij} \equiv 0 \pmod{\ell^{i+2}}$ for all $2 \le j \le \ell$; this is an easy computation and uses that $\binom{\ell}{j} \equiv 0 \pmod{\ell}$ when $2 \le j < \ell$. □

4.2. **Lie algebras.** Set $\mathcal{G} := \mathcal{G}_{A,\ell}$. Take any $\mathbb{Z}_\ell$-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

$$\mathcal{G}(R[\varepsilon]) \to \mathcal{G}(R). \tag{4.4}$$

Let $L(R)$ be the set of $B \in M_{2g}(R)$ for which $I + \varepsilon B$ lies in the kernel of (4.4). Observe that $L(R)$ is a *Lie algebra* over R; it is an R-submodule of $M_{2g}(R)$ that is closed under the pairing $[B_1, B_2] = B_1 B_2 - B_2 B_1$.

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

Let $\mathfrak{g}$ 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 4.4. *If $\ell \gg_A 1$, then $\mathfrak{g}$ is the Lie algebra of $\mathcal{G}_{\mathbb{F}_\ell}$.*

Proof. By Proposition 2.4, we may take ℓ large enough so that $\mathbb{Z}_\ell$-group scheme $\mathcal{G}$ is reductive. 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 $L(\mathbb{F}_\ell) = \mathfrak{g}$ since we have an inclusion $\mathfrak{g} \subseteq L(\mathbb{F}_\ell)$ of vector spaces of the same dimension. □

Lemma 4.5.

(i) *There is an integer $e \ge 0$, depending on A and ℓ, such that the cokernel of the reduction map $L(\mathbb{Z}_\ell) \to L(\mathbb{Z}/\ell^i\mathbb{Z})$ has cardinality dividing ℓ^e for all $i \ge 1$.*

(ii) *Take any integer $i \geq 1$ and suppose that $i \geq 2$ if $\ell = 2$. If H is a closed subgroup of $\mathcal{G}(\mathbb{Z}_\ell)$, then $\mathfrak{h}_i \subseteq \mathfrak{g}$.*

(iii) *Consider $H = \mathcal{G}(\mathbb{Z}_\ell)$. If $i \gg_A 1$ or $\ell \gg_A 1$, then $\mathfrak{h}_i = \mathfrak{g}$.*

Proof. Let x be the $2g \times 2g$ matrix whose (i,j)-th entry is the variable $x_{i,j}$. Let $\{f_\alpha\}_{\alpha \in I}$ be a finite collection of polynomials in $\mathbb{Z}_\ell[\{x_{i,j}\}_{1 \leq i,j \leq 2g}]$ that cut out the subscheme $\mathcal{G}$ of $\mathrm{GL}_{2g,\mathbb{Z}_\ell}$. For any $\alpha \in I$, we have

$$f_\alpha(I + \varepsilon x) = \sum_{i,j} c_{i,j}^\alpha x_{i,j} \cdot \varepsilon$$

for unique $c_{i,j}^\alpha \in \mathbb{Z}_\ell$. Thus $L(R)$ is the R-module consisting of common solutions $x \in M_{2g}(R)$ to the linear equations $\sum_{i,j} c_{i,j}^\alpha x_{i,j} = 0$ with $\alpha \in I$.

Denote by r the rank of $\mathbb{Z}_\ell$-module $L(\mathbb{Z}_\ell)$. The image of the reduction map $L(\mathbb{Z}_\ell) \to L(\mathbb{Z}/\ell^i\mathbb{Z})$ thus has cardinality ℓ^{ir}. So to prove part (i), it suffices to show that $|L(\mathbb{Z}/\ell^i\mathbb{Z})| \ll \ell^{ir}$, where the implicit constant does not depend on i.

By choosing a basis of the $\mathbb{Z}_\ell$-module $M_{2g}(\mathbb{Z}_\ell)$, we obtain a matrix $T \in M_{m,n}(\mathbb{Z}_\ell)$ (with $m = |I|$ and $n = (2g)^2$) such that we can identify $L(\mathbb{Z}_\ell)$ and $L(\mathbb{Z}/\ell^i\mathbb{Z})$ with the kernel of the homomorphisms $\mathbb{Z}_\ell^n \to \mathbb{Z}_\ell^m$ and $\overline{T}\colon (\mathbb{Z}/\ell^i\mathbb{Z})^n \to (\mathbb{Z}/\ell^i\mathbb{Z})^m$, respectively, defined by T. By changing bases appropriately and using that $\mathbb{Z}_\ell$ is a PID, we may assume that $T(\mathbb{Z}_\ell^n)$ is of the form $\bigoplus_{j=1}^{n-r} \ell^{a_j}\cdot\mathbb{Z}_\ell \oplus \bigoplus_{j=n-r+1}^{m} 0\cdot\mathbb{Z}_\ell \subseteq \mathbb{Z}_\ell^m$ with nonnegative integers a_j. Therefore, $|\operatorname{Im}(\overline{T})| \gg \ell^{i(n-r)}$ and hence

$$|L(\mathbb{Z}/\ell^i\mathbb{Z})| = |\ker(\overline{T})| = |(\mathbb{Z}/\ell^i\mathbb{Z})^n|/|\operatorname{Im}(\overline{T})| \ll \ell^{in}/\ell^{i(n-r)} = \ell^{ir},$$

where the implicit constants do not depend on i. This completes our proof of (i).

We now prove part (ii). With $e \geq 0$ as in part (i), take any integer $n \geq e+1$. Take any element $I + \ell^n B \in H_n$. For each $\alpha \in I$, we have $0 = f_\alpha(I + \ell^n B) \equiv \sum_{i,j} c_{i,j}^\alpha B_{i,j} \cdot \ell^n \pmod{\ell^{2n}}$. Therefore,

$$\sum_{i,j} c_{i,j}^\alpha B_{i,j} \equiv 0 \pmod{\ell^n}$$

and hence B modulo ℓ^n lies in $L(\mathbb{Z}/\ell^n\mathbb{Z})$. By part (i), there is a matrix $C \in L(\mathbb{Z}_\ell)$ such that $\ell^e B \equiv \ell^e C \pmod{\ell^n}$. So $\ell^e B = \ell^e C + \ell^n D$ for a matrix $D \in M_{2g}(\mathbb{Z}_\ell)$. Multiplying by ℓ^{n-e} and adding I gives $I + \ell^n B = I + \ell^n C + \ell^{2n-e} D$. We have $2n - e \geq n+1$ by our choice of n, so $I + \ell^n B \equiv I + \ell^n C \pmod{\ell^{n+1}}$. Therefore, $B \equiv C \pmod{\ell}$ with $C \in L(\mathbb{Z}_\ell)$ and hence B modulo ℓ lies in $\mathfrak{g}$. Since $I + \ell^n B \in H_n$ was arbitrary, this proves that $\mathfrak{h}_n \subseteq \mathfrak{g}$. Since $\mathfrak{h}_n \subseteq \mathfrak{g}$ for all sufficiently large n, part (ii) follows from Lemma 4.3.

We now prove part (iii). Suppose that $\mathfrak{h}_i \neq \mathfrak{g}$ for infinitely many i. By part (ii) and Lemma 4.3, we have $\mathfrak{h}_i \subsetneq \mathfrak{g}$ for all $i \geq 2$. By (4.3), we find that

$$|H(\ell^i)| \ll_{A,\ell} \ell^{i(\dim \mathfrak{g} - 1)} = \ell^{i(\dim G_{A,\ell} - 1)}. \tag{4.5}$$

The group $H = \mathcal{G}(\mathbb{Z}_\ell) = G_{A,\ell}(\mathbb{Q}_\ell) \cap \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ is open in $G_{A,\ell}(\mathbb{Q}_\ell)$. We have $|H(\ell^i)| \gg_{A,\ell} \ell^{i \dim G_{A,\ell}}$; this follows from the more general result [Ser81, Théorème 9]. However, this contradicts (4.5) for i large enough, so we must have $\mathfrak{h}_i = \mathfrak{g}$ for all sufficiently large i.

By excluding a finite number of primes, we can assume by Proposition 2.4 that $\mathcal{G}$ is a reductive group scheme over $\mathbb{Z}_\ell$ and that ℓ is odd. To finish the proof of (iii), it suffices to show that $\mathfrak{h}_i = \mathfrak{g}$ for all $i \geq 1$. By part (ii) and Lemma 4.3, it suffices to show that $\mathfrak{h}_1 \supseteq \mathfrak{g}$.

Take any $\overline{B} \in \mathfrak{g}$ and choose a matrix $B \in M_{2g}(\mathbb{Z}/\ell^2\mathbb{Z})$ for which $B \equiv \overline{B} \pmod{\ell}$. For each $\alpha \in I$, we have $f_\alpha(I + \ell B) \equiv \sum_{i,j} c_{i,j}^\alpha B_{i,j} \cdot \ell \pmod{\ell^2}$. We have $\sum_{i,j} c_{i,j}^\alpha B_{i,j} \equiv 0 \pmod{\ell}$ since $\overline{B} \in \mathfrak{g}$, and thus $f_\alpha(I + \ell B) = 0$ for all $\alpha \in I$. Therefore, $I + \ell B \in \mathcal{G}(\mathbb{Z}/\ell^2\mathbb{Z})$. The reduction map $H = \mathcal{G}(\mathbb{Z}_\ell) \to \mathcal{G}(\mathbb{Z}/\ell^2\mathbb{Z})$ is surjective since $\mathcal{G}$ is smooth over $\mathbb{Z}_\ell$. So there is a matrix $B' \in M_{2g}(\mathbb{Z}_\ell)$ for which $I + \ell B' \in \mathcal{G}(\mathbb{Z}_\ell)$ is congruent to $I + \ell B$ modulo ℓ^2. We have $I + \ell B' \in H_1$ and $B' \equiv B \equiv \overline{B} \pmod{\ell}$, so $\overline{B} \in \mathfrak{h}_1$. Since $\overline{B}$ was an arbitrary element of $\mathfrak{g}$, we deduce that $\mathfrak{g} \subseteq \mathfrak{h}_1$. □

For each subspace W of $\mathbb{F}_\ell^{2g}$, denote by $\mathfrak{g}_W$ the Lie subalgebra of $\mathfrak{g}$ consisting of those $B \in \mathfrak{g}$ that satisfy $Bw = 0$ for all $w \in W$.

Proposition 4.6. *For any subspace W of $\mathbb{F}_\ell^{2g}$, we have $\gamma_{A,\ell}(\dim \mathfrak{g} - \dim \mathfrak{g}_W) \geq \dim W$.*

Proof. Set $\mathfrak{G} = L(\mathbb{Q}_\ell) \subseteq M_{2g}(\mathbb{Q}_\ell)$; it is the Lie algebra of $G_{A,\ell}$. Choose a $\mathbb{Z}_\ell$-submodule $\mathcal{W}$ of $\mathbb{Z}_\ell^{2g}$ whose rank is equal to the dimension of W such that the reduction modulo ℓ map gives a surjection $\mathcal{W} \to W$. Therefore,

$$\dim \mathfrak{g}_W = \operatorname{rank}_{\mathbb{Z}_\ell}\{B \in L(\mathbb{Z}_\ell) | Bw = 0 \text{ for all } w \in \mathcal{W}\} = \dim \mathfrak{G}_{\mathcal{W}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell},$$

where $\mathfrak{G}_{\mathcal{W}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell}$ is the Lie subalgebra of $\mathfrak{G}$ consisting of all $B \in \mathfrak{G}$ that satisfy $Bw = 0$ for all $w \in \mathcal{W}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$. Since $\mathfrak{G}_{\mathcal{W}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell}$ is the Lie algebra of the group $(G_{A,\ell})_{\mathcal{W}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell}$, we deduce that $\dim \mathfrak{g}_W = \dim((G_{A,\ell})_{\mathcal{W}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell})$. Therefore,

$$\dim \mathfrak{g} - \dim \mathfrak{g}_W = \dim G_{A,\ell} - \dim((G_{A,\ell})_{\mathcal{W}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell}).$$

By (4.2), we deduce that $\gamma_{A,\ell}(\dim \mathfrak{g} - \dim \mathfrak{g}_W) = \gamma_{A,\ell}(\dim G_{A,\ell} - \dim((G_{A,\ell})_{\mathcal{W}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell}))$ is greater than or equal to $\dim(\mathcal{W}\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell) = \dim W$. □

We can now approximate the degrees $[K(A[\ell^i]) : K]$.

Lemma 4.7. *For each integer $i \geq 1$, we have $[K(A[\ell^i]) : K] = |\rho_{A,\ell^i}(\mathrm{Gal}_K)| \asymp_A \ell^{i \dim G_{A,\ell}}$.*

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 $[\mathcal{G}(\mathbb{Z}_\ell) : \rho_{A,\ell^\infty}(\mathrm{Gal}_K)] \ll_A 1$. So by Lemma 4.5(iii), we find that if $i \gg_A 1$ or $\ell \gg_A 1$, then $\mathfrak{h}_i = \mathfrak{g}$. By (4.3), we deduce that

$$[K(A[\ell^i]) : K] = |H(\ell^i)| \asymp_A |H(\ell)| \cdot \ell^{(i-1)\dim \mathfrak{g}} = |H(\ell)| \cdot \ell^{(i-1)\dim G_{A,\ell}}.$$

Since $[\mathcal{G}(\mathbb{F}_\ell) : H(\ell)] \ll_A 1$, it suffices to show that $|\mathcal{G}(\mathbb{F}_\ell)| \asymp_A \ell^{\dim G_{A,\ell}}$. By Proposition 2.4, we may assume that ℓ is large enough so that $\mathcal{G}$ is reductive. We have $\dim \mathcal{G}_{\mathbb{F}_\ell} = \dim \mathcal{G}_{\mathbb{Q}_\ell} = \dim G_{A,\ell}$. By Proposition 2.9 (with $W = 0$), we have $|\mathcal{G}(\mathbb{F}_\ell)| \asymp_A \ell^{\dim \mathcal{G}_{\mathbb{F}_\ell}} = \ell^{\dim G_{A,\ell}}$. □

4.3. **Proof of Proposition 4.1.** Fix a finite extension L/K. Define the group $W := A(L)[\ell^\infty]$, i.e., the group of torsion points in $A(L)$ whose order is a power of ℓ. The group $W \subseteq A(L)_{\mathrm{tors}}$ is finite. For each $i \geq 0$, let $W[\ell^i]$ be the group of $P \in W$ 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 $W[\ell^{i+1}]/W[\ell^i]$ with a subgroup of $A[\ell^{i+1}]/A[\ell^i]$, so we can define

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

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

Lemma 4.8. *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 $i \geq 1$, where $i \neq 1$ if $\ell = 2$. Take any $I + \ell^i B \in H_i$. Since $\mathfrak{h}_i \subseteq \mathfrak{g}$ by Lemma 4.5(ii), to prove the claim, we need only show that $Bw = 0$ for every $w \in W_i$. 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 $P \in W[\ell^{i+1}]$ since $W \subseteq A(L)$. Therefore, $I + \ell^i B$ fixes each element of $\psi_i(W[\ell^{i+1}])$. So for each $w \in \psi_i(W[\ell^{i+1}])$, we have $(I + \ell^i B)w = w$ and hence $\ell^i Bw = 0$. Therefore, $Bw \equiv 0 \pmod{\ell}$ for all $w \in \psi_i(W[\ell^{i+1}])$. The claim is now immediate since W_i is the image of $\psi_i(W[\ell^{i+1}]/W[\ell^i])$ modulo ℓ.

Take any $i \geq 1$. By Lemma 4.3 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 $W[\ell] \subseteq A(L)$, 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 2.9, we have $|H(\ell)| \leq |\mathcal{H}_{W_0}(\mathbb{F}_\ell)| \ll_A \ell^{\dim \mathcal{H}_{W_0}}$. Therefore,

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

So it suffices to show that $\dim \mathcal{H}_{W_0} = \dim \mathfrak{g}_{W_0}$ for $\ell \gg_A 1$. By taking ℓ large enough, in terms of A, we may assume that the algebraic group $\mathcal{H}$ has Lie algebra $\mathfrak{g}$ by Lemma 4.4. So $\mathcal{H}_{W_0}$ has Lie algebra $\mathfrak{g}_{W_0}$ and hence $\dim \mathcal{H}_{W_0} = \dim \mathfrak{g}_{W_0}$. □

Take any $i \geq 1$ large enough so that $W[\ell^i] = W = A(L)[\ell^\infty]$. Using $\dim \mathfrak{g} = \dim G_{A,\ell}$ and Lemmas 4.7 and 4.8, we deduce that

$$[L : K] \geq [\rho_{A,\ell^i}(\mathrm{Gal}_K) : \rho_{A,\ell^i}(\mathrm{Gal}_L)] \gg_A \ell^{\sum_{j=0}^{i-1}(\dim \mathfrak{g} - \dim \mathfrak{g}_{W_j})}.$$

Raising both sides to the power $\gamma_{A,\ell}$ gives $[L : K]^{\gamma_{A,\ell}} \gg_A \ell^{\sum_{j=0}^{i-1} \gamma_{A,\ell} \cdot (\dim \mathfrak{g} - \dim \mathfrak{g}_{W_j})}$; note that $\gamma_{A,\ell} \leq 2 \dim A$ and in particular we have $\gamma_{A,\ell} \ll_A 1$. Proposition 4.6 implies that

$$\ell^{\sum_{j=0}^{i-1} \dim W_j} \ll_A [L : K]^{\gamma_{A,\ell}} \tag{4.6}$$

We now compute the series $\sum_{j=0}^{i-1} \dim W_j$. We have

$$\sum_{j=0}^{i-1} \dim W_j = \sum_{j=0}^{i-1} (\log_\ell |W[\ell^{j+1}]| - \log_\ell |W[\ell^j]|) = \log_\ell |W[\ell^i]| - \log_\ell |W[\ell^0]| = \log_\ell |A(L)[\ell^\infty]|,$$

where we have used that the series is telescoping. By (4.6), this gives $|A(L)[\ell^\infty]| \ll_A [L : K]^{\gamma_{A,\ell}}$ which completes our proof of Proposition 4.1.

5. Bounds on 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 5.1. *Let B be an abelian variety over a finite extension K'/K that is isogenous to $A_{K'}$. Then $\beta_A = \beta_B$.*

Proof. Take any finite extension K'/K. We claim that $\beta_{A_{K'}} = \beta_A$. The inequality $\beta_{A_{K'}} \leq \beta_A$ is trivially 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

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

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

Now take any abelian variety B that is isogenous to A. We claim that $\beta_A = \beta_B$; by symmetry, it suffices to prove that $\beta_A \leq \beta_B$. Fix an isogeny $\varphi \colon A \to B$ and denote its degree by d. Take any finite extension L/K. The kernel of the homomorphism $A(L)_{\mathrm{tors}} \to B(L)_{\mathrm{tors}}$ induced by φ has kernel of order at most d and hence $|A(L)_{\mathrm{tors}}| \leq d|B(L)_{\mathrm{tors}}|$. So for any $\varepsilon > 0$, we have $|A(L)_{\mathrm{tors}}| \ll_d |B(L)_{\mathrm{tors}}| \ll_{B,\varepsilon} [L : K]^{\beta_B + \varepsilon}$. This proves that $\beta_A \leq \beta_B$.

The lemma is an immediate consequence of the two claims. □

We now consider bounds for β_A. By Lemma 5.1, there is no harm in replacing A by its base extension by a fixed finite extension of K or by an isogenous abelian variety. So by Proposition 2.8, we may assume that the representations $\{\rho_{A,\ell^\infty}\}_\ell$ are independent. We may also assume that $A = \prod_{i=1}^n A_i^{m_i}$, where the A_i/K are geometrically simple and pairwise geometrically nonisogenous abelian varieties. For each subset $I \subseteq \{1, \ldots, n\}$, define the abelian subvariety $A_I := \prod_{i \in I} A_i^{m_i}$ of A.

We now prove unconditional lower and upper bounds for β_A.

Theorem 5.2. *We have*

$$\max_\ell \left(\max_{\emptyset \neq I \subseteq \{1,\ldots,n\}} \frac{2 \dim A_I}{\dim G_{A_I,\ell}} \right) \leq \beta_A \leq \max_\ell \gamma_{A,\ell},$$

where the maximum is over all primes ℓ.

Proof. We first prove the upper bound for β_A. Define $\xi_A := \max_\ell \gamma_{A,\ell}$. Let J be the set of primes that divide $|A(L)_{\mathrm{tors}}|$. For each $\ell \in J$, define the field $L_\ell := K(A(L)[\ell^\infty])$. Note that the fields $\{L_\ell\}_{\ell\in J}$ are linearly disjoint extensions of K since the representations $\{\rho_{A,\ell^\infty}\}_\ell$ are independent.

By Proposition 4.1, 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

$$|A(L)_{\mathrm{tors}}| = \prod_{\ell\in J} |A(L)[\ell^\infty]| \le C^{|J|} \Big(\prod_{\ell\in J} [L_\ell : K]\Big)^{\xi_A} \le C^{|J|}[L : K]^{\xi_A}, \tag{5.1}$$

where the last inequality uses that the fields L_ℓ are linearly disjoint extensions of K that are subfields of L.

Take any $\varepsilon > 0$ and set $\delta := 1 - 1/(1+\varepsilon/\xi_A)$; we have $0 < \delta < 1$. We have $C^{|J|} \ll_{A,\varepsilon} \prod_{\ell\in J} \ell^\delta \le |A(L)_{\mathrm{tors}}|^\delta$. Using (5.1), 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 the lower bound for β_A. Take any prime ℓ and nonempty subset $I \subseteq \{1, \dots, n\}$.

Take any integer $i \ge 1$ and define the field $L := K(A_I[\ell^i])$. We have $[L : K] \asymp_A \ell^{i \dim G_{A_I,\ell}}$ by Lemma 4.7. For any $\varepsilon > 0$, we have

$$\ell^{i\cdot 2\dim A_I} = |A_I[\ell^i]| \le |A(L)_{\mathrm{tors}}| \ll_{A,\varepsilon} [L : K]^{\beta_A+\varepsilon} \ll_A \ell^{i \dim G_{A_I,\ell}\cdot(\beta_A+\varepsilon)}.$$

Since this holds for all $i \ge 1$ and $\varepsilon > 0$, we have $2\dim A_I \le \dim G_{A_I,\ell}\cdot\beta_A$ and hence $\beta_A \ge 2\dim A_I/\dim G_{A_I,\ell}$. The lower bound follows since the prime ℓ and the nonempty subset $I \subseteq \{1, \dots, n\}$ were arbitrary. □

Remark 5.3. Conjecturally, the two inequalities in Theorem 5.2 are both equalities. Assuming the Mumford–Tate conjecture for A, our proof of Theorem 1.1 will show that the upper and lower bounds of β_A in Theorem 5.2 both equal γ_A.

Corollary 5.4. *We have $\beta_A \ge \gamma_A$.*

Proof. By Proposition 2.6(i), we have $\dim G_{A_I,\ell} \le \dim G_{A_I}$ for all ℓ and $I \subseteq \{1, \dots, n\}$. By Theorem 5.2, we deduce that

$$\beta_A \ge \max_\ell \Big(\max_{\emptyset\ne I\subseteq\{1,\dots,n\}} \frac{2\dim A_I}{\dim G_{A_I,\ell}} \Big) \ge \max_{\emptyset\ne I\subseteq\{1,\dots,n\}} \frac{2\dim A_I}{\dim G_{A_I}} = \gamma_A,$$

where the equality uses that the A_i are simple and pairwise isogenous even after base extending to $\mathbb{C}$. □

6. Proof of Theorems 1.1 and 1.3

First suppose that the Mumford–Tate conjecture for A holds. So for each prime ℓ, we have $\gamma_{A,\ell} = \gamma_A$ by Lemma 4.2. Theorem 5.2 now implies that $\beta_A \le \gamma_A$. We deduce that $\beta_A = \gamma_A$ since $\beta_A \ge \gamma_A$ by Corollary 5.4.

Now suppose that A is geometrically simple and the Mumford–Tate conjecture for A fails. Theorem 5.2 and our geometrically simple assumption implies that

$$\beta_A \ge \max_\ell \Big(\max_{\emptyset\ne I\subseteq\{1,\dots,n\}} \frac{2\dim A_I}{\dim G_{A_I,\ell}} \Big) = \max_\ell \frac{2\dim A}{\dim G_{A,\ell}}$$

and similarly $\gamma_A = 2\dim A/\dim G_A$. Proposition 2.6 (with our assumption that the Mumford–Tate conjecture for A fails) implies that $\dim G_{A,\ell} < \dim G_A$ for all ℓ. Therefore,

$$\beta_A \ge \max_\ell \frac{2\dim A}{\dim G_{A,\ell}} > \frac{2\dim A}{\dim G_A} = \gamma_A.$$

In particular, $\beta_A \ne \gamma_A$.

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 5.1, 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 and pairwise geometrically nonisogenous.

For each prime ℓ, let $\gamma_{A,\ell}$ be the constant defined in §4.

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

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

Note that both sides in Conjecture 7.1 equal γ_A when the Mumford–Tate conjecture for A holds; this uses Lemma 4.2.

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

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

Proof. This is an immediate consequence of Theorem 5.2 and Conjecture 7.1 for A. □

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 7.3. *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 the 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 $n = 1$. By Theorem 3.3, we find that

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

Remark 7.4. Let us briefly sketch why we are currently unable to extend the proof of Proposition 7.3 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 isotypical decomposition of $V_\ell(A)$ as a representation of $G_{A,\ell}$ and that $G_{A,\ell}$ is reductive. Using Theorem 3.3, one can show that

$$\gamma_{A,\ell} = \max_{\mathcal{L} \neq \emptyset} \frac{\dim V_{\mathcal{L}}}{\dim G_{A,\ell} - \dim(G_{A,\ell})_{V_{\mathcal{L}}}}, \tag{7.1}$$

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 (7.1) is obtained with $\mathcal{L} = \{\lambda : \lambda|\ell\}$; this is obvious in the case of Proposition 7.3 where $E = \mathbb{Q}$.

Refeerences

[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

[CF17] Victoria Cantoral Farfán, *Points de torsion sur les variétés abéliennes de type III* (2017). (In preparation). ↑1

[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 ↑2.3

[EHK12] Jordan S. Ellenberg, Chris Hall, and Emmanuel Kowalski, *Expander graphs, gonality, and variation of Galois representations*, Duke Math. J. **161** (2012), no. 7, 1233–1275, DOI 10.1215/00127094-1593272. MR2922374 ↑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. **73** (1983), no. 3, 349–366; ibid. **75** (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz. MR861971 ↑2.2, 7

[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, 3.2

[HR16] ———, *Torsion pour les variétés abéliennes de type I et II*, Algebra Number Theory **10** (2016), no. no. 9, 1845–1891. MR3576113 ↑1, 3.2

[Kat01] Nicholas M. Katz, *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. **7** (2001), no. 1, 29–44, DOI 10.1006/ffta.2000.0303. Dedicated to Professor Chao Ko on the occasion of his 90th birthday. MR1803934 ↑2.5

[LP95] M. Larsen and R. 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] Michael Larsen and Richard Pink, *A connectedness criterion for l-adic Galois representations*, Israel J. Math. **97** (1997), 1–10. MR1441234 (98k:11066) ↑2.2

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

[MW95] D. W. Masser and G. Wüstholz, *Refinements of the Tate conjecture for abelian varieties*, Abelian varieties (Egloffstein, 1993), de Gruyter, Berlin, 1995, pp. 211–223. MR1336608 ↑2.5

[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 ↑2.5

[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) ↑4.2

[Ser00] ———, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000. 1985–1998. MR1730973 (2001e:01037) ↑2.2, 2.4, 2.4, 2.5

[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

[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] J.-P. 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, 2.5