THE SPLITTING OF REDUCTIONS OF AN ABELIAN VARIETY

DAVID ZYWINA

Abstract. Consider an absolutely simple abelian variety A defined over a number field K. For most places v of K, we study how the reduction A_v of A modulo v splits up to isogeny. Assuming the Mumford–Tate conjecture for A and possibly increasing the field K, we will show that A_v is isogenous to the m-th power of an absolutely simple abelian variety for all places v of K away from a set of density 0, where m is an integer depending only on the endomorphism ring $\mathrm{End}(A_{\overline{K}})$. This proves many cases, and supplies justification, of a conjecture of Murty and Patankar. Under the same assumptions, we will also describe the Galois extension of $\mathbb{Q}$ generated by the Weil numbers of A_v for most v.

1. Introduction

Let A be a non-zero abelian variety defined over a number field K. Let Σ_K be the set of finite places of K, and for each place $v \in \Sigma_K$ let $\mathbb{F}_v$ be the corresponding residue field. The abelian variety A has good reduction at all but finitely many places $v \in \Sigma_K$. For a place $v \in \Sigma_K$ for which A has good reduction, the reduction A modulo v is an abelian variety A_v defined over $\mathbb{F}_v$. We know that A_v is isogenous to a product of simple abelian varieties (all defined over $\mathbb{F}_v$). The goal of this paper is study how A_v factors for "almost all" places v, that is, for those v away from a subset of Σ_K with (natural) density 0. In particular, we will supply evidence for the following reformulation of a conjecture of Murty and Patankar [MP08].

Conjecture 1.1 (Murty–Patankar)**.** *Let A be an absolutely simple abelian variety over a number field K. Let $\mathcal{V}$ be the set of finite places v of K for which A has good reduction and $A_v/\mathbb{F}_v$ is simple. Then, after possibly replacing K by a finite extension, the density of $\mathcal{V}$ exists and $\mathcal{V}$ has density 1 if and only if $\mathrm{End}(A_{\overline{K}})$ is commutative.*

The conjecture in [MP08] is stated without the condition that K possibly needs to be replaced by a finite extension. An extra condition is required since one can find counterexamples to the original conjecture. (For example, let $A/\mathbb{Q}$ be the Jacobian of the smooth projective curve defined by the equation $y^2 = x^5 - 1$. We have $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(\zeta_5)$, and in particular A is absolutely simple. For each prime $p \equiv -1 \pmod 5$, the abelian variety A has good reduction at p and A_p is isogenous to E_p^2, where E_p is an elliptic curve over $\mathbb{F}_p$ that satisfies $|E_p(\mathbb{F}_p)| = p+1$. Conjecture 1.1 will hold for A with $K = \mathbb{Q}(\zeta_5)$, equivalently, A_p is simple for all primes $p \equiv 1 \pmod 5$ away from a set of density 0.)

We shall relate Conjecture 1.1 to the arithmetic of the Mumford–Tate group of A, see §2.5 for a definition of this group and §2.6 for a statement of the Mumford–Tate conjecture for A. In our work, we will first replace K by an explicit finite Galois extension K_A^{conn}. The field K_A^{conn} is the smallest extension of K for which all the ℓ-adic monodromy groups associated to A over K_A^{conn} are

2000 *Mathematics Subject Classification.* Primary 14K15; Secondary 11F80.

Key words and phrases. Reductions of abelian varieties, Galois representations.

This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155.

connected, cf. §2.3. We now give an alternative description of this field due to Larsen and Pink [LP95]. For each prime number ℓ, let $A[\ell^\infty]$ be the subgroup of $A(\overline{K})$ consisting of those points whose order is some power of ℓ. Let $K(A[\ell^\infty])$ be the smallest extension of K in $\overline{K}$ over which all the points of $A[\ell^\infty]$ are defined. We then have

$$K_A^{\mathrm{conn}} = \bigcap_\ell K(A[\ell^\infty]).$$

Theorem 1.2. *Let A be an absolutely simple abelian variety defined over a number field K such that $K_A^{\mathrm{conn}} = K$. Define the integer $m = [\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} : E]^{1/2}$ where E is the center of the division algebra $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

- ((i)) *For all $v \in \Sigma_K$ away from a set of density 0, A_v is isogenous to B^m for some abelian variety $B/\mathbb{F}_v$.*
- ((ii)) *Suppose that the Mumford–Tate conjecture for A holds. Then for all $v \in \Sigma_K$ away from a set of density 0, A_v is isogenous to B^m for some absolutely simple abelian variety $B/\mathbb{F}_v$.*

Corollary 1.3. *Let A be an absolutely simple abelian variety defined over a number field K such that $K_A^{\mathrm{conn}} = K$. Let $\mathcal{V}$ be the set of finite places v of K for which A has good reduction and $A_v/\mathbb{F}_v$ is simple. If $\mathrm{End}(A)$ is non-commutative, then $\mathcal{V}$ has density 0. If $\mathrm{End}(A)$ is commutative and the Mumford–Tate conjecture for A holds, then $\mathcal{V}$ has density 1.*

We will observe later that $\mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ when $K_A^{\mathrm{conn}} = K$; so the above corollary shows that Conjecture 1.1 is a consequence of the Mumford–Tate conjecture. Using Theorem 1.2, we will prove the following general version.

Theorem 1.4. *Let A be a non-zero abelian variety defined over a number field K such that $K_A^{\mathrm{conn}} = K$. The abelian variety A is isogenous to $A_1^{n_1} \times \cdots \times A_s^{n_s}$, where the abelian varieties A_i/K are simple and pairwise non-isogenous. For $1 \le i \le s$, define the integer $m_i = [\mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Q} : E_i]^{1/2}$, where E_i is the center of $\mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Q}$.*

Suppose that the Mumford–Tate conjecture for A holds. Then for all places $v \in \Sigma_K$ away from a set of density 0, A_v is isogenous to a product $\prod_{i=1}^s B_i^{m_i n_i}$, where the B_i are absolutely simple abelian varieties over $\mathbb{F}_v$ that are pairwise non-isogenous and satisfy $\dim(B_i) = \dim(A_i)/m_i$.

Observe that the integer s and the pairs (n_i, m_i) from Theorem 1.4 can be determined from the endomorphism ring $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

1.1. **The Galois group of characteristic polynomials.** Let A be a non-zero abelian variety over a number field K. Fix a finite place v of K for which A has good reduction. Let π_{A_v} be the Frobenius endomorphism of A_v and let $P_{A_v}(x)$ be the characteristic polynomial of π_{A_v}. The polynomial $P_{A_v}(x)$ is monic of degree $2 \dim A$ with integral coefficients and can be characterized by the property that $P_{A_v}(n)$ is the degree of the isogeny $n - \pi_{A_v}$ of A_v for each integer n.

Let $\mathcal{W}_{A_v}$ be the set of roots of $P_{A_v}(x)$ in $\overline{\mathbb{Q}}$. Honda–Tate theory shows that A_v is isogenous to a power of a simple abelian variety if and only if $P_{A_v}(x)$ is a power of an irreducible polynomial; equivalently, if and only if the action of $\mathrm{Gal}_{\mathbb{Q}}$ on $\mathcal{W}_{A_v}$ is transitive.

The following theorem will be important in the proof of Theorem 1.2. Let $\mathbf{G}_A$ be the Mumford–Tate group of A; it is a reductive group over $\mathbb{Q}$ which we will recall in §2.5. Let $W(\mathbf{G}_A)$ be the Weyl group of $\mathbf{G}_A$. We define the splitting field $k_{\mathbf{G}_A}$ of $\mathbf{G}_A$ to be the intersection of all the subfields $L \subseteq \overline{\mathbb{Q}}$ for which the group $\mathbf{G}_{A,L}$ is split.

Theorem 1.5. *Let A be an absolutely simple abelian variety over a number field K that satisfies $K_A^{\mathrm{conn}} = K$. Assume that the Mumford–Tate conjecture for A holds and let L be a finite extension of $k_{\mathbf{G}_A}$. Then*

$$\mathrm{Gal}(L(\mathcal{W}_{A_v})/L) \cong W(\mathbf{G}_A).$$

for all places $v \in \Sigma_K$ away from a set of density 0.

Moreover, we expect the following conjecture to hold.

Conjecture 1.6. *Let A be a non-zero abelian variety over a number field K that satisfies $K_A^{\mathrm{conn}} = K$. There is a group $\Pi(\mathbf{G}_A)$ such that $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A_v})/\mathbb{Q}) \cong \Pi(\mathbf{G}_A)$ for all $v \in \Sigma_K$ away from a set with natural density 0.*

We shall later on give an explicit candidate for the group $\Pi(\mathbf{G}_A)$; it has $W(\mathbf{G}_A)$ as a normal subgroup. We will also prove the conjecture in several cases, cf. §8.

1.2. **Some previous results.** We briefly recall a few earlier known cases of Theorems 1.2 and 1.5.

Let A be an abelian variety over a number field K such that $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$ and such that $2\dim(A)$ is not a k-th power and not of the form $\binom{2k}{k}$ for every odd $k > 1$. Under these assumptions, Pink has shown that $\mathbf{G}_A$ is isomorphic to $\mathbf{GSp}_{2\dim(A),\mathbb{Q}}$ and that the Mumford–Tate conjecture for A holds [Pin98, Theorem 5.14]. We will have $K_A^{\mathrm{conn}} = K$, so Theorem 1.2 says that $A_v/\mathbb{F}_v$ is absolutely simple for all places $v \in \Sigma_K$ away from a set of density 0. We have $k_{\mathbf{G}_A} = \mathbb{Q}$ since $\mathbf{G}_A$ is split, so Theorem 1.5 implies that $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A_v})/\mathbb{Q})$ is isomorphic to the Weyl group $W(\mathbf{GSp}_{2\dim(A),\mathbb{Q}}) = W(\mathbf{Sp}_{2\dim(A),\mathbb{Q}}) \cong W(C_{\dim(A)})$ for all $v \in \Sigma_K$ away from a set of density 0. These results are due to Chavdarov [Cha97, Cor. 6.9] in the special case where $\dim(A)$ is 2, 6 or odd (these dimensions are used to cite a theorem of Serre which gives a mod ℓ version of Mumford–Tate).

Now consider the case where A is an absolutely simple CM abelian variety defined over a number field K; so $F := \mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a number field that satisfies $[F : \mathbb{Q}] = 2\dim(A)$. After replacing K by a finite extension, we may assume that $F = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. We have $\mathbf{G}_A \cong \mathrm{Res}_{F/\mathbb{Q}}(\mathbb{G}_{m,F})$, where $\mathrm{Res}_{F/\mathbb{Q}}$ denotes restriction of scalars from F to $\mathbb{Q}$. The theory of complex multiplication shows that A satisfies the Mumford–Tate conjecture and hence Theorem 1.2 says that $A_v/\mathbb{F}_v$ is absolutely simple for almost all places $v \in \Sigma_K$; this is also [MP08, Theorem 3.1] where it is proved using L-functions and Hecke characters. Theorem 1.5 is not so interesting in this case since $W(\mathbf{G}_A) = 1$.

Several cases of Theorem 1.2 were proved by J. Achter [Ach09, Ach11]; for example, those abelian varieties A/K such that $F := \mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a totally real number field and $\dim(A)/[F : \mathbb{Q}]$ is odd. A key ingredient is some of the known cases of the Mumford–Tate conjecture from the papers [Vas08], [BGK06] and [BGK10]. Achter's approach is very similar to this paper and boils down to showing that $P_{A_v}(x)$ is an appropriate power of an irreducible polynomial for almost all places $v \in \Sigma_K$. In the case where $\mathrm{End}(A_{\overline{K}})$ is commutative, Achter uses the basic property that if $P_{A_v}(x) \bmod \ell$ is irreducible in $\mathbb{F}_\ell[x]$, then $P_{A_v}(x)$ is irreducible in $\mathbb{Z}[x]$; unfortunately, this approach will not work for all absolutely simple abelian varieties A/K for which $K_A^{\mathrm{conn}} = K$ and $\mathrm{End}(A_{\overline{K}})$ is commutative (see §8.1 for an example). Corollary 1.6 in the non-commutative case also follows from [Ach09, Theorem B].

1.3. **Overview.** We set some notation. The symbol ℓ will always denote a rational prime. If X is a scheme over a ring R and we have a ring homomorphism $R \to R'$, then we denote by $X_{R'}$ the scheme $X \times_{\mathrm{Spec}\, R} \mathrm{Spec}\, R'$ over R'. The homomorphism is implicit in the notation; it will usually be a natural inclusion or quotient homomorphism; for example, $\mathbb{Q} \to \mathbb{Q}_\ell$, $\mathbb{Z}_\ell \to \mathbb{Q}_\ell$, $\mathbb{Z}_\ell \to \mathbb{F}_\ell$, $K \hookrightarrow \overline{K}$. For a field K, we will denote by $\overline{K}$ a fixed algebraic closure and define the absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$.

For a number field K, a topological ring R and a finitely generated R-module M, consider a Galois representation $\rho\colon \mathrm{Gal}_K \to \mathrm{Aut}_R(M)$; our representations will always be continuous (for finite R, we always use the discrete topology). If v is a finite place of K for which ρ is unramified, then we denote by $\rho(\mathrm{Frob}_v)$ the conjugacy class of $\rho(\mathrm{Gal}_K)$ arising from the Frobenius automorphism

at v.

Let A be a non-zero abelian variety over a number field K that satisfies $K_A^{\mathrm{conn}} = K$. Fix an embedding $K \subseteq \mathbb{C}$. In §2, we review the basics about the ℓ-adic representations arising from the action of Gal_K on the ℓ-power torsion points of A. To each prime ℓ, we will associate an algebraic group $\mathbf{G}_{A,\ell}$ over $\mathbb{Q}_\ell$. Conjecturally, the connected components of the groups $\mathbf{G}_{A,\ell}$ are isomorphic to the base extension of a certain reductive group $\mathbf{G}_A$ defined over $\mathbb{Q}$; this is the Mumford–Tate group of A. The group $\mathbf{G}_A$ comes with a faithful action on $H_1(A(\mathbb{C}), \mathbb{Q})$. In §3, we review some facts about reductive groups and in particular define the group $\Pi(\mathbf{G}_A)$ of Conjecture 1.6.

Let us hint at how Theorems 1.2 and 1.5 are connected; further details will be supplied later. For the sake of simplicity, suppose that $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$. Fix a maximal torus $\mathbf{T}$ of $\mathbf{G}_A$ and a number field L for which $\mathbf{T}_L$ is split. Let $X(\mathbf{T})$ be the group of characters of $\mathbf{T}_{\overline{\mathbb{Q}}}$ and let $\Omega \subseteq X(\mathbf{T})$ be the set of weights arising from the representation of $\mathbf{T} \subseteq \mathbf{G}_A$ on $H_1(A(\mathbb{C}), \mathbb{Q})$. The Weyl group $W(\mathbf{G}_A, \mathbf{T})$ has a natural faithful action on the set Ω.

Using the geometry of $\mathbf{G}_A$ and our additional assumption $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$, one can show that action of $W(\mathbf{G}_A, \mathbf{T})$ on Ω is transitive. Assuming the Mumford–Tate conjecture, we will show that for all $v \in \Sigma_K$ away from a set of density 0 there is a bijection $\mathcal{W}_{A_v} \leftrightarrow \Omega$ such that the action of Gal_L on $\mathcal{W}_{A_v}$ corresponds with the action of some subgroup of $W(\mathbf{G}_A, \mathbf{T})$ on Ω (this will be described in §6.2 and it makes vital use of a theorem of Noot described in §4). So for almost all $v \in \Sigma_K$, we find that $\mathrm{Gal}(L(\mathcal{W}_{A_v})/L)$ is isomorphic to a subgroup of $W(\mathbf{G}_A, \mathbf{T})$. If $\mathrm{Gal}(L(\mathcal{W}_{A_v})/L)$ is isomorphic to $W(\mathbf{G}_A, \mathbf{T})$, then we deduce that Gal_L acts transitively on $\mathcal{W}_{A_v}$ and hence $P_{A_v}(x)$ is a power of an irreducible polynomial. The assumption $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$ also ensures that $P_{A_v}(x)$ is separable for almost all v, and thus we deduce that $P_{A_v}(x)$ is almost always irreducible (and hence A_v is almost always simple). To show that $\mathrm{Gal}(L(\mathcal{W}_{A_v})/L)$ is maximal for all $v \in \Sigma_K$ away from a set of density 0, we will use a version of Jordan's lemma with some local information from §5.

The proof of Theorem 1.4 can be found in §7; it is easily reduced to the absolutely simple case. In §8 we discuss Conjecture 1.6 further and give an extended example. Finally, we will prove effective versions of Theorems 1.2 and 1.5 in §9.

2. Abelian varieties and Galois representations: background

Starting in §2.2, we fix a non-zero abelian variety A defined over a number field K. In this section, we review some theory concerning the ℓ-adic representations associated to A. In particular, we will define the Mumford–Tate group of A and state the Mumford–Tate conjecture. For basics on abelian varieties, see [Mil86]. The papers [Ser77] and [Ser94] supply overviews of several motivic conjectures for A and how they conjecturally relate with its ℓ-adic representations.

2.1. **Characteristic polynomials.** Fix a finite field $\mathbb{F}_q$ with cardinality q. Let B be a non-zero abelian variety defined over $\mathbb{F}_q$ and let π_B be the Frobenius endomorphism of B. The characteristic polynomial of B is the unique polynomial $P_B(x) \in \mathbb{Z}[x]$ for which the isogeny $n - \pi_B$ of B has degree $P_B(n)$ for all integers n. The polynomial $P_B(x)$ is monic of degree $2 \dim B$. We define $\mathcal{W}_B$ to be the set of roots of $P_B(x)$ in $\overline{\mathbb{Q}}$. The elements of $\mathcal{W}_B$ are algebraic integers with absolute value $q^{1/2}$ under any embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. We define Φ_B to be the subgroup of $\overline{\mathbb{Q}}^\times$ generated by $\mathcal{W}_B$.

The following lemma says that, under some additional conditions, the factorization of $P_B(x)$ into irreducible polynomials corresponds to the factorization of B into simple abelian varieties.

Lemma 2.1. *Let B be a non-zero abelian variety defined over $\mathbb{F}_p$, where p is a prime. Assume that $P_B(x)$ is not divisible by $x^2 - p$. If $P_B(x) = \prod_{i=1}^s Q_i(x)^{m_i}$, where the $Q_i(x)$ are distinct monic*

irreducible polynomials in $\mathbb{Z}[x]$*, then* B *is isogenous to* $\prod_{i=1}^{s} B_i^{m_i}$*, where* B_i *is a simple abelian variety over* $\mathbb{F}_p$ *satisfying* $P_{B_i}(x) = Q_i(x)$*.*

Proof. This is a basic application of Honda–Tate theory; see [WM71]. We know that B is isogenous to $\prod_{i=1}^{t} B_i^{n_i}$, where the $B_i/\mathbb{F}_p$ are simple and pairwise non-isogenous. We have $P_B(x) = \prod_{i=1}^{t} P_{B_i}(x)^{n_i}$. Honda–Tate theory says that $P_{B_i}(x) = Q_i(x)^{e_i}$ where the $Q_i(x)$ are distinct irreducible monic polynomials in $\mathbb{Z}[x]$ and the e_i are positive integers. After possibly reordering the B_i, we have the factorization of $P_B(x)$ in the statement of the lemma with $m_i = n_i e_i$ and $s = t$. It thus suffices to show that $e_i = 1$ for $1 \le i \le t$.

Fix $1 \le i \le t$. Since B_i is simple, the ring $E := \mathrm{End}(B_i) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division algebra with center $\Phi := \mathbb{Q}(\pi_{B_i})$. By Waterhouse and Milne [WM71, I. Theorem 8], we have $e_i = [E : \Phi]^{1/2}$. If the number field Φ has a real place, then $\pi_{B_i} = \pm p^{1/2}$ since $|\pi_{B_i}| = p^{1/2}$. However, if $\pi_{B_i} = \pm p^{1/2}$, then $x^2 - p$ divides $P_{B_i}(x) \in \mathbb{Q}[x]$. So by our assumption that $x^2 - p$ does not divide $P_B(x)$, we conclude that Φ has no real places. Using that $\mathbb{Q}(\pi_{B_i})$ has no real places and $\mathbb{F}_p$ has prime cardinality, [Wat69, Theorem 6.1] implies that E is commutative and hence $e_i = [E : \Phi]^{1/2} = 1$. □

2.2. **Galois representations.** For each positive integer m, let $A[m]$ be the m-torsion subgroup of $A(\overline{K})$; it is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $2 \dim A$. For a fixed rational prime ℓ, let $T_\ell(A)$ be the inverse limit of the groups $A[\ell^e]$ where the transition maps are multiplication by ℓ. We call $T_\ell(A)$ the Tate module of A at ℓ; it is a free $\mathbb{Z}_\ell$-module of rank $2 \dim A$. Define $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. There is a natural action of Gal_K on the groups $A[m]$, $T_\ell(A)$, and $V_\ell(A)$. Let

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

be the Galois representation which describes the Galois action on the $\mathbb{Q}_\ell$-vector space $V_\ell(A)$.

Fix a finite place v of K for which A has good reduction. Denote by A_v the abelian variety over $\mathbb{F}_v$ obtained by reducing A modulo v. If $v \nmid \ell$, then $\rho_{A,\ell}$ is unramified at v and satisfies

$$P_{A_v}(x) = \det(xI - \rho_{A,\ell}(\mathrm{Frob}_v))$$

where $P_{A_v}(x) \in \mathbb{Z}[x]$ is the degree $2 \dim A$ monic polynomial of §2.1. Furthermore, $\rho_{A,\ell}(\mathrm{Frob}_v)$ is the conjugacy class of a semisimple element of $\mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) \cong \mathbf{GL}_{2\dim A}(\mathbb{Q}_\ell)$.

2.3. **ℓ-adic monodromy groups.** Let $\mathbf{GL}_{V_\ell(A)}$ be the algebraic group defined over $\mathbb{Q}_\ell$ for which $\mathbf{GL}_{V_\ell(A)}(L) = \mathrm{Aut}_L(L \otimes_{\mathbb{Q}_\ell} V_\ell(A))$ for all field extensions $L/\mathbb{Q}_\ell$. The image of $\rho_{A,\ell}$ lies in $\mathbf{GL}_{V_\ell(A)}(\mathbb{Q}_\ell)$. Let $\mathbf{G}_{A,\ell}$ be the Zariski closure in $\mathbf{GL}_{V_\ell(A)}$ of $\rho_{A,\ell}(\mathrm{Gal}_K)$; it is an algebraic subgroup of $\mathbf{GL}_{V_\ell(A)}$ called the ℓ-adic algebraic monodromy group of A. Denote by $\mathbf{G}^\circ_{A,\ell}$ the identity component of $\mathbf{G}_{A,\ell}$.

Let K_A^{conn} be the fixed field in $\overline{K}$ of $\rho_{A,\ell}^{-1}(\mathbf{G}^\circ_{A,\ell}(\mathbb{Q}_\ell))$; it is a finite Galois extension of K that does not depend on ℓ, cf. [Ser00, 133 p.17]. Thus, for any finite extension L of K_A^{conn} in $\overline{K}$, the group $\rho_{A,\ell}(\mathrm{Gal}(\overline{K}/L))$ is Zariski dense in $\mathbf{G}^\circ_{A,\ell}$ (equivalently, $\mathbf{G}_{A_L,\ell} = \mathbf{G}^\circ_{A,\ell}$). We have $K_A^{\mathrm{conn}} = K$ if and only if all the ℓ-adic monodromy groups $\mathbf{G}_{A,\ell}$ are connected.

Proposition 2.2. *Assume that* $K_A^{\mathrm{conn}} = K$*.*

((i)) *The commutant of* $\mathbf{G}_{A,\ell}$ *in* $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ *is naturally isomorphic to* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$*.*

((ii)) *The group* $\mathbf{G}_{A,\ell}$ *is reductive.*

((iii)) *We have* $\mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$*.*

Proof. Faltings proved that the representation $\rho_{A,\ell}$ is semisimple and that the natural homomorphism

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

is an isomorphism, cf. [Fal86, Theorems 3–4]. So the commutant of $\mathbf{G}_{A,\ell}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ equals $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. It easily follows that $\mathbf{G}_{A,\ell}$ is reductive.

Let L be a finite extension of K for which $\mathrm{End}(A_{\overline{K}}) = \mathrm{End}(A_L)$. Since $\mathbf{G}_{A_L,\ell} = \mathbf{G}_{A,\ell}$, we obtain an isomorphism between their commutants; $\mathrm{End}(A_L) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$. By comparing dimensions, we find that the injective map $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \to \mathrm{End}(A_L) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an isomorphism. □

The following result of Bogomolov [Bog80, Bog81] says that the image of $\rho_{A,\ell}$ in $\mathbf{G}_{A,\ell}$ is large.

Proposition 2.3. *The group $\rho_{A,\ell}(\mathrm{Gal}_K)$ is an open subgroup of $\mathbf{G}_{A,\ell}(\mathbb{Q}_\ell)$ with respect to the ℓ-adic topology.*

Using that $\rho_{A,\ell}(\mathrm{Gal}_K)$ is an open and compact subgroup of $\mathbf{G}_{A,\ell}(\mathbb{Q}_\ell)$, we find that the algebraic group $\mathbf{G}_{A,\ell}$ describes the image of $\rho_{A,\ell}$ up to commensurability. For each place $v \in \Sigma_K$ for which A has good reduction, we have a group Φ_{A_v} as defined in §2.1.

Proposition 2.4. *Assume that $K_A^{\mathrm{conn}} = K$.*

((i)) *The rank of the reductive group $\mathbf{G}_{A,\ell}$ does not depend on ℓ.*

((ii)) *Let r be the common rank of the groups $\mathbf{G}_{A,\ell}$. Then the set of $v \in \Sigma_K$ for which Φ_{A_v} is a free abelian group of rank r has density 1.*

Proof. Fix a prime ℓ. For a place v where A has good reduction, let $\mathbf{T}_v$ be the Zariski closure in $\mathbf{G}_{A,\ell}$ of the subgroup generated by a fixed (semisimple) element in the conjugacy class $\rho_{A,\ell}(\mathrm{Frob}_v)$. The set of places v for which $\mathbf{T}_v$ is a maximal torus of $\mathbf{G}_{A,\ell}$ has density 1; this follows from [LP97a, Theorem 1.2]. Observe that $\mathbf{T}_v$ is a maximal torus of $\mathbf{G}_{A,\ell}$ if and only if Φ_{A_v} (the multiplicative group generated by the eigenvalues of $\rho_{A,\ell}(\mathrm{Frob}_v)$) is a free abelian group whose rank equals the reductive rank of $\mathbf{G}_{A,\ell}$. Parts (i) and (ii) follow since the rank of Φ_{A_v} does not depend on ℓ. □

2.4. **The set $\mathcal{S}_A$.** We define $\mathcal{S}_A$ to be the set of places $v \in \Sigma_K$ that satisfy the following conditions:

- A has good reduction at v;
- $\mathbb{F}_v$ has prime cardinality;
- Φ_{A_v} is a free abelian group whose rank equals the common rank of the groups $\mathbf{G}_{A,\ell}$.

Using Proposition 2.4(ii), $\mathcal{S}_A$ has density 1 if $K_A^{\mathrm{conn}} = K$. Since we are willing to exclude a set of places with density 0 from our main theorems, it will suffice to restrict our attention to the places $v \in \mathcal{S}_A$.

2.5. **The Mumford–Tate group.** Fix a field embedding $K_A^{\mathrm{conn}} \subseteq \mathbb{C}$. The homology group $V = H_1(A(\mathbb{C}), \mathbb{Q})$ is a vector space of dimension $2 \dim A$ over $\mathbb{Q}$. It is naturally endowed with a $\mathbb{Q}$-Hodge structure of type $\{(-1,0),(0,-1)\}$, and hence a decomposition

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

such that $V^{0,-1} = \overline{V^{-1,0}}$. Let

$$\mu \colon \mathbb{G}_{m,\mathbb{C}} \to \mathbf{GL}_{V \otimes_{\mathbb{Q}} \mathbb{C}}$$

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 $z \in \mathbb{C}^\times = \mathbb{G}_m(\mathbb{C})$.

Definition 2.5. *The Mumford–Tate group of A is the smallest algebraic subgroup of $\mathbf{GL}_V$, defined over $\mathbb{Q}$, which contains $\mu(\mathbb{G}_{m,\mathbb{C}})$. We shall denote it by $\mathbf{G}_A$.*

The endomorphism ring $\mathrm{End}(A_{\mathbb{C}})$ acts on V; this action preserves the Hodge decomposition, and hence commutes with μ and thus also $\mathbf{G}_A$. Moreover, the ring $\mathrm{End}(A_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is naturally isomorphic to the commutant of $\mathbf{G}_A$ in $\mathrm{End}_{\mathbb{Q}}(V)$. The group $\mathbf{G}_A/\mathbb{Q}$ is reductive since the $\mathbb{Q}$-Hodge structure for V is pure and polarizable. Using our fixed embedding $K_A^{\mathrm{conn}} \subseteq \mathbb{C}$ and Proposition 2.2(iii), we have a natural isomorphism $\mathrm{End}(A_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}(A_{K_A^{\mathrm{conn}}}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

2.6. **The Mumford–Tate conjecture.** The comparison isomorphism $V_\ell(A) \cong V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ induces an isomorphism $\mathbf{GL}_{V_\ell(A)} \cong \mathbf{GL}_{V,\mathbb{Q}_\ell}$. The following conjecture says that $\mathbf{G}^\circ_{A,\ell}$ and $\mathbf{G}_{A,\mathbb{Q}_\ell}$ are the same algebraic group when we use the comparison isomorphism as an identification, cf. [Ser77, §3].

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

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. The Mumford–Tate conjecture for A holds if and only if the common rank of the groups $\mathbf{G}^\circ_{A,\ell}$ equals the rank of $\mathbf{G}_A$ [LP95, Theorem 4.3]; in particular, the conjecture holds for one prime ℓ if and only if it holds for all ℓ. The following proposition says that one inclusion of the Mumford–Tate conjecture is known unconditionally, see Deligne's proof in [DMOS82, I, Prop. 6.2].

Proposition 2.7. *For each prime ℓ, we have $\mathbf{G}^\circ_{A,\ell} \subseteq \mathbf{G}_{A,\mathbb{Q}_\ell}$.*

Using this proposition, we obtain a well-defined Galois representation $\rho_{A,\ell}\colon \mathrm{Gal}_{K_A^{\mathrm{conn}}} \to \mathbf{G}_A(\mathbb{Q}_\ell)$ for each prime ℓ.

2.7. **A conjecture on Frobenius conjugacy classes.** Let R be the affine coordinate ring of $\mathbf{G}_A$. The group $\mathbf{G}_A$ acts on R by composition with inner automorphisms (more precisely, $\mathbf{G}_A(k)$ acts on $R \otimes_{\mathbb{Q}} k$ for each extension $k/\mathbb{Q}$). We define $R^{\mathbf{G}_A}$ to be the $\mathbb{Q}$-subalgebra of R consisting of those elements fixed by this $\mathbf{G}_A$-action; it is the algebra of central functions on $\mathbf{G}_A$. Define $\mathrm{Conj}(\mathbf{G}_A) := \mathrm{Spec}(R^{\mathbf{G}_A})$; it is a variety over $\mathbb{Q}$ which we call the variety of (semi-simple) conjugacy classes of $\mathbf{G}_A$. We define $\mathrm{cl}_{\mathbf{G}_A}\colon \mathbf{G}_A \to \mathrm{Conj}(\mathbf{G}_A)$ to be the morphism arising from the inclusion $R^{\mathbf{G}_A} \hookrightarrow R$ of $\mathbb{Q}$-algebras.

Let L be an algebraically closed extension of $\mathbb{Q}$. Each $g \in \mathbf{G}_A(L)$ can be expressed uniquely in the form $g_s g_u$ with commuting $g_s, g_u \in \mathbf{G}_A(L)$ such that g_s is semisimple and g_u is unipotent. For $g, h \in \mathbf{G}_A(L)$, we have $g_s = h_s$ if and only if $\mathrm{cl}_{\mathbf{G}_A}(g) = \mathrm{cl}_{\mathbf{G}_A}(h)$.

Assume that $K_A^{\mathrm{conn}} = K$. We can then view $\rho_{A,\ell}$ as having image in $\mathbf{G}_A(\mathbb{Q}_\ell)$. The following conjecture says that the conjugacy class of $\mathbf{G}_A$ containing $\rho_{A,\ell}(\mathrm{Frob}_v)$ does not depend on ℓ; see [Ser94, C.3.3] for a more refined version.

Conjecture 2.8. *Suppose that $K_A^{\mathrm{conn}} = K$. Let v be a finite place of K for which A has good reduction. Then there exists an $F_v \in \mathrm{Conj}(\mathbf{G}_A)(\mathbb{Q})$ such that $\mathrm{cl}_{\mathbf{G}_A}(\rho_{A,\ell}(\mathrm{Frob}_v)) = F_v$ for all primes ℓ satisfying $v \nmid \ell$.*

Remark 2.9. The algebra of class functions of $\mathbf{GL}_V$ is $\mathbb{Q}[a_1, \ldots, a_n]$ where the a_i are the morphisms of $\mathbf{GL}_V$ that satisfy $\det(xI - g) = x^n + a_1(g)x^{n-1} + \ldots + a_{n-1}(g)x + a_n(g)$ for $g \in \mathbf{GL}_V(\mathbb{Q})$. The inclusion $\mathbf{G}_A \subseteq \mathbf{GL}_V$ induces a morphism $f\colon \mathrm{Conj}(\mathbf{G}_A) \to \mathrm{Conj}(\mathbf{GL}_V) := \mathrm{Spec}\,\mathbb{Q}[a_1, \ldots, a_n] \cong \mathbb{A}^n_{\mathbb{Q}}$. The morphism $f \circ \mathrm{cl}_{\mathbf{G}_A}$ can thus be viewed as mapping an element of $\mathbf{G}_A$ to its characteristic polynomial.

Let v be a finite place of K for which A has good reduction. Conjecture 2.8 implies that for any prime ℓ satisfying $v \nmid \ell$, $f(\mathrm{cl}_{\mathbf{G}_A}(\rho_{A,\ell}(\mathrm{Frob}_v)))) = f(F_v)$ belongs to $\mathrm{Conj}(\mathbf{GL}_V)(\mathbb{Q})$ and is independent of ℓ; this consequence is true, and is just another way of saying that $\det(xI - \rho_{A,\ell}(\mathrm{Frob}_v))$ has coefficients in $\mathbb{Q}$ and is independent of ℓ.

In §4, we will state a theorem of Noot that gives a weakened version of Conjecture 2.8.

2.8. **Image modulo ℓ.** Let $\mathbf{GL}_{T_\ell(A)}$ be the group scheme over $\mathbb{Z}_\ell$ for which $\mathbf{GL}_{T_\ell(A)}(R) = \mathrm{Aut}_R(R \otimes_{\mathbb{Z}_\ell} T_\ell(A))$ for all (commutative) $\mathbb{Z}_\ell$-algebras R. Note that the generic fiber of $\mathbf{GL}_{T_\ell(A)}$ is $\mathbf{GL}_{V_\ell(A)}$ and the image of $\rho_{A,\ell}$ lies in $\mathbf{GL}_{T_\ell(A)}(\mathbb{Z}_\ell)$. Let $\mathcal{G}_{A,\ell}$ be the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}_K)$ in $\mathbf{GL}_{T_\ell(A)}$; it is a group scheme over $\mathbb{Z}_\ell$ with generic fiber $\mathbf{G}_{A,\ell}$.

Let $\bar{\rho}_{A,\ell}\colon \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Z}/\ell\mathbb{Z}}(A[\ell])$ be the representation describing the Galois action on the ℓ-torsion points of A. Observe that $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ is naturally a subgroup of $\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)$; the following results show that these groups are almost equal.

Proposition 2.10. *Suppose that $K_A^{\mathrm{conn}} = K$ and that A is absolutely simple.*

((i)) *For ℓ sufficiently large, $\mathcal{G}_{A,\ell}$ is a reductive group over $\mathbb{Z}_\ell$.*
((ii)) *There is a constant C such that the inequality $[\mathcal{G}_{A,\ell}(\mathbb{F}_\ell) : \bar{\rho}_{A,\ell}(\mathrm{Gal}_K)] \le C$ holds for all primes ℓ.*
((iii)) *For ℓ sufficiently large, the group $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ contains the commutator subgroup of $\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)$.*

Proof. In Serre's 1985-1986 course at the Collège de France [Ser00, #136], he showed that the groups $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ are essentially the $\mathbb{F}_\ell$-points of certain reductive groups. For each prime ℓ, he constructs a certain connected algebraic subgroup H_ℓ of $\mathbf{GL}_{T_\ell(A),\mathbb{F}_\ell} \cong \mathbf{GL}_{2\dim A,\mathbb{F}_\ell}$. There exists a finite extension L/K for which the following properties hold for all sufficiently large primes ℓ:

- H_ℓ is reductive.
- $\bar{\rho}_{A,\ell}(\mathrm{Gal}_L)$ is a subgroup of $H_\ell(\mathbb{F}_\ell)$ and the index $[H_\ell(\mathbb{F}_\ell) : \bar{\rho}_{A,\ell}(\mathrm{Gal}_L)]$ can be bounded independently of ℓ.
- $\bar{\rho}_{A,\ell}(\mathrm{Gal}_L)$ contains the commutator subgroup of $H_\ell(\mathbb{F}_\ell)$.

Detailed sketches of Serre's results were supplied in letters that have since been published in his collected papers; see the beginning of [Ser00], in particular the letter to M.-F. Vignéras [Ser00, #137]. The paper of Wintenberger [Win02] also contains everything we need.

In [Win02, §3.4], it is shown that Serre's group H_ℓ equals the special fiber of $\mathcal{G}_{A,\ell}$ for all sufficiently large ℓ. Parts (ii) and (iii) then follow from the properties of H_ℓ. For part (i), see [Win02, §2.1] and [LP95]. □

2.9. **Independence.** Combining all our ℓ-adic representations together, we obtain a single Galois representation

$$\rho_A\colon \mathrm{Gal}_K \to \prod_\ell \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$$

which describes the Galois action on all the torsion points of A. The following theorem shows that, after possibly replacing K by a finite extension, the Galois representations $\rho_{A,\ell}$ will be *independent*.

Proposition 2.11. *(Serre [Ser00, #138]) There is a finite Galois extension K' of K in $\overline{K}$ such that $\rho_A(\mathrm{Gal}_{K'})$ equals $\prod_\ell \rho_{A,\ell}(\mathrm{Gal}_{K'})$.*

We will need the following straightforward consequence:

Proposition 2.12. *Fix an extension K'/K as in Proposition 2.11. Let Λ be a finite set of rational primes. For each prime $\ell \in \Lambda$, fix a subset U_ℓ of the group $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ that is stable under conjugation. Let $\mathcal{S}$ be the set of $v \in \Sigma_K$ such that $\bar{\rho}_{A,\ell}(\mathrm{Frob}_v) \subseteq U_\ell$ for all $\ell \in \Lambda$. Then $\mathcal{S}$ has density*

$$\sum_C \frac{|C|}{|\mathrm{Gal}(K'/K)|} \cdot \prod_{\ell\in\Lambda} \frac{|\bar{\rho}_{A,\ell}(\Gamma_C) \cap U_\ell|}{|\bar{\rho}_{A,\ell}(\Gamma_C)|}$$

where C varies over the conjugacy classes of $\mathrm{Gal}(K'/K)$ and Γ_C is the set of $\sigma \in \mathrm{Gal}_K$ for which $\sigma|_{K'} \in C$.

Proof. Set $m := \prod_{\ell\in\Lambda} \ell$, and define $U_m := \prod_{\ell|m} U_\ell$, which we view as a subset of $\mathrm{Aut}_{\mathbb{Z}/m\mathbb{Z}}(A[m])$. Let $\bar{\rho}_{A,m}\colon \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Z}/m\mathbb{Z}}(A[m])$ be the homomorphism describing the Galois action on $A[m]$. Let μ and μ' be the Haar measures on Gal_K normalized so that $\mu(\mathrm{Gal}_K) = 1$ and $\mu'(\mathrm{Gal}_{K'}) = 1$.

The Chebotarev density theorem says that the density δ of $\mathcal{S}$ is defined and equals $\mu(\{\sigma \in \mathrm{Gal}_K : \bar{\rho}_{A,m}(\sigma) \in U_m\})$. Let $\{\sigma_i\}_{i\in I}$ be a subset of Gal_K consisting of representatives of the cosets of $\mathrm{Gal}_{K'}$ in Gal_K. We then have

$$[K' : K]\delta = \sum_{i\in I} \mu'(\{\sigma \in \sigma_i \mathrm{Gal}_{K'} : \bar{\rho}_{A,m}(\sigma) \in U_m\}) = \sum_{i\in I} \frac{|\bar{\rho}_{A,m}(\sigma_i \mathrm{Gal}_{K'}) \cap U_m|}{|\bar{\rho}_{A,m}(\sigma_i \mathrm{Gal}_{K'})|}.$$

We have $\bar{\rho}_{A,m}(\mathrm{Gal}_{K'}) = \prod_{\ell|m} \bar{\rho}_{A,\ell}(\mathrm{Gal}_{K'})$ by our choice of K' and hence $\bar{\rho}_{A,m}(\sigma_i \mathrm{Gal}_{K'})$ equals $\prod_{\ell|m} \bar{\rho}_{A,\ell}(\sigma_i \mathrm{Gal}_{K'})$ for all $i \in I$. Therefore,

$$[K' : K]\delta = \sum_{i\in I} \prod_{\ell|m} \frac{|\bar{\rho}_{A,\ell}(\sigma_i \mathrm{Gal}_{K'}) \cap U_\ell|}{|\bar{\rho}_{A,\ell}(\sigma_i \mathrm{Gal}_{K'})|}.$$

Since U_ℓ is stable under conjugation, we find that $|\bar{\rho}_{A,\ell}(\sigma_i \mathrm{Gal}_{K'}) \cap U_\ell|/|\bar{\rho}_{A,\ell}(\sigma_i \mathrm{Gal}_{K'})|$ depends only on the conjugacy class C of $\mathrm{Gal}(K'/K)$ containing $\sigma_i|_{K'}$ and equals $|\bar{\rho}_{A,\ell}(\Gamma_C) \cap U_\ell|/|\bar{\rho}_{A,\ell}(\Gamma_C)|$. Using this and grouping the σ_i by their conjugacy class when restricted to K', we deduce that

$$[K' : K]\delta = \sum_{C} |C| \prod_{\ell|m} \frac{|\bar{\rho}_{A,\ell}(\Gamma_C) \cap U_\ell|}{|\bar{\rho}_{A,\ell}(\Gamma_C)|}$$

where C varies over the conjugacy classes of $\mathrm{Gal}(K'/K)$. □

3. Reductive groups: background

Fix a perfect field k and an algebraic closure $\bar{k}$.

3.1. **Tori.** An (algebraic) torus over k is an algebraic group $\mathbf{T}$ defined over k for which $\mathbf{T}_{\bar{k}}$ is isomorphic to $\mathbb{G}^r_{m,\bar{k}}$ for some integer r. Fix a torus $\mathbf{T}$ over k. Let $X(\mathbf{T})$ be the group of characters $\mathbf{T}_{\bar{k}} \to \mathbb{G}_{m,\bar{k}}$; it is a free abelian group whose rank equals the dimension of $\mathbf{T}$. Let $\mathrm{Aut}(\mathbf{T}_{\bar{k}})$ be the group of automorphisms of the algebraic group $\mathbf{T}_{\bar{k}}$. For each $f \in \mathrm{Aut}(\mathbf{T}_{\bar{k}})$, we have an isomorphism $f_*\colon X(\mathbf{T}) \to X(\mathbf{T})$, $\alpha \mapsto \alpha \circ f^{-1}$; this gives a group isomorphism

$$\mathrm{Aut}(\mathbf{T}_{\bar{k}}) \xrightarrow{\sim} \mathrm{Aut}(X(\mathbf{T})),\ f \mapsto f_*$$

which we will often use as an identification. There is a natural action of the absolute Galois group Gal_k on $X(\mathbf{T})$; it satisfies $\sigma(\alpha(t)) = \sigma(\alpha)(\sigma(t))$ for all $\sigma \in \mathrm{Gal}_k$, $\alpha \in X(\mathbf{T})$ and $t \in \mathbf{T}(\bar{k})$. Let $\varphi_{\mathbf{T}}\colon \mathrm{Gal}_k \to \mathrm{Aut}(X(\mathbf{T}))$ be the homomorphism describing this action, that is, $\varphi_{\mathbf{T}}(\sigma)\alpha = \sigma(\alpha)$ for $\sigma \in \mathrm{Gal}_k$ and $\alpha \in X(\mathbf{T})$. Note that the torus $\mathbf{T}$, up to isomorphism, can be recovered from the representation $\varphi_{\mathbf{T}}$. We say that the torus $\mathbf{T}$ is split if it is isomorphic to $\mathbb{G}^r_{m,k}$; equivalently, if $\varphi_{\mathbf{T}}(\mathrm{Gal}_k) = 1$.

Let $\mathbf{G}$ be a reductive group over k. A maximal torus of $\mathbf{G}$ is a closed algebraic subgroup that is a torus (also defined over k) and is not contained in any larger such subgroup. If $\mathbf{T}$ and $\mathbf{T}'$ are maximal tori of $\mathbf{G}$, then $\mathbf{T}_{\bar{k}}$ and $\mathbf{T}'_{\bar{k}}$ are maximal tori of $\mathbf{G}_{\bar{k}}$ and are conjugate by some element of $\mathbf{G}(\bar{k})$. The group $\mathbf{G}$ has a maximal torus whose dimension is called the rank of $\mathbf{G}$. We say that $\mathbf{G}$ is split if it has a maximal torus that is split.

3.2. **Weyl group.** Let $\mathbf{G}$ be a connected reductive group over k. Fix a maximal torus $\mathbf{T}$ of $\mathbf{G}$. The (absolute) Weyl group of $\mathbf{G}$ with respect to $\mathbf{T}$ is the finite group

$$W(\mathbf{G}, \mathbf{T}) := N_{\mathbf{G}}(\mathbf{T})(\bar{k})/\mathbf{T}(\bar{k})$$

where $N_{\mathbf{G}}(\mathbf{T})$ is the normalizer of $\mathbf{T}$ in $\mathbf{G}$. For an element $g \in N_{\mathbf{G}}(\mathbf{T})(\bar{k})$, the morphism $\mathbf{T}_{\bar{k}} \to \mathbf{T}_{\bar{k}}$, $t \mapsto gtg^{-1}$ is an isomorphism that depends only on the image of g in $W(\mathbf{G}, \mathbf{T})$; this induces a

faithful action of $W(\mathbf{G},\mathbf{T})$ on $\mathbf{T}_{\bar{k}}$. So, we can identify $W(\mathbf{G},\mathbf{T})$ with a subgroup of $\mathrm{Aut}(\mathbf{T}_{\bar{k}})$ and hence also of $\mathrm{Aut}(X(\mathbf{T}))$.

There is a natural action of Gal_k on $W(\mathbf{G},\mathbf{T})$. For $\sigma \in \mathrm{Gal}_k$ and $w \in W(\mathbf{G},\mathbf{T})$, we have $\varphi_{\mathbf{T}}(\sigma) \circ w \circ \varphi_{\mathbf{T}}(\sigma)^{-1} = \sigma(w)$. In particular, note that the action of Gal_k of $W(\mathbf{G},\mathbf{T})$ is trivial if $\mathbf{T}$ is split.

We define $\Pi(\mathbf{G},\mathbf{T})$ to be subgroup of $\mathrm{Aut}(X(\mathbf{T}))$ generated by $W(\mathbf{G},\mathbf{T})$ and $\varphi_{\mathbf{T}}(\mathrm{Gal}_k)$. The Weyl group $W(\mathbf{G},\mathbf{T})$ is a normal subgroup of $\Pi(\mathbf{G},\mathbf{T})$. Up to isomorphism, the groups $W(\mathbf{G},\mathbf{T})$ and $\Pi(\mathbf{G},\mathbf{T})$ are independent of $\mathbf{T}$ (for the group $\Pi(\mathbf{G},\mathbf{T})$, see Proposition 2.1 of [JKZ11]); we shall denote the abstract groups by $W(\mathbf{G})$ and $\Pi(\mathbf{G})$, respectively.

3.3. **Maximal tori over finite fields.** We now assume that k is a finite field $\mathbb{F}_q$ with q elements. Let $\mathbf{G}$ be a connected reductive group defined over $\mathbb{F}_q$. Assume further that $\mathbf{G}$ is split and fix a split maximal torus $\mathbf{T}$. Let $\mathbf{T}'$ be any maximal torus of $\mathbf{G}$. There is an element $g \in \mathbf{G}(\overline{\mathbb{F}}_q)$ such that $g\mathbf{T}'_{\overline{\mathbb{F}}_q}g^{-1} = \mathbf{T}_{\overline{\mathbb{F}}_q}$. Since $\mathbf{T}$ and $\mathbf{T}'$ are defined over $\mathbb{F}_q$, we find that $\mathrm{Frob}_q(g)\mathbf{T}'_{\overline{\mathbb{F}}_q}\mathrm{Frob}_q(g)^{-1} = \mathbf{T}_{\overline{\mathbb{F}}_q}$ and hence $g\,\mathrm{Frob}_q(g)^{-1}$ belongs to $N_{\mathbf{G}}(\mathbf{T})(\overline{\mathbb{F}}_q)$. Let $\theta_{\mathbf{G}_A}(\mathbf{T}')$ be the conjugacy class of $W(\mathbf{G},\mathbf{T})$ containing the coset represented by $g\,\mathrm{Frob}_q(g)^{-1}$. These conjugacy classes have the following interpretation:

Proposition 3.1. *The map $\mathbf{T}' \mapsto \theta_{\mathbf{G}}(\mathbf{T}')$ defines a bijection between the maximal tori of $\mathbf{G}$ up to conjugation in $\mathbf{G}(\mathbb{F}_q)$ and the conjugacy classes of $W(\mathbf{G},\mathbf{T})$.*

Proof. This is [Car85, Prop. 3.3.3]. Note that the action of Frob_q on $W(\mathbf{G},\mathbf{T})$ is trivial since $\mathbf{T}$ is split, so the Frob_q-conjugacy classes of $W(\mathbf{G},\mathbf{T})$ in [Car85] are just the usual conjugacy classes of $W(\mathbf{G},\mathbf{T})$. □

Let $\mathbf{G}(\mathbb{F}_q)_{sr}$ be the set of $g \in \mathbf{G}(\mathbb{F}_q)$ that are semisimple and regular in $\mathbf{G}$. Each $g \in \mathbf{G}(\mathbb{F}_q)_{sr}$ is contained in a unique maximal torus $\mathbf{T}_g$ of $\mathbf{G}$. We define the map

$$\theta_{\mathbf{G}} \colon \mathbf{G}(\mathbb{F}_q)_{sr} \to W(\mathbf{G},\mathbf{T})^\sharp, \quad g \mapsto \theta_{\mathbf{G}}(\mathbf{T}_g)$$

where $W(\mathbf{G},\mathbf{T})^\sharp$ is the set of conjugacy classes of $W(\mathbf{G},\mathbf{T})$. We will need the following equidistribution result later.

Lemma 3.2. *Let $\mathbf{G}$ be a connected and split reductive group over a finite field $\mathbb{F}_q$, and fix a split maximal torus $\mathbf{T}$. Let C be a subset of $W(\mathbf{G},\mathbf{T})$ that is stable under conjugation and let κ be a subset of $\mathbf{G}(\mathbb{F}_q)$ that is a union of cosets of the commutator subgroup of $\mathbf{G}(\mathbb{F}_q)$. Then*

$$\frac{|\{g \in \kappa \cap \mathbf{G}(\mathbb{F}_q)_{sr} : \theta_{\mathbf{G}}(g) \subseteq C\}|}{|\kappa|} = \frac{|C|}{|W(\mathbf{G},\mathbf{T})|} + O(1/q)$$

where the implicit constant depends only on the type of $\mathbf{G}$ (and in particular, not on q, $\mathbf{T}$, C and κ).

Proof. We shall reduce to a special case treated in [JKZ11] which deals with semisimple groups. Let $\mathbf{G}^{\mathrm{ad}}$ be the quotient of $\mathbf{G}$ by its center and let $\varphi \colon \mathbf{G} \to \mathbf{G}^{\mathrm{ad}}$ be the quotient homomorphism. Let $\mathbf{T}^{\mathrm{ad}}$ be the image of $\mathbf{T}$ under φ; it is a split maximal torus of $\mathbf{G}^{\mathrm{ad}}$. The homomorphism φ induces a group isomorphism $\varphi_* \colon W(\mathbf{G},\mathbf{T}) \xrightarrow{\sim} W(\mathbf{G}^{\mathrm{ad}},\mathbf{T}^{\mathrm{ad}})$. An element $g \in \mathbf{G}(\overline{\mathbb{F}}_q)$ is regular and semisimple in $\mathbf{G}$ if and only if $\varphi(g)$ is regular and semisimple in $\mathbf{G}^{\mathrm{ad}}$. For $g \in \mathbf{G}(\mathbb{F}_q)_{sr}$, one can check that $\theta_{\mathbf{G}}(g) \subseteq C$ if and only if $\theta_{\mathbf{G}^{\mathrm{ad}}}(\varphi(g)) \subseteq \varphi_*(C)$. Therefore,

$$\frac{|\{g \in \kappa \cap \mathbf{G}(\mathbb{F}_q)_{sr} : \theta_{\mathbf{G}}(g) \subseteq C\}|}{|\kappa|} = \frac{|\{g \in \varphi(\kappa) \cap \mathbf{G}^{\mathrm{ad}}(\mathbb{F}_q)_{sr} : \theta_{\mathbf{G}^{\mathrm{ad}}}(g) \subseteq \varphi_*(C)\}|}{|\varphi(\kappa)|}. \tag{3.1}$$

Let $\mathbf{G}^{\mathrm{der}}$ be the derived subgroup of $\mathbf{G}$ and let $\pi\colon \mathbf{G}^{\mathrm{sc}} \to \mathbf{G}^{\mathrm{der}}$ be the simply connected cover of $\mathbf{G}^{\mathrm{der}}$. The homomorphism $\pi' := \varphi \circ \pi\colon \mathbf{G}^{\mathrm{sc}} \to \mathbf{G}^{\mathrm{ad}}$ is a simply connected cover of $\mathbf{G}^{\mathrm{ad}}$. Since $\mathbf{G}^{\mathrm{ad}}$ is adjoint, it is the product of simple adjoint groups defined over $\mathbb{F}_q$.

Excluding a finite number of q, depending only on the type of $\mathbf{G}$, we may assume that the group $\pi'(\mathbf{G}^{\mathrm{sc}}(\mathbb{F}_q))$ agrees with the commutator subgroup of $\mathbf{G}^{\mathrm{ad}}(\mathbb{F}_q)$ and is a product of simple groups of Lie type, see [Lar95, §2.1] for background. (We can later on choose the implicit constant in the lemma to deal with the finitely many excluded q.) Since $\pi'(\mathbf{G}^{\mathrm{sc}}(\mathbb{F}_q))$ is perfect, we find that the image of the commutator subgroup of $\mathbf{G}(\mathbb{F}_q)$ under φ is $\pi'(\mathbf{G}^{\mathrm{sc}}(\mathbb{F}_q))$. In particular, $\varphi(\kappa) \subseteq \mathbf{G}^{\mathrm{ad}}(\mathbb{F}_q)$ consists of cosets of $\pi'(\mathbf{G}^{\mathrm{sc}}(\mathbb{F}_q))$. Proposition 4.6 of [JKZ11] now applies, and shows that the right-hand side of (3.1) equals $|\varphi_*(C)|/|W(\mathbf{G}^{\mathrm{ad}}, \mathbf{T}^{\mathrm{ad}})| + O(1/q) = |C|/|W(\mathbf{G}, \mathbf{T})| + O(1/q)$, where the implicit constants depend only on the type of $\mathbf{G}^{\mathrm{ad}}$; the proposition is only stated for a single $\pi'(\mathbf{G}^{\mathrm{sc}}(\mathbb{F}_q))$ coset, but one observes that the index $[\mathbf{G}^{\mathrm{ad}}(\mathbb{F}_q) : \pi'(\mathbf{G}^{\mathrm{sc}}(\mathbb{F}_q))]$ can be bounded in terms of the type of $\mathbf{G}^{\mathrm{ad}}$. □

4. Frobenius conjugacy classes

Let A be a non-zero abelian variety over a number field K. Assume that $K_A^{\mathrm{conn}} = K$ and fix an embedding $K \subseteq \mathbb{C}$. In this section, we state a theorem of R. Noot which gives a weakened version of Conjecture 2.8.

4.1. **The variety $\mathbf{Conj}'(\mathbf{G}_A)$.** We first need to define a variant of the variety $\mathrm{Conj}(\mathbf{G}_A)$ from §2.7. Let $\mathbf{G}_A^{\mathrm{der}}$ be the derived subgroup of $\mathbf{G}_A$. Let $\{\mathbf{H}_i\}_{i\in I}$ be the minimal non-trivial normal connected closed subgroups of $(\mathbf{G}_A^{\mathrm{der}})_{\overline{\mathbb{Q}}}$. The groups $\mathbf{H}_i$ are semisimple. The morphism $\prod_{i\in I} \mathbf{H}_i \to (\mathbf{G}_A^{\mathrm{der}})_{\overline{\mathbb{Q}}}$, $(g_i)_{i\in I} \mapsto \prod_{i\in I} g_i$ is a homomorphism of algebraic groups and has finite kernel.

Let J be the set of $i \in I$ for which $\mathbf{H}_i$ is isomorphic to $\mathbf{SO}(2k_i)_{\overline{\mathbb{Q}}}$ for some integer $k_i \geq 4$. For each $i \in J$, we identify $\mathbf{H}_i$ with $\mathbf{SO}(2k_i)_{\overline{\mathbb{Q}}}$ and we set $\mathbf{H}_i' := \mathbf{O}(2k_i)_{\overline{\mathbb{Q}}}$. For $i \in I - J$, we set $\mathbf{H}_i' := \mathbf{H}_i$.

Let $\mathbf{C}$ be the center of $\mathbf{G}_A$. We define $\mathcal{A}$ to be the group of automorphisms f of the algebraic group $\mathbf{G}_{A,\overline{\mathbb{Q}}}$ which satisfies the following properties:

- $f(\mathbf{H}_i) = \mathbf{H}_i$ for all $i \in I$,
- the morphism $f|_{\mathbf{H}_i}\colon \mathbf{H}_i \to \mathbf{H}_i$ agrees with conjugation by some element in $\mathbf{H}_i'$,
- the morphism $f|_{\mathbf{C}_{\overline{\mathbb{Q}}}}\colon \mathbf{C}_{\overline{\mathbb{Q}}} \to \mathbf{C}_{\overline{\mathbb{Q}}}$ is the identity map.

One can verify that $\mathcal{A}$ is an algebraic group which is actually defined over $\mathbb{Q}$.

Let R be the affine coordinate ring of $\mathbf{G}_A$. The group $\mathcal{A}$ acts on R by composition, and we define $R^{\mathcal{A}}$ to be the $\mathbb{Q}$-subalgebra of R consisting of those elements fixed by the $\mathcal{A}$-action. Define the $\mathbb{Q}$-variety $\mathrm{Conj}'(\mathbf{G}_A) := \mathrm{Spec}(R^{\mathcal{A}})$ and let $\mathrm{cl}'_{\mathbf{G}_A}\colon \mathbf{G}_A \to \mathrm{Conj}'(\mathbf{G}_A)$ be the morphism arising from the inclusion $R^{\mathcal{A}} \hookrightarrow R$ of $\mathbb{Q}$-algebras.

4.2. **A theorem of Noot.** By Proposition 2.7 and our ongoing assumption $K_A^{\mathrm{conn}} = K$, the representation $\rho_{A,\ell}$ has image in $\mathbf{G}_A(\mathbb{Q}_\ell)$. The following is a consequence of [Noo09, Théorème 1.8].

Theorem 4.1 (Noot)**.** *Let v be a finite place of K for which A has good reduction. Suppose that $\pi_1\pi_2^{-1}$ is not a root of unity for all distinct roots $\pi_1, \pi_2 \in \overline{\mathbb{Q}}$ of $P_{A_v}(x)$. Then there exists an $F_v' \in \mathrm{Conj}'(\mathbf{G}_A)(\mathbb{Q})$ such that $F_v' = \mathrm{cl}'_{\mathbf{G}_A}(\rho_{A,\ell}(\mathrm{Frob}_v))$ for all primes ℓ satisfying $v \nmid \ell$.*

The group of inner automorphisms of $\mathbf{G}_{A,\overline{\mathbb{Q}}}$ is a normal subgroup of finite index in $\mathcal{A}$. So each element of $R^{\mathcal{A}}$ is a central function of $\mathbf{G}_A$, and we have a natural morphism $\varphi\colon \mathrm{Conj}(\mathbf{G}_A) \to \mathrm{Conj}'(\mathbf{G}_A)$ that satisfies $\mathrm{cl}'_{\mathbf{G}_A} = \varphi \circ \mathrm{cl}_{\mathbf{G}_A}$. Observe that if Conjecture 2.8 holds, then the F_v' in Noot's theorem equals $\varphi(F_v)$.

4.3. **The group Γ.** Fix a maximal torus $\mathbf{T}$ of $\mathbf{G}_A$. Let $\mathcal{A}(\mathbf{T})$ be the subgroup of $f \in \mathcal{A}$ that satisfy $f(\mathbf{T}_{\overline{\mathbb{Q}}}) = \mathbf{T}_{\overline{\mathbb{Q}}}$. Every element of $\mathcal{A}$ is conjugate to an element of $\mathcal{A}(\mathbf{T})$ by an inner automorphism of $\mathbf{G}_{A,\overline{\mathbb{Q}}}$. Define

$$\Gamma := \{f|_{\mathbf{T}_{\overline{\mathbb{Q}}}} : f \in \mathcal{A}(\mathbf{T})\};$$

it is a (finite) subgroup of $\mathrm{Aut}(\mathbf{T}_{\overline{\mathbb{Q}}})$ which is stable under the action of $\mathrm{Gal}_{\mathbb{Q}}$. For $t_1, t_2 \in \mathbf{T}(\overline{\mathbb{Q}})$, we have $\mathrm{cl}'_{\mathbf{G}_A}(t_1) = \mathrm{cl}'_{\mathbf{G}_A}(t_2)$ if and only if $t_2 = \beta(t_1)$ for some $\beta \in \Gamma$. So, using $\mathrm{cl}'_{\mathbf{G}_A}$, we find that the variety $\mathrm{Conj}'(\mathbf{G}_A)_{\overline{\mathbb{Q}}}$ is the quotient of the torus $\mathbf{T}_{\overline{\mathbb{Q}}}$ by Γ.

Observe that $W(\mathbf{G}_A, \mathbf{T})$ is a normal subgroup of Γ. The following technical lemma will be found important later.

Lemma 4.2. *Suppose H is a subgroup of Γ such that $H \cap C \neq \emptyset$ for each conjugacy class C of Γ contained in $W(\mathbf{G}_A, \mathbf{T})$. Then $H \supseteq W(\mathbf{G}_A, \mathbf{T})$.*

Proof. Since $W(\mathbf{G}_A, \mathbf{T})$ is a normal subgroup of Γ, there no harm in replacing H by $H \cap W(\mathbf{G}_A, \mathbf{T})$; thus, without loss of generality, we may assume that H is a subgroup of $W(\mathbf{G}_A, \mathbf{T})$.

Let $\Phi := \Phi(\mathbf{G}_A, \mathbf{T}) \subseteq X(\mathbf{T})$ be the set of roots of $\mathbf{G}_A$ with respect to $\mathbf{T}$, cf. [Bor91, §8.17]. The set of roots with the embedding $\Phi \hookrightarrow X(\mathbf{T}_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{R}$ form an abstract root system. The root system Φ is the disjoint union of its irreducible components $\{\Phi_i\}_{i \in I}$, where the root systems Φ_i correspond with our subgroups $\mathbf{H}_i$.

We can identify Γ with a subgroup of $\mathrm{Aut}(X(\mathbf{T}))$. For $f \in \Gamma$, we have $f(\Phi) = \Phi$; moreover, $f(\Phi_i) = \Phi_i$ for $i \in I$. For each $i \in I$, we have a homomorphism $\Gamma \to \mathrm{Aut}(\Phi_i), f \mapsto f|_{\Phi_i}$ whose image we denote by Γ_i. Let $W(\Phi_i)$ be the Weyl group of Φ_i; it is a subgroup of index at most 2 in Γ_i. If $i \notin J$, then we have $\Gamma_i = W(\Phi_i)$. The group $W(\mathbf{G}_A, \mathbf{T})$ acts faithfully on Φ, and one can then check that Γ also acts faithfully on Φ. Therefore, the natural map $\Gamma \to \prod_{i \in I} \Gamma_i \subseteq \mathrm{Aut}(\Phi)$ is injective and $W(\mathbf{G}_A, \mathbf{T})$ is mapped to the Weyl group $\prod_{i \in I} W(\Phi_i) = W(\Phi)$. We may thus identify H with a subgroup of $\prod_{i \in I} \Gamma_i$. Let H_i be the group of $(f_j)_{j \in I} \in \prod_{j \in I} \Gamma_j$ that belongs to H and satisfies $f_j = 1$ for $j \neq i$. We have $\prod_{i \in I} H_i \subseteq H \subseteq W(\Phi)$, so it suffices to show that $W(\Phi_i) \subseteq H_i$ for every $i \in I$.

Fix any $i \in I$. From our assumptions on H, we find that H_i is a subgroup of $W(\Phi_i)$ such that $H_i \cap C \neq \emptyset$ for every conjugacy classes C of Γ_i that is contained in $W(\Phi_i)$. If $\Gamma_i = W(\Phi_i)$, then we have $H_i = W(\Phi_i)$ by Jordan's lemma [Ser03, Theorem 4']. It remains to consider the case where $\Gamma_i \neq W(\Phi)$.

We have reduced the lemma to the following situation: let Φ be an irreducible root system of type D_n with $n \geq 4$. Let Γ be a subgroup of $\mathrm{Aut}(\Phi)$ that contains $W(\Phi)$ and satisfies $[\Gamma : W(\Phi)] = 2$. Let H be a subgroup of $W(\Phi)$ that satisfies $H \cap C \neq \emptyset$ for all conjugacy classes C of Γ contained in $W(\Phi)$. We need to show that $H = W(\Phi)$.

We can identify the root system Φ with the set of vectors $\pm e_i \pm e_j$ with $1 \leq i < j \leq n$ in $\mathbb{R}^n$, where $e_1, \ldots, e_n$ is the standard basis of $\mathbb{R}^n$. Let Γ' be the group of automorphisms f of the vector space $\mathbb{R}^n$ such that for each $1 \leq i \leq n$, we have $f(e_i) = \varepsilon_i e_j$ for some $j \in \{1, \ldots, n\}$ and $\varepsilon_i \in \{\pm 1\}$. Ignoring the signs, each $f \in \Gamma'$ gives a permutation of $\{1, \ldots, n\}$; this defines a short exact sequence

$$1 \to N \to \Gamma' \xrightarrow{\varphi} S_n \to 1$$

where the group N consists of those $f \in \Gamma'$ that satisfy $f(e_i) = \pm e_i$ for all $1 \leq i \leq n$. The Weyl group $W(\Phi)$ is the subgroup of index 2 in Γ' consisting of those f for which $\prod_{i=1}^n \varepsilon_i = 1$. We may assume that $\Gamma = \Gamma'$; for $n > 5$, this is because $\Gamma' = \mathrm{Aut}(\Phi)$ (for $n = 4$, the subgroups of $\mathrm{Aut}(\Phi)$ that contain $W(\Phi)$ as an index subgroup of order 2 are all conjugate to Γ'). Restricting φ to $W(\Phi)$, we have a short exact sequence

$$1 \to N' \to W(\Phi) \xrightarrow{\varphi|_{W(\Phi)}} S_n \to 1$$

where N' is the group of $f \in N$ for which $f(e_i) = \varepsilon_i e_i$ and $\prod_i \varepsilon_i = 1$. Since $\varphi(\Gamma) = \varphi(W(\Phi)) = S_n$, our assumption on H implies that $\varphi(H) \cap C \neq \emptyset$ for each conjugacy class C of S_n. We thus have $\varphi(H) = S_n$ by Jordan's lemma [Ser03, Theorem 4']. It thus suffices to prove that $H \supseteq N'$.

For a subset $B \subseteq \{1, \dots, n\}$ with cardinality 2, we let f_B be the element of N' for which $f_B(e_i) = -e_i$ if $i \in B$ and $f_B(e_i) = e_i$ otherwise. For $g \in \Gamma$, we have $g f_B g^{-1} = f_{\sigma(B)}$ where $\sigma := \varphi(g)$. Therefore, H contains an element of the form f_B for some set $B \subseteq \{1, \dots, n\}$ with cardinality 2 (such functions form a conjugacy class of Γ in $W(\Phi)$). Since $\varphi(H) = S_n$, we deduce that H contains all the f_B with $|B| = 2$, and hence $H \supseteq N'$ since N' is generated by such f_B. □

5. Local representations

Fix a non-zero abelian variety A defined over a number field K such that $K_A^{\mathrm{conn}} = K$. Fix a prime ℓ and suppose that $\mathcal{G}_{A,\ell}$ is a reductive group scheme over $\mathbb{Z}_\ell$ which has a split maximal torus $\mathcal{T}$. Denote the generic fiber of $\mathcal{T}$ by $\mathbf{T}$; it is a maximal torus of $\mathbf{G}_{A,\ell}$.

Take any place $v \in \mathcal{S}_A$ that satisfies $v \nmid \ell$. Define the set

$$\mathcal{I}_{v,\ell} := \left\{ t \in \mathbf{T}(\overline{\mathbb{Q}}_\ell) : t \text{ and } \rho_{A,\ell}(\mathrm{Frob}_v) \text{ are conjugate in } \mathbf{G}_{A,\ell}(\overline{\mathbb{Q}}_\ell) \right\}$$

and fix an element $t_{v,\ell} \in \mathcal{I}_{v,\ell}$. Conjugation induces an action of the Weyl group $W(\mathbf{G}_{A,\ell}, \mathbf{T})$ on $\mathcal{I}_{v,\ell}$. Since v belongs to $\mathcal{S}_A$, we find that the group generated by $t_{v,\ell}$ is Zariski dense in $\mathbf{T}_{\overline{\mathbb{Q}}_\ell}$ and hence the action of $W(\mathbf{G}_{A,\ell}, \mathbf{T})$ on $\mathcal{I}_{v,\ell}$ is simply transitive.

Since $\mathbf{G}_{A,\ell}$, $\mathbf{T}$ and $\rho_{A,\ell}(\mathrm{Frob}_v)$ are defined over $\mathbb{Q}_\ell$, we also have a natural action of $\mathrm{Gal}_{\mathbb{Q}_\ell}$ on $\mathcal{I}_{v,\ell}$. So for each $\sigma \in \mathrm{Gal}_{\mathbb{Q}_\ell}$, there is a unique $\psi_{v,\ell}(\sigma) \in W(\mathbf{G}_{A,\ell}, \mathbf{T})$ that satisfies $\sigma(t_{v,\ell}) = \psi_{v,\ell}(\sigma)^{-1}(t_{v,\ell})$. Using that $\mathbf{T}$ is split, one can show that map

$$\psi_{v,\ell} \colon \mathrm{Gal}_{\mathbb{Q}_\ell} \to W(\mathbf{G}_{A,\ell}, \mathbf{T}), \quad \sigma \mapsto \psi_{v,\ell}(\sigma)$$

is a group homomorphism. Note that a different choice of $t_{v,\ell}$ would alter $\psi_{v,\ell}$ by an inner automorphism of $W(\mathbf{G}_{A,\ell}, \mathbf{T})$. Choose an embedding $\overline{\mathbb{Q}} \subseteq \overline{\mathbb{Q}}_\ell$. The homomorphism $\psi_{v,\ell}$ then factors through an injective group homomorphism $\mathrm{Gal}(\mathbb{Q}_\ell(\mathcal{W}_{A_v})/\mathbb{Q}_\ell) \hookrightarrow W(\mathbf{G}_{A,\ell}, \mathbf{T})$.

Lemma 5.1. *Fix a subset C of $W(\mathbf{G}_{A,\ell}, \mathbf{T})$ that is stable under conjugation. There is a subset U_ℓ of $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ that is stable under conjugation and satisfies the following properties:*

- *If $v \in \mathcal{S}_A$ satisfies $v \nmid \ell$ and $\bar{\rho}_{A,\ell}(\mathrm{Frob}_v) \subseteq U_\ell$, then $\psi_{v,\ell}$ is unramified and $\psi_{v,\ell}(\mathrm{Frob}_\ell) \subseteq C$.*
- *Let K' be a finite extension of K and let κ be a subset of Gal_K that consists of a union of cosets of $\mathrm{Gal}_{K'}$. Then we have*

$$\frac{|\bar{\rho}_{A,\ell}(\kappa) \cap U_\ell|}{|\bar{\rho}_{A,\ell}(\kappa)|} = \frac{|C|}{|W(\mathbf{G}_{A,\ell}, \mathbf{T})|} + O(1/\ell)$$

where the implicit constant depends only on A and K'.

Proof. Set $\mathcal{G} := \mathcal{G}_{A,\ell}$; it is a reductive group scheme over $\mathbb{Z}_\ell$ by assumption. The special fiber $\mathcal{G}_{\mathbb{F}_\ell}$ is a reductive group with split maximal torus $\mathcal{T}_{\mathbb{F}_\ell}$. Assuming ℓ is sufficiently large, the derived subgroups of $\mathcal{G}_{\mathbb{F}_\ell}$ and $\mathcal{G}_{\mathbb{Q}_\ell} = \mathbf{G}_{A,\ell}$ are of the same Lie type; this follows from [Win02, Théorème 2]. Note that we can set $U_\ell = \emptyset$ for the finitely many excluded primes. Therefore, the Weyl groups $W(\mathbf{G}_{A,\ell}, \mathbf{T})$ and $W(\mathcal{G}_{\mathbb{F}_\ell}, \mathcal{T}_{\mathbb{F}_\ell})$ are abstractly isomorphic; we now describe an explicit isomorphism. The homomorphism

$$N_{\mathcal{G}}(\mathcal{T})(\mathbb{Z}_\ell)/\mathcal{T}(\mathbb{Z}_\ell) \hookrightarrow N_{\mathcal{G}}(\mathcal{T})(\mathbb{Q}_\ell)/\mathcal{T}(\mathbb{Q}_\ell) = W(\mathcal{G}_{\mathbb{Q}_\ell}, \mathcal{T}_{\mathbb{Q}_\ell}) = W(\mathbf{G}_{A,\ell}, \mathbf{T}) \tag{5.1}$$

is injective; the identification with the Weyl group uses that $\mathcal{T}_{\mathbb{Q}_\ell} = \mathbf{T}$ is split. The normalizer $N_{\mathcal{G}}(\mathcal{T})$ is a closed and smooth subscheme of $\mathcal{G}$; for smoothness, see [DG70, XXII Corollaire 5.3.11].

The homomorphisms $N_{\mathcal{G}}(\mathcal{T})(\mathbb{Z}_\ell) \to N_{\mathcal{G}}(\mathcal{T})(\mathbb{F}_\ell)$ and $\mathcal{T}(\mathbb{Z}_\ell) \to \mathcal{T}(\mathbb{F}_\ell)$ are thus surjective by Hensel's lemma, and we obtain a surjective homomorphism

$$N_{\mathcal{G}}(\mathcal{T})(\mathbb{Z}_\ell)/\mathcal{T}(\mathbb{Z}_\ell) \twoheadrightarrow N_{\mathcal{G}_{\mathbb{F}_\ell}}(\mathcal{T}_{\mathbb{F}_\ell})(\mathbb{F}_\ell)/\mathcal{T}_{\mathbb{F}_\ell}(\mathbb{F}_\ell) = W(\mathcal{G}_{\mathbb{F}_\ell}, \mathcal{T}_{\mathbb{F}_\ell}). \tag{5.2}$$

Since (5.1) and (5.2) are injective and surjective homomorphisms, respectively, into isomorphic groups, we deduce that they are both isomorphisms. Combining the isomorphisms (5.1) and (5.2), we obtain the desired isomorphism $W(\mathbf{G}_{A,\ell}, \mathbf{T}) \xrightarrow{\sim} W(\mathcal{G}_{\mathbb{F}_\ell}, \mathcal{T}_{\mathbb{F}_\ell})$.

Now fix a place $v \in \mathcal{S}_A$ and let $h \in \mathcal{G}(\mathbb{Z}_\ell)$ be a representative of the conjugacy class $\rho_{A,\ell}(\mathrm{Frob}_v)$. We know that h is semisimple and regular in $\mathcal{G}_{\mathbb{Q}_\ell} = \mathbf{G}_{A,\ell}$ by our choice of $\mathcal{S}_A$.

Suppose that the image $\bar{h}$ of h in $\mathcal{G}(\mathbb{F}_\ell)$ is semisimple and regular. The centralizer $\mathcal{T}_h$ of h in $\mathcal{G}$ is then a smooth and closed subscheme whose generic and special fibers are both maximal tori, that is, $\mathcal{T}_h$ is a maximal torus of $\mathcal{G}$. The transporter $\mathrm{Transp}_{\mathcal{G}}(\mathcal{T}_h, \mathcal{T})$ is a closed and smooth group scheme in $\mathcal{G}$; again for smoothness, see [DG70, XXII Corollaire 5.3.11]. Recall that for any $\mathbb{Z}_\ell$-algebra R, we have

$$\mathrm{Transp}_{\mathcal{G}}(\mathcal{T}_h, \mathcal{T})(R) = \{g \in \mathcal{G}(R) : g\,\mathcal{T}_{h,R}\,g^{-1} = \mathcal{T}_R\}.$$

Choose any point $\overline{g} \in \mathrm{Transp}_{\mathcal{G}}(\mathcal{T}_h, \mathcal{T})(\overline{\mathbb{F}}_\ell)$. Let $\mathbb{Z}_\ell^{un}$ be the ring of integers in the maximal unramified extension of $\mathbb{Q}_\ell$ in $\overline{\mathbb{Q}}_\ell$. Since $\mathrm{Transp}_{\mathcal{G}}(\mathcal{T}_h, \mathcal{T})$ is smooth and $\mathbb{Z}_\ell^{un}$ is Henselian, there is a $g \in \mathrm{Transp}_{\mathcal{G}}(\mathcal{T}_h, \mathcal{T})(\mathbb{Z}_\ell^{un})$ that lifts $\overline{g}$. The element $g\,\mathrm{Frob}_\ell(g)^{-1}$ belongs to $N_{\mathcal{G}}(\mathcal{T})(\mathbb{Z}_\ell^{un})$ and under the reduction map it is sent to $\bar{g}\,\mathrm{Frob}_\ell(\bar{g})^{-1} \in N_{\mathcal{G}_{\mathbb{F}_\ell}}(\mathcal{T}_{\mathbb{F}_\ell})(\overline{\mathbb{F}}_\ell)$. The element of $W(\mathcal{G}_{\mathbb{F}_\ell}, \mathcal{T}_{\mathbb{F}_\ell})$ represented by $\bar{g}\,\mathrm{Frob}_\ell(\bar{g})^{-1}$ belongs to the conjugacy class $\theta_{\mathcal{G}_{\mathbb{F}_\ell}}(\bar{h})$ as in §3.3. Define $t := ghg^{-1}$; it is an element of the set $\mathcal{I}_{v,\ell}$. We have

$$\mathrm{Frob}_\ell(t) = \mathrm{Frob}_\ell(g)h\,\mathrm{Frob}_\ell(g)^{-1} = (g\,\mathrm{Frob}_\ell(g)^{-1})^{-1} \cdot t \cdot (g\,\mathrm{Frob}_\ell(g)^{-1})$$

since h is defined over $\mathbb{Q}_\ell$. Therefore, the conjugacy class of $\psi_{v,\ell}(\mathrm{Frob}_\ell)$ in $W(\mathcal{G}_{\mathbb{Q}_\ell}, \mathcal{T}_{\mathbb{Q}_\ell}) = W(\mathbf{G}_{A,\ell}, \mathbf{T})$ is represented by $g\,\mathrm{Frob}_\ell(g)^{-1}$. Since g is defined over $\mathbb{Z}_\ell^{un}$, we deduce that $\psi_{v,\ell}$ is unramified at ℓ. With respect to our isomorphism $W(\mathbf{G}_{A,\ell}, \mathbf{T}) = W(\mathcal{G}_{\mathbb{Q}_\ell}, \mathcal{T}_{\mathbb{Q}_\ell}) \cong W(\mathcal{G}_{\mathbb{F}_\ell}, \mathcal{T}_{\mathbb{F}_\ell})$, we find that $\psi_{v,\ell}(\mathrm{Frob}_\ell)$ lies in the conjugacy class $\theta_{\mathcal{G}_{\mathbb{F}_\ell}}(\bar{\rho}_{A,\ell}(\mathrm{Frob}_v))$ of $W(\mathbf{G}_{A,\ell}, \mathbf{T})$.

Let U_ℓ be the set of $h \in \bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ that are semisimple and regular in $\mathcal{G}_{\mathbb{F}_\ell}$ and satisfy $\theta_{\mathcal{G}_{\mathbb{F}_\ell}}(h) \subseteq C$; it is stable under conjugation by $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$. If $v \in \mathcal{S}_A$ satisfies $v \nmid \ell$ and $\bar{\rho}_{A,\ell}(\mathrm{Frob}_v) \subseteq U_\ell$, then the above work shows that $\psi_{v,\ell}$ is unramified and $\psi_{v,\ell}(\mathrm{Frob}_\ell)$ lies in the conjugacy class $\theta_{\mathcal{G}_{\mathbb{F}_\ell}}(\bar{\rho}_{A,\ell}(\mathrm{Frob}_v)) \subseteq C$.

It remains to show that U_ℓ satisfies the second property in the statement of the lemma. Proposition 2.10(iii) tells us that $\bar{\rho}_{A,\ell}(\mathrm{Gal}_{K'})$ contains the commutator subgroup of $\mathcal{G}_{\mathbb{F}_\ell}(\mathbb{F}_\ell)$ for ℓ sufficiently large. For such primes ℓ, $\bar{\rho}_{A,\ell}(\kappa)$ consists of cosets of the commutator subgroup of $\mathcal{G}_{\mathbb{F}_\ell}(\mathbb{F}_\ell)$, and hence

$$\frac{|\bar{\rho}_{A,\ell}(\kappa) \cap U_\ell|}{|\bar{\rho}_{A,\ell}(\kappa)|} = \frac{|C|}{|W(\mathcal{G}_{\mathbb{F}_\ell}, \mathcal{T}_{\mathbb{F}_\ell})|} + O(1/\ell) = \frac{|C|}{|W(\mathbf{G}_{A,\ell}, \mathbf{T})|} + O(1/\ell)$$

by Lemma 3.2 where the implicit constant depends only on A and K' (the dimension of $\mathbf{G}_{A,\ell}$ is bounded in terms of $\dim A$, and hence there are only finite many possible Lie types for the groups $\mathbf{G}_{A,\ell}$ as ℓ varies). □

6. Proofs of Theorems 1.2 and 1.5

Fix an absolutely simple abelian variety A defined over a number field K. We have assumed that $K_A^{\mathrm{conn}} = K$; equivalently, all the groups $\mathbf{G}_{A,\ell}$ are connected. Fix an embedding $K \subseteq \mathbb{C}$ and let $\mathbf{G}_A \subseteq \mathbf{GL}_V$ be the Mumford–Tate group of A where $V = H_1(A(\mathbb{C}), \mathbb{Q})$. Fix a maximal torus $\mathbf{T}$ of $\mathbf{G}_A$. Let $\mathcal{S}_A$ be the set of places from §2.4. We shall assume that the Mumford–Tate conjecture for A holds starting in §6.2.

6.1. **Weights.** We first describe some properties of the representation $\mathbf{G}_A \hookrightarrow \mathbf{GL}_V$. We will use the group theory of [Ser79, §3] (the results on *strong Mumford–Tate pairs* in [Pin98, §4] are also relevant).

By Proposition 2.2(i), the commutant of $\mathbf{G}_A$ in $\mathrm{End}_{\mathbb{Q}}(V)$ is naturally isomorphic to the ring $\Delta := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. The ring Δ is a division algebra since A is simple. The center E of Δ is a number field. Define the integers $r := [E : \mathbb{Q}]$ and $m := [\Delta : E]^{1/2}$. The representation $\mathbf{G}_A \hookrightarrow \mathbf{GL}_V$ is irreducible since Δ is a division algebra.

For each character $\alpha \in X(\mathbf{T})$, let $V(\alpha)$ be the subspace of $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ consisting of those vectors v for which $t \cdot v = \alpha(t)v$ for all $t \in \mathbf{T}(\overline{\mathbb{Q}})$. We say that $\alpha \in X(\mathbf{T})$ is a weight of V if $V(\alpha) \neq 0$, and we denote the set of such weights by Ω. We have a decomposition $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} = \oplus_{\alpha \in \Omega} V(\alpha)$, and hence

$$\det(xI - t) = \prod_{\alpha \in \Omega} (x - \alpha(t))^{m_\alpha} \tag{6.1}$$

for each $t \in \mathbf{T}(\overline{\mathbb{Q}})$, where $m_\alpha := \dim_{\overline{\mathbb{Q}}} V(\alpha)$ is the multiplicity of α. The set Ω of weights is stable under the actions of $W(\mathbf{G}_A, \mathbf{T})$ and $\mathrm{Gal}_{\mathbb{Q}}$ on $X(\mathbf{T})$, so $\Pi(\mathbf{G}_A, \mathbf{T})$ also acts on Ω.

Lemma 6.1.

((i)) *The representation $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ of $\mathbf{G}_{A,\overline{\mathbb{Q}}}$ is the direct sum of r irreducible representations $V_1, \dots, V_r$. Let $\Omega_i \subseteq X(\mathbf{T})$ be the set of weights of V_i. Then Ω is the disjoint union of the sets $\Omega_1, \dots, \Omega_r$.*

((ii)) *The group $W(\mathbf{G}_A, \mathbf{T})$ acts transitively on each set Ω_i. In particular, the action of $W(\mathbf{G}_A, \mathbf{T})$ on Ω has r orbits.*

((iii)) *The group $\Pi(\mathbf{G}_A, \mathbf{T})$ acts transitively on Ω.*

((iv)) *For each $\alpha \in \Omega$, we have $m_\alpha = m$.*

Proof. All of these properties follow from the results of Serre in §3.2 (in particular, see p.183) of [Ser79]; note that the Mumford–Tate group $\mathbf{G}_A$ satisfies the hypotheses of that section. Fix a Borel subgroup $\mathbf{B}$ of $\mathbf{G}_{A,\overline{\mathbb{Q}}}$ that contains $\mathbf{T}$. Serre shows that $\Omega = W(\mathbf{G}_A, \mathbf{T}) \cdot \Omega^+$ where Ω^+ is the set of highest weights of the irreducible representations of $V \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ (the notion of highest weight will depend on our choice of $\mathbf{B}$). The set Ω^+ has r elements. The sets $\Omega_1, \dots, \Omega_r$ in the statement of the lemma are the orbits $W(\mathbf{G}_A, \mathbf{T}) \cdot \alpha$ with $\alpha \in \Omega^+$. The group $\mathrm{Gal}_{\mathbb{Q}}$ acts transitively on Ω_+, so we find that $\Pi(\mathbf{G}_A, \mathbf{T})$ acts transitively on Ω. That $\Pi(\mathbf{G}_A, \mathbf{T})$ acts transitively on Ω implies that each weight $\alpha \in \Omega$ has the same multiplicity; Serre shows that it is m. □

We now give some basic arithmetic consequences of these geometric properties.

Lemma 6.2. *Fix a place $v \in \mathcal{S}_A$ and an element $t \in \mathbf{T}(\overline{\mathbb{Q}})$ that satisfies $\det(xI - t) = P_{A_v}(x)$. Then the map*

$$\gamma \colon X(\mathbf{T}) \to \Phi_{A_v}, \quad \alpha \mapsto \alpha(t)$$

is a well-defined homomorphism that satisfies $\gamma(\Omega) = \mathcal{W}_{A_v}$. The homomorphism γ is surjective; it is an isomorphism if and only if the Mumford–Tate conjecture for A holds.

Proof. The map $\alpha \mapsto \alpha(t)$ certainly gives a homomorphism $\gamma \colon X(\mathbf{T}) \to L^\times$. We need to show that γ has image in Φ_{A_v}. By (6.1), the roots of $\det(xI - t)$ in L are the values $\alpha(t)$ with $\alpha \in \Omega$. Since $P_{A_v}(x) = \det(xI - t)$ by assumption, we have $\mathcal{W}_{A_v} = \{\alpha(t) : \alpha \in \Omega\} = \gamma(\Omega)$. The set Ω generates $X(\mathbf{T})$ since $\mathbf{G}_A$ acts faithfully on V. Since $\gamma(\Omega) = \mathcal{W}_{A_v}$ and $\mathcal{W}_{A_v}$ generates Φ_{A_v}, we deduce that $\gamma(X(\mathbf{T})) = \Phi_{A_v}$. This proves that $\gamma \colon X(\mathbf{T}) \to \Phi_{A_v}$ is a well-defined surjective homomorphism.

The group Φ_{A_v} is a free abelian group of rank $\tilde{r}$ by our definition of $\mathcal{S}_A$ where $\tilde{r}$ is the common rank of the groups $\mathbf{G}_{A,\ell}$. The group $X(\mathbf{T})$ is a free abelian group whose rank equals the rank of $\mathbf{G}_A$. Since γ is a surjective map of free abelian groups, we find that γ is an isomorphism if and only

if $\tilde{r}$ equals the rank of $\mathbf{G}_A$. By Larsen–Pink [LP95, Theorem 4.3], the Mumford–Tate conjecture for A holds if and only if $\tilde{r}$ equals the rank of $\mathbf{G}_A$. □

Using that $\mathcal{S}_A$ has density 1, Theorem 1.2(i) will follow immediately from the next lemma.

Lemma 6.3. *Fix a place $v \in \mathcal{S}_A$.*

((i)) *The abelian variety A_v is isogenous to B^m for an abelian variety B over $\mathbb{F}_v$.*
((ii)) *If the Mumford–Tate conjecture for A holds, then $P_B(x)$ is separable where $B/\mathbb{F}_v$ is as in (i).*
((iii)) *If $P_B(x)$ is irreducible, then the abelian variety $B/\mathbb{F}_v$ in (i) is absolutely simple.*

Proof. Fix a prime ℓ such that $v \nmid \ell$ and choose an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. By Proposition 2.7, $\rho_{A,\ell}(\mathrm{Frob}_v)$ gives a conjugacy class in $\mathbf{G}_A(\mathbb{Q}_\ell)$. Choose an element $t \in \mathbf{T}(\overline{\mathbb{Q}}_\ell)$ that is conjugate to $\rho_{A,\ell}(\mathrm{Frob}_v)$ in $\mathbf{G}_A(\overline{\mathbb{Q}}_\ell)$. By (6.1) and Lemma 6.1((iv)), we have

$$P_{A_v}(x) = \det(xI - t) = \Big(\prod_{\alpha \in \Omega} (x - \alpha(t)) \Big)^m \tag{6.2}$$

and hence $P_{A_v}(x)$ is the m-th power of a monic polynomial $Q(x)$ in $\mathbb{Z}[x]$. Since $\mathbf{T}$ is defined over $\mathbb{Q}$ and has only finitely many elements with characteristic polynomial $P_{A_v}(x)$, we find that t belongs to $\mathbf{T}(\overline{\mathbb{Q}})$.

The field $\mathbb{F}_v$ has prime cardinality $p := N(v)$ since $v \in \mathcal{S}_A$. The polynomial $x^2 - p$ does not divide $P_{A_v}(x)$; if it did, then $-1 = (-\sqrt{p})/\sqrt{p}$ would belong to Φ_{A_v}, which is impossible since Φ_{A_v} is torsion-free by our choice of $\mathcal{S}_A$. Lemma 2.1 thus implies that A_v is isogenous to B^m for some abelian variety $B/\mathbb{F}_v$ which satisfies $P_B(x) = Q(x)$. This proves (i). If the Mumford–Tate conjecture for A holds, then $Q(x)$ is separable by (6.2) and Lemma 6.2; this proves (ii).

Finally, we consider (iii); suppose that $P_B(x)$ is irreducible. Take any positive integer i and let $\mathbb{F}$ be the degree i extension of $\mathbb{F}_v$. We have $P_{B_\mathbb{F}}(x) = \prod_{\pi \in \mathcal{W}_{A_v}} (x - \pi^i)$ since $P_B(x)$ is separable with roots $\mathcal{W}_{A_v}$. For $\sigma \in \mathrm{Gal}_\mathbb{Q}$ and $\pi_1, \pi_2 \in \mathcal{W}_{A_v}$, we claim that $\sigma(\pi_1^i) = \pi_2^i$ if and only if $\sigma(\pi_1) = \pi_2$. If $\sigma(\pi_1) = \pi_2$, then we have $\sigma(\pi_1^i) = \pi_2^i$ by taking i-th powers. If $\sigma(\pi_1^i) = \pi_2^i$, then $\sigma(\pi_1)/\pi_2$ equals 1 since it is an i-th root of unity that belongs to the torsion-free subgroup Φ_{A_v} of $\overline{\mathbb{Q}}^\times$. The group $\mathrm{Gal}_\mathbb{Q}$ acts transitively on $\mathcal{W}_{A_v}$ since $P_B(x)$ is irreducible. The claim then implies that $P_{B_\mathbb{F}}(x) \in \mathbb{Z}[x]$ is irreducible and hence $B_\mathbb{F}$ is simple. The abelian variety B is absolutely simple since i was arbitrary. □

6.2. **Galois action.** For the rest of §6, we shall assume that the Mumford–Tate conjecture for A holds. Fix a place $v \in \mathcal{S}_A$. Choose an element $t_v \in \mathbf{T}(\overline{\mathbb{Q}})$ such that $\mathrm{cl}'_{\mathbf{G}_A}(t_v) = F'_v$, where $F'_v \in \mathrm{Conj}'(\mathbf{G}_A)(\mathbb{Q})$ is as in Theorem 4.1; the place v satisfies the condition of the theorem since Φ_{A_v} is torsion-free. Since $F'_v = \mathrm{cl}'_{\mathbf{G}_A}(\rho_{A,\ell}(\mathrm{Frob}_v))$ for any prime ℓ satisfying $v \nmid \ell$, we may further assume that t_v is chosen so that $\det(xI - t_v) = P_{A_v}(x)$. Let Γ be the subgroup of $\mathrm{Aut}(\mathbf{T}_{\overline{\mathbb{Q}}}) \cong \mathrm{Aut}(X(\mathbf{T}))$ from §4.

By Lemma 6.2, the map

$$\gamma \colon X(\mathbf{T}) \to \Phi_{A_v}, \quad \alpha \mapsto \alpha(t_v)$$

is a homomorphism that satisfies $\gamma(\Omega) = \mathcal{W}_{A_v}$; it is an isomorphism since we have assumed that the Mumford–Tate conjecture for A holds. For each $\sigma \in \mathrm{Gal}_\mathbb{Q}$, we define $\psi_v(\sigma)$ to be the unique automorphism of $X(\mathbf{T})$ for which the following diagram commutes:

$$\begin{array}{ccc} X(\mathbf{T}) & \xrightarrow{\gamma}_{\sim} & \Phi_{A_v} \\ {\scriptstyle \psi_v(\sigma)}\downarrow & & \downarrow{\scriptstyle \sigma} \\ X(\mathbf{T}) & \xrightarrow{\gamma}_{\sim} & \Phi_{A_v}. \end{array}$$

This defines a Galois representation

$$\psi_v\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(X(\mathbf{T})).$$

For each prime ℓ, we choose an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. With respect to this embedding, the restriction map gives an injective homomorphism $\mathrm{Gal}_{\mathbb{Q}_\ell} \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}$. This embedding and our assumption that the Mumford–Tate conjecture for A holds, gives an isomorphism $W(\mathbf{G}_A, \mathbf{T}) \xrightarrow{\sim} W(\mathbf{G}_{A,\mathbb{Q}_\ell}, \mathbf{T}_{\mathbb{Q}_\ell}) = W(\mathbf{G}_{A,\ell}, \mathbf{T}_{\mathbb{Q}_\ell})$. If $\mathbf{T}_{\mathbb{Q}_\ell}$ is split and $v \nmid \ell$, then using this isomorphism of Weyl groups and the construction of §5, we have a group homomorphism

$$\psi_{v,\ell}\colon \mathrm{Gal}_{\mathbb{Q}_\ell} \to W(\mathbf{G}_A, \mathbf{T}).$$

Lemma 6.4. *Fix notation as above and let ℓ be a prime for with $\mathbf{T}_{\mathbb{Q}_\ell}$ is split and $v \nmid \ell$. Then for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}_\ell}$, $\psi_v(\sigma)$ and $\psi_{v,\ell}(\sigma)$ are elements of $W(\mathbf{G}_A, \mathbf{T})$ that lie in the same conjugacy class of Γ.*

Proof. Recall that to define $\psi_{v,\ell}$, we chose an element $t_{v,\ell} \in \mathbf{T}(\overline{\mathbb{Q}}_\ell)$ such that $t_{v,\ell}$ is conjugate to $\rho_{A,\ell}(\mathrm{Frob}_v)$ in $\mathbf{G}_{A,\ell}(\overline{\mathbb{Q}}_\ell) = \mathbf{G}_A(\overline{\mathbb{Q}}_\ell)$. This implies that $\mathrm{cl}'_{\mathbf{G}_A}(t_{v,\ell}) = \mathrm{cl}'_{\mathbf{G}_A}(\rho_{A,\ell}(\mathrm{Frob}_v)) = F'_v$. So, there is a unique $\beta \in \Gamma$ such that $t_{v,\ell} = \beta(t_v)$. Now take any $\sigma \in \mathrm{Gal}_{\mathbb{Q}_\ell}$ and $\alpha \in X(\mathbf{T})$. We have

$$\sigma(\alpha(t_v)) = \sigma(\alpha(\beta^{-1}(t_{v,\ell}))) = \alpha(\beta^{-1}(\sigma(t_{v,\ell})))$$

where we have used that β and α are defined over $\mathbb{Q}_\ell$ since $\mathbf{T}_{\mathbb{Q}_\ell}$ is split. By the definition of $\psi_{v,\ell}$, we have

$$\sigma(\alpha(t_v)) = \alpha(\beta^{-1}(\psi_{v,\ell}(\sigma)^{-1}(t_{v,\ell}))) = \big(\alpha \circ (\beta^{-1} \circ \psi_{v,\ell}(\sigma)^{-1} \circ \beta)\big)(t_v).$$

From our characterization of $\psi_v(\sigma)$, we deduce that $\psi_v(\sigma)$ equals $\beta^{-1} \circ \psi_{v,\ell}(\sigma) \circ \beta$; it is an element of $W(\mathbf{G}_A, \mathbf{T})$ since $\psi_{v,\ell}(\sigma) \in W(\mathbf{G}_A, \mathbf{T})$ and $W(\mathbf{G}_A, \mathbf{T})$ is a normal subgroup of Γ. □

Recall that we defined $k_{\mathbf{G}_A}$ to be the intersection of all the subfields $L \subseteq \overline{\mathbb{Q}}$ for which $\mathbf{G}_{A,L}$ is split; it is a finite Galois extension of $\mathbb{Q}$. The following gives a strong constraint on the image of ψ_v.

Lemma 6.5. *With notation as above, $\psi_v(\mathrm{Gal}_{k_{\mathbf{G}_A}})$ is a subgroup of $W(\mathbf{G}_A, \mathbf{T})$.*

Proof. Let $L \subseteq \overline{\mathbb{Q}}$ be a finite extension of $\mathbb{Q}$ for which $\mathbf{T}_L$ is split. Let Λ be the set of primes ℓ for which ψ_v is unramified at ℓ, $v \nmid \ell$, and ℓ splits completely in L. The torus $\mathbf{T}_{\mathbb{Q}_\ell}$ is split for all $\ell \in \Lambda$. From Lemma 6.4, we find that $\psi_v(\mathrm{Frob}_\ell)$ belongs to $W(\mathbf{G}_A, \mathbf{T})$ for all $\ell \in \Lambda$. The Chebotarev density theorem then ensures that $\psi_v(\mathrm{Gal}_L) \subseteq W(\mathbf{G}_A, \mathbf{T})$.

Now suppose that $L \subseteq \overline{\mathbb{Q}}$ is *any* finite extension of $\mathbb{Q}$ for which $\mathbf{G}_{A,L}$ is split. Choose a maximal torus $\mathbf{T}'$ of $\mathbf{G}_A$ for which $\mathbf{T}'_L$ is split. Fix an element $g \in \mathbf{G}_A(\overline{\mathbb{Q}})$ such that $\mathbf{T}'_{\overline{\mathbb{Q}}} = g\mathbf{T}_{\overline{\mathbb{Q}}}g^{-1}$, and define $t'_v := gt_vg^{-1}$. We have $\mathrm{cl}'_{\mathbf{G}_A}(t'_v) = F'_v$ and $\det(xI - t'_v) = P_{A_v}(x)$. As above, we can define a homomorphism $\psi'_v\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}(X(\mathbf{T}'))$ that is characterized by the property $\sigma(\alpha(t'_v)) = \big(\psi'_v(\sigma)\alpha\big)(t'_v)$ for all $\alpha \in X(\mathbf{T}')$ and $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. The argument from the beginning of the proof shows that $\psi'_v(\mathrm{Gal}_L) \subseteq W(\mathbf{G}_A, \mathbf{T}')$. We now need to relate ψ_v and ψ'_v.

Define the isomorphisms $\beta\colon \mathbf{T}_{\overline{\mathbb{Q}}} \to \mathbf{T}'_{\overline{\mathbb{Q}}}$, $t \mapsto gtg^{-1}$ and $\beta_*\colon \mathrm{Aut}(\mathbf{T}_{\overline{\mathbb{Q}}}) \to \mathrm{Aut}(\mathbf{T}'_{\overline{\mathbb{Q}}})$, $f \mapsto \beta \circ f \circ \beta^{-1}$. One readily checks that $\beta_*(W(\mathbf{G}_A, \mathbf{T})) = W(\mathbf{G}_A, \mathbf{T}')$. Take any $\alpha \in X(\mathbf{T})$ and $\sigma \in \mathrm{Gal}_L$. For the rest of the proof, it will be convenient to view $\psi_v(\sigma)$ and $\psi'_v(\sigma)$ as elements of $\mathrm{Aut}(\mathbf{T}_{\overline{\mathbb{Q}}})$ and $\mathrm{Aut}(\mathbf{T}'_{\overline{\mathbb{Q}}})$, respectively. By the defining property of $\psi'_v(\sigma)$, we have

$$\sigma(\alpha(t_v)) = \sigma((\alpha \circ \beta^{-1})(t'_v)) = (\alpha \circ \beta^{-1} \circ \psi'_v(\sigma)^{-1})(t'_v) = (\alpha \circ \beta^{-1} \circ \psi'_v(\sigma)^{-1} \circ \beta)(t_v).$$

By our characterization of $\psi_v(\sigma)$, we deduce that $\psi_v(\sigma) = \beta^{-1} \circ \psi'_v(\sigma) \circ \beta = \beta_*^{-1}(\psi'_v(\sigma))$. Therefore, $\psi_v(\mathrm{Gal}_L) \subseteq \beta_*^{-1}(W(\mathbf{G}_A, \mathbf{T}')) = W(\mathbf{G}_A, \mathbf{T})$.

We have shown that $\psi_v(\mathrm{Gal}_L) \subseteq W(\mathbf{G}_A, \mathbf{T})$ for every finite extension $L/\mathbb{Q}$ for which $\mathbf{G}_{A,L}$ is split. It is then easy to show that $\psi_v(\mathrm{Gal}_{k_{\mathbf{G}_A}}) \subseteq W(\mathbf{G}_A, \mathbf{T})$. □

We will now prove that ψ_v has large image for most places v.

Proposition 6.6. *Fix a finite extension L of $k_{\mathbf{G}_A}$. Then $\psi_v(\mathrm{Gal}_L) = W(\mathbf{G}_A, \mathbf{T})$ for all places $v \in \mathcal{S}_A$ away from a set of density 0.*

Proof. By Lemma 6.5, we know that $\psi_v(\mathrm{Gal}_L)$ is a subgroup of $W(\mathbf{G}_A, \mathbf{T})$ for all $v \in \mathcal{S}_A$. There is no harm in replacing L by a larger extension, so we may assume that $\mathbf{T}_L$ is split. Let Λ be the set of primes ℓ that split completely in L, and let Λ_Q be the set of $\ell \in \Lambda$ that satisfy $\ell \leq Q$. The torus $\mathbf{T}_{\mathbb{Q}_\ell}$ is split for all $\ell \in \Lambda$. After removing a finite number of primes from Λ, we may assume by Proposition 2.10(i) that $\mathcal{G}_{A,\ell}$ is a reductive scheme over $\mathbb{Z}_\ell$ for all $\ell \in \Lambda$.

Let $\mathscr{T}$ be the Zariski closure of $\mathbf{T}$ in the group scheme $\mathbf{GL}_{H_1(A(\mathbb{C}),\mathbb{Z})}$ over $\mathbb{Z}$; note that the generic fiber of $\mathbf{GL}_{H_1(A(\mathbb{C}),\mathbb{Z})}$ is $\mathbf{GL}_V$. For ℓ sufficiently large, $\mathscr{T}_{\mathbb{Z}_\ell}$ is a torus over $\mathbb{Z}_\ell$. Since the Mumford–Tate conjecture for A has been assumed, we find that $\mathscr{T}_{\mathbb{Z}_\ell}$ is a maximal torus of $\mathcal{G}_{A,\ell}$ for all sufficiently large primes ℓ. So after possibly removing a finite number of primes from Λ, we find that $\mathscr{T}_{\mathbb{Z}_\ell}$ is a split maximal torus of the reductive scheme $\mathcal{G}_{A,\ell}$ for all $\ell \in \Lambda$.

Let K'/K be an extension as in Proposition 2.11. Fix a non-empty subset C of $W(\mathbf{G}_A, \mathbf{T})$ that is stable under conjugation by Γ. For each $\ell \in \Lambda$, we can identify C with a subset of $W(\mathbf{G}_{A,\ell}, \mathbf{T}_{\mathbb{Q}_\ell}) = W((\mathcal{G}_{A,\ell})_{\mathbb{Q}_\ell}, (\mathscr{T}_{\mathbb{Z}_\ell})_{\mathbb{Q}_\ell})$. With our fixed C and K', let U_ℓ be the sets of Lemma 5.1 for $\ell \in \Lambda$.

Let $\mathcal{V}_C$ be the set of places $v \in \mathcal{S}_A$ for which $\bar{\rho}_{A,\ell}(\mathrm{Frob}_v) \not\subseteq U_\ell$ for all $\ell \in \Lambda$ that satisfy $v \nmid \ell$. Let $\mathcal{V}_C(Q)$ be the set of places $v \in \mathcal{S}_A$ such that $\bar{\rho}_{A,\ell}(\mathrm{Frob}_v) \not\subseteq U_\ell$ for all $\ell \in \Lambda_Q$ that satisfy $v \nmid \ell$. By Proposition 2.12 and using that $\mathcal{S}_A$ has density 1, we find that $\mathcal{V}_C(Q)$ has density

$$\delta_Q := \sum_{\mathcal{C}} \frac{|\mathcal{C}|}{|\mathrm{Gal}(K'/K)|} \cdot \prod_{\ell \in \Lambda_Q} \frac{|\bar{\rho}_{A,\ell}(\Gamma_{\mathcal{C}}) \cap (\bar{\rho}_{A,\ell}(\mathrm{Gal}_K) - U_\ell)|}{|\bar{\rho}_{A,\ell}(\Gamma_{\mathcal{C}})|}$$

where $\mathcal{C}$ varies over the conjugacy classes of $\mathrm{Gal}(K'/K)$ and $\Gamma_{\mathcal{C}}$ is the set of $\sigma \in \mathrm{Gal}_K$ for which $\sigma|_{K'} \in \mathcal{C}$. Using the bounds of Lemma 5.1, we have

$$\delta_Q \ll \prod_{\ell \in \Lambda_Q} \Big(1 - \frac{|C|}{|W(\mathbf{G}_{A,\ell}, \mathbf{T}_{\mathbb{Q}_\ell})|} + O(1/\ell)\Big) = \prod_{\ell \in \Lambda_Q} \Big(1 - \frac{|C|}{|W(\mathbf{G}_A, \mathbf{T})|} + O(1/\ell)\Big).$$

where the implicit constants do not depend on Q. Since Λ is infinite and C is non-empty, we find that $\lim_{Q \to +\infty} \delta_Q = 0$. Since $\mathcal{V}_C$ is a subset of $\mathcal{V}_C(Q)$ for every Q, we deduce that the density of $\mathcal{V}_C$ exists and equals 0.

Now take any place $v \in \mathcal{S}_A - \mathcal{V}_C$. There is some prime $\ell \in \Lambda$ for which $v \nmid \ell$ and $\bar{\rho}_{A,\ell}(\mathrm{Frob}_v) \subseteq U_\ell$. By the properties of U_ℓ from Lemma 5.1, we find that $\psi_{v,\ell}$ is unramified at ℓ and $\psi_{v,\ell}(\mathrm{Frob}_\ell) \subseteq C$. Since C is stable under conjugation by Γ, Lemma 6.4 implies that $\psi_v(\mathrm{Frob}_\ell) \subseteq C$. Since ℓ splits completely in L, we deduce that $\psi_v(\mathrm{Gal}_L) \cap C \neq \emptyset$.

For each $v \in \mathcal{S}_A$, we have $\psi_v(\mathrm{Gal}_L) \subseteq W(\mathbf{G}_A, \mathbf{T})$ by Lemma 6.5. By considering the finitely many C, we find that for all places $v \in \mathcal{S}_A$ away from a set of density 0, we have $\psi_v(\mathrm{Gal}_L) \cap C \neq \emptyset$ for every non-empty subset C of $W(\mathbf{G}_A, \mathbf{T})$ that is stable under conjugation by Γ. By Lemma 4.2, we deduce that $\psi_v(\mathrm{Gal}_L) = W(\mathbf{G}_A, \mathbf{T})$ for all places $v \in \mathcal{S}_A$ away from a set of density 0. □

6.3. **Proof of Theorem 1.5.** Take $v \in \mathcal{S}_A$. The group Φ_{A_v} is generated by $\mathcal{W}_{A_v}$. Using this and Lemma 6.5, we find that $\psi_v|_{\mathrm{Gal}_L}$ factors through an injective homomorphism $\mathrm{Gal}(L(\mathcal{W}_{A_v})/L) \hookrightarrow W(\mathbf{G}_A, \mathbf{T}) \cong W(\mathbf{G}_A)$. It is an isomorphism for all $v \in \mathcal{S}_A$ away from a set of density 0 by Proposition 6.6. The theorem follows by noting that $\mathcal{S}_A$ has density 1.

6.4. **Proof of Theorem 1.2(ii).** Fix a place $v \in \mathcal{S}_A$. The following lemma says that if the image of ψ_v is as large as possible, then $P_{A_v}(x)$ factors in the desired manner. Take any embedding $E \subseteq \overline{\mathbb{Q}}$ and let $\widetilde{E}$ be the Galois closure of E over $\mathbb{Q}$.

Lemma 6.7. *Let L be a finite extension of $k_{\mathbf{G}_A}$ which contains $\widetilde{E}$. If $\psi_v(\mathrm{Gal}_L) = W(\mathbf{G}_A, \mathbf{T})$, then $P_{A_v}(x)$ is the m-th power of an irreducible polynomial.*

Proof. The isomorphism $\gamma\colon X(\mathbf{T}) \to \Phi_{A_v}$ of §6.2 gives a bijection between Ω and $\mathcal{W}_{A_v}$. By Lemma 6.1(ii), the action of $W(\mathbf{G}_A, \mathbf{T})$ partitions Ω into r orbits. Since $\psi_v(\mathrm{Gal}_L) = W(\mathbf{G}_A, \mathbf{T})$ by assumption, we deduce that the Gal_L-action partitions $\mathcal{W}_{A_v}$ into r orbits. Since $\mathcal{W}_{A,v}$ is the set of roots of $P_{A,v}(x)$, we deduce that $P_{A_v}(x)$ has r distinct irreducible factors in $L[x]$ (each distinct irreducible factor corresponds to a Gal_L-orbit of $\mathcal{W}_{A_v}$). From Lemma 6.3, we know that $P_{A_v}(x)$ is the m-th power of a separable polynomial. So, there are distinct monic irreducible polynomials $Q_1(x), \dots, Q_r(x) \in L[x]$ such that

$$P_{A_v}(x) = Q_1(x)^m \cdots Q_r(x)^m. \tag{6.3}$$

We will describe these r irreducible factors, but we first recall some basic facts about λ-adic representations where λ is a finite place of E. A good exposition on λ-adic representations can be found in [Rib76, I–II].

The ring $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, and hence also the field E, acts on $V = H_1(A(\mathbb{C}), \mathbb{Q})$. Therefore, $V_\ell(A) = V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is a module over $E_\ell := E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. We have $E_\ell = \prod_{\lambda|\ell} E_\lambda$, where λ runs over the places of E dividing ℓ. Setting $V_\lambda(A) := V_\ell(A) \otimes_{E_\ell} E_\lambda$, we have a decomposition $V_\ell(A) = \bigoplus_{\lambda|\ell} V_\lambda(A)$. Since $E \subseteq \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, the action of Gal_K on $V_\ell(A)$ is E_ℓ-linear. Therefore, Gal_K acts E_λ-linearly on $V_\lambda(A)$ and hence defines a Galois representation

$$\rho_{A,\lambda}\colon \mathrm{Gal}_K \to \mathrm{Aut}_{E_\lambda}(V_\lambda(A)).$$

(Of course when $E = \mathbb{Q}$, we have our usual ℓ-adic representations.) For each λ, we will denote the rational prime it divides by $\ell(\lambda)$. Since A has good reduction at v, there is a polynomial $P_{A_v,E}(x) \in E[x]$ such that

$$P_{A_v,E}(x) = \det(xI - \rho_{A,\lambda}(\mathrm{Frob}_v))$$

for all finite places λ of E for which $v \nmid \ell(\lambda)$. The connection with our polynomial $P_{A_v}(x) \in \mathbb{Q}[x]$ is that

$$P_{A_v}(x) = N_{E/\mathbb{Q}}(P_{A_v,E}(x)),$$

cf. [Shi67, 11.8–11.10] (the polynomial $N_{E/\mathbb{Q}}(P_{A_v,E}(x))$ is the product of the $\sigma(P_{A_v,E}(x))$ where σ varies over the embeddings $E \hookrightarrow L$).

Choose a prime ℓ that splits completely in E for which $v \nmid \ell$. We then have a decomposition $V_\ell(A) = \prod_{\lambda|\ell} V_\lambda(A)$ and Gal_K acts on each of the $r = [E : \mathbb{Q}]$ vector spaces $V_\lambda(A)$. This implies that $V_\lambda(A)$ is a representation of $\mathbf{G}_{A,\ell} = \mathbf{G}_{A,\mathbb{Q}_\ell}$ for each λ dividing ℓ.

Using Lemma 6.1, we deduce that $V_\lambda(A) \subseteq V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is an absolutely irreducible representation of $\mathbf{G}_{A,\mathbb{Q}_\ell}$ and that each weight has multiplicity m. Therefore, $P_{A_v,E}(x)$ is the m-th power of a unique monic polynomial $Q_v(x) \in E[x]$, and hence $P_{A_v}(x) = N_{E/\mathbb{Q}}(P_{A_v,E}(x)) = N_{E/\mathbb{Q}}(Q_v(x))^m$. So,

$$P_{A_v}(x) = \prod_{\sigma\colon E \hookrightarrow L} \sigma(Q_v(x))^m$$

where the product is over the r field embeddings of E into L (this uses our assumption that $\widetilde{E} \subseteq L$). From our factorization (6.3), we deduce that the polynomials $\sigma(Q_v(x))$ are irreducible over $L[x]$. In particular, $Q_v(x)$ is irreducible over E. That $Q_v(x)$ is irreducible in $E[x]$ implies that $P_{A_v}(x) = N_{E/\mathbb{Q}}(Q_v(x))^m$ is a power of some irreducible polynomial over $\mathbb{Q}$. Since $P_{A_v}(x) \in \mathbb{Z}[x]$ is the m-th power of a separable polynomial, we deduce that $P_{A_v}(x)$ is the m-th power of an irreducible polynomial. □

Fix a finite extension L of $k_{\mathbf{G}_A}$ which contains $\widetilde{E}$. By Proposition 6.6, there is a subset $\mathcal{T} \subseteq \Sigma_K$ with density 0 such that $\psi_v(\mathrm{Gal}_L) = W(\mathbf{G}_A, \mathbf{T})$ for all $v \in \mathcal{S}_A - \mathcal{T}$. By Lemmas 6.7 and 6.3, we deduce that for all $v \in \mathcal{S}_A - \mathcal{T}$, A_v is isogenous to B^m where B is an absolutely simple abelian variety over $\mathbb{F}_v$. Our theorem follows by noting that $\mathcal{S}_A$ has density 1 and $\mathcal{T}$ has density 0.

7. Proof of Theorem 1.4

After replacing A by an isogenous abelian variety, we may assume that $A = \prod_{i=1}^s A_i^{n_i}$, where the A_i are simple abelian varieties over K which are pairwise non-isogenous.

Lemma 7.1. *Fix an integer $1 \leq i \leq s$. The abelian variety A_i/K is absolutely simple, $K_{A_i}^{\mathrm{conn}} = K$, and the Mumford–Tate conjecture for A_i holds.*

Proof. Take any prime ℓ. We have $V_\ell(A) = \prod_{i=1}^s V_\ell(A_i)^{n_i}$ and each $V_\ell(A_i)$ is stable under the action of Gal_K. Projecting $V_\ell(A)$ to one of the factors $V_\ell(A_i)$ defines a homomorphism $\pi\colon \mathbf{G}_{A,\ell} \to \mathbf{G}_{A_i,\ell}$ of algebraic groups for which $\pi(\mathbf{G}_{A,\ell})$ is Zariski dense in $\mathbf{G}_{A_i,\ell}$. Since $\mathbf{G}_{A,\ell}$ is connected by our assumption $K_A^{\mathrm{conn}} = K$, we deduce that $\mathbf{G}_{A_i,\ell}$ is also connected. Therefore, $K_{A_i}^{\mathrm{conn}} = K$.

Since A_i is simple, we know by Faltings that $V_\ell(A_i)$ is an irreducible $\mathbb{Q}_\ell[\mathrm{Gal}_K]$-module, and is hence an irreducible representation of $\mathbf{G}_{A_i,\ell}$. Take any finite extension L of K. The group $\rho_{A,\ell}(\mathrm{Gal}_L)$ is Zariski dense in $\mathbf{G}_{A,\ell}$ since $\mathbf{G}_{A,\ell}$ is connected, so $\rho_{A_i,\ell}(\mathrm{Gal}_L)$ is Zariski dense in $\mathbf{G}_{A_i,\ell}$. Therefore, $V_\ell(A_i)$ is an irreducible $\mathbb{Q}_\ell[\mathrm{Gal}_L]$-module, and hence $A_{i,L}$ is simple. Since L was an arbitrary finite extension of K, we deduce that A_i is absolutely simple.

Again by viewing A_i as one of the factors of A, we can view $H_1(A_i(\mathbb{C}), \mathbb{Q})$ as a subspace of $H_1(A(\mathbb{C}), \mathbb{Q})$, which induces a homomorphism $\mathbf{G}_A \to \mathbf{G}_{A_i}$. One can show that this is compatible with the corresponding map π, and that the Mumford–Tate conjecture for A_i follows from our assumption that the Mumford–Tate conjecture for A holds. □

Fix an integer $1 \leq i \leq s$. Lemma 7.1 allows us to apply Theorem 1.2(ii) to each A_i. By Theorem 1.2(ii), there is a subset $\mathcal{T}_i \subseteq \Sigma_K$ with density 0 such that for all $v \in \Sigma_K - \mathcal{T}_i$, A_i modulo v is isogenous to $B_{i,v}^{m_i}$, where $B_{i,v}$ is an absolutely simple abelian variety over $\mathbb{F}_v$. Set $\mathcal{T} = \bigcup_{i=1}^s \mathcal{T}_i$; it has density 0. For all $v \in \Sigma_K - \mathcal{T}$, we find that A_v is isogenous to a product $\prod_{i=1}^s B_{i,v}^{m_i n_i}$ where each $B_{i,v}$ is absolutely simple over $\mathbb{F}_v$.

It remains to show that the abelian varieties $B_{1,v}, \dots, B_{s,v}$ are pairwise non-isogenous for all $v \in \Sigma_k - \mathcal{T}$ away from a set of density 0. It suffices to consider fixed $1 \leq i < j \leq s$. Fix a prime ℓ. If $B_{i,v}$ is isogenous to $B_{j,v}$, then $A_i^{m_j}$ and $A_j^{m_i}$ modulo v are isogenous, and hence

$$m_j \operatorname{tr}(\rho_{A_i,\ell}(\mathrm{Frob}_v)) = \operatorname{tr}(\rho_{A_i^{m_j},\ell}(\mathrm{Frob}_v)) = \operatorname{tr}(\rho_{A_j^{m_i},\ell}(\mathrm{Frob}_v)) = m_i \operatorname{tr}(\rho_{A_j,\ell}(\mathrm{Frob}_v))$$

if $v \nmid \ell$. Let $\mathcal{P}$ be the set of $v \in \Sigma_K$ for which A_i and A_j have good reduction at v and $m_j \operatorname{tr}(\rho_{A_i,\ell}(\mathrm{Frob}_v)) = m_i \operatorname{tr}(\rho_{A_j,\ell}(\mathrm{Frob}_v))$. To finish the proof, it suffices to show that $\mathcal{P}$ has density 0.

We can view $\mathbf{G}_{A_i \times A_j,\ell}$ as an algebraic subgroup of $\mathbf{G}_{A_i,\ell} \times \mathbf{G}_{A_j,\ell}$. Let $W/\mathbb{Q}_\ell$ be the subvariety of $\mathbf{G}_{A_i,\ell} \times \mathbf{G}_{A_j,\ell}$ defined by the equation $m_j \operatorname{tr}(g) = m_i \operatorname{tr}(g')$ with $(g, g') \in \mathbf{G}_{A_i,\ell} \times \mathbf{G}_{A_j,\ell}$.

First suppose that $\mathbf{G}_{A_i \times A_j,\ell} \subseteq W$. Then $\operatorname{tr} \circ \rho_{A_i^{m_j},\ell} = m_j \cdot \operatorname{tr} \circ \rho_{A_i,\ell} = m_i \cdot \operatorname{tr} \circ \rho_{A_j,\ell} = \operatorname{tr} \circ \rho_{A_j^{m_i},\ell}$, and hence $A_i^{m_j}$ and $A_j^{m_i}$ are isogenous by the work of Faltings. Since A_i and A_j are simple, we deduce that they are isogenous; this contradicts our factorization of A.

Therefore, $\mathbf{G}_{A_i \times A_j,\ell} \not\subseteq W$. Arguing as in Lemma 7.1, we find that the group $\mathbf{G}_{A_i \times A_j,\ell}$ is connected. Since $\mathbf{G}_{A_i \times A_j,\ell}$ is connected, $\mathbf{G}_{A_i \times A_j,\ell} \cap W$ is of codimension at least 1 in $\mathbf{G}_{A_i \times A_j,\ell}$. The Chebotarev density theorem then implies that $\mathcal{P}$ has density 0, as desired.

8. Remarks on Conjecture 1.6

We restate Conjecture 1.6, but now emphasize that $\Pi(\mathbf{G}_A)$ is the group defined in §3.2.

Conjecture 8.1. *Let A be a non-zero abelian variety defined over a number field K that satisfies $K_A^{\mathrm{conn}} = K$. Then $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A_v})/\mathbb{Q}) \cong \Pi(\mathbf{G}_A)$ for all $v \in \Sigma_K$ away from a subset with natural density 0.*

When A is also absolutely simple, we shall show that this conjecture follows from other well-known conjectures which have already been discussed.

Theorem 8.2. *Let A be an absolutely simple abelian variety defined over a number field K that satisfies $K_A^{\mathrm{conn}} = K$. Suppose that the Mumford–Tate conjecture for A holds and that a class $F_v \in \mathrm{Conj}(\mathbf{G}_A)(\mathbb{Q})$ as in Conjecture 2.8 exists for all $v \in \Sigma_K$ away from a set of density 0. Then Conjecture 8.1 for A is true.*

Remark 8.3.

((i)) Let A be an absolutely simple abelian variety defined over a number field K such that $K_A^{\mathrm{conn}} = K$ and such that the Mumford–Tate conjecture for A holds. Suppose further that $(\mathbf{G}_A^{\mathrm{der}})_{\overline{\mathbb{Q}}}$ has no normal subgroups isomorphic to $\mathbf{SO}(2k)_{\overline{\mathbb{Q}}}$ with $k \geq 4$. Theorem 4.1 then implies that a class $F_v \in \mathrm{Conj}(\mathbf{G}_A)(\mathbb{Q})$ as in Conjecture 2.8 exists for all $v \in \mathcal{S}_A$ (where $\mathcal{S}_A$ is the set of density 1 from §2.4).

((ii)) Theorem 8.2 should remain true without the assumption that A is absolutely simple. We required this assumption in order to apply Proposition 6.6. That proposition in turn needed the assumption in order to use Proposition 2.10 (note that in [Win02, §3.4], Wintenberger shows that the special fiber of $\mathcal{G}_{A,\ell}$ agrees with the reductive group constructed by Serre, but only in the case where A is absolutely simple).

((iii)) Under the stronger hypotheses of Theorem 8.2 it is easier to prove Theorem 1.2. Using that $\Pi(\mathbf{G}_A, \mathbf{T})$ acts transitively on the set of weights Ω (Lemma 6.1), one can show that if $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A_v})/\mathbb{Q})) \cong \Pi(\mathbf{G}_A)$, then $\mathrm{Gal}_{\mathbb{Q}}$ acts transitively on the set $\mathcal{W}_{A_v}$. This avoids the more complicated argument in the proof of Lemma 6.7.

8.1. **Example: abelian varieties of Mumford type.** There are abelian varieties A/K of dimension 4 with $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$ for which $\mathbf{G}_A \neq \mathbf{GSp}_{8,\mathbb{Q}}$. We say that such an abelian variety is of Mumford type. Such abelian varieties were show to exist by Mumford [Mum69]. For further details about such varieties, see [Noo00].

Let A be an abelian variety over a number field K that is of Mumford type and satisfies $K_A^{\mathrm{conn}} = K$. Let $\mathbf{G}_A^{\mathrm{der}}$ be the derived subgroup of $\mathbf{G}_A$. One can show that the group $\mathbf{G}_A^{\mathrm{der}}$ is simple over $\mathbb{Q}$ and that $(\mathbf{G}_A^{\mathrm{der}})_{\overline{\mathbb{Q}}}$ is isogenous to $\mathbf{SL}_{2,\overline{\mathbb{Q}}}^3$. The Mumford–Tate conjecture for A holds by Pink [Pin98, Theorem 5.15]. By Theorem 1.2, we deduce that the reduction $A_v/\mathbb{F}_v$ is absolutely simple for all $v \in \Sigma_K$ away from a set of density 0; this is Theorem C of [Ach11].

By Theorem 8.2 and Remark 8.3(i), we also deduce that $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A_v})/\mathbb{Q})$ is isomorphic to $\Pi(\mathbf{G}_A)$ for all $v \in \Sigma_K$ away from a set of density 0. Let us describe the possibilities for the group $\Pi(\mathbf{G}_A)$. The center of $\mathbf{G}_A$ is the group of homotheties $\mathbf{G}_m$ since $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$. Since the center of $\mathbf{G}_A$ is split, we find that the groups $\Pi(\mathbf{G}_A)$ and $\Pi(\mathbf{G}_A^{\mathrm{der}})$ are isomorphic. Let Φ be a root system associated to $\mathbf{G}_A^{\mathrm{der}}$. Using that $\mathbf{G}_A^{\mathrm{der}}$ is semisimple, we see that the group $\Pi(\mathbf{G}_A)$ is isomorphic to a subgroup of $\mathrm{Aut}(\Phi)$ that contains the Weyl group $W(\Phi) \cong W(\mathbf{G}_A) \cong (\mathbb{Z}/2\mathbb{Z})^3$. The group $\mathrm{Aut}(\Phi)$ is isomorphic to the semidirect product $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$, where S_3 acts on $(\mathbb{Z}/2\mathbb{Z})^3$ by permuting coordinates. Using that the algebraic group $\mathbf{G}_A^{\mathrm{der}}$ is simple over $\mathbb{Q}$, we find that $\Pi(\mathbf{G}_A)$ must contain an element of order 3. Therefore, $\Pi(\mathbf{G}_A)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$ or $(\mathbb{Z}/2\mathbb{Z})^3 \rtimes A_3$. (See also Lemma 3.5 of [?Noot:2001].)

Remark 8.4. We have just shown that $P_{A_v}(x)$ is irreducible and $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A_v})/\mathbb{Q}) \cong \Pi(\mathbf{G}_A)$ for all $v \in \Sigma_K$ away from a set of density 0. Fix such a place v. Even though $P_{A_v}(x)$ is irreducible, we find that $P_{A_v}(x) \pmod{\ell}$ is reducible in $\mathbb{F}_\ell[x]$ for *every* prime ℓ (one uses that the polynomial $P_{A_v}(x)$ has degree 8 while $\Pi(\mathbf{G}_A)$ has no elements of order 8).

8.2. **Proof of Theorem 8.2.** Fix an embedding $K \subseteq \mathbb{C}$ and let $\mathbf{G}_A$ be the Mumford–Tate group of A. Choose a maximal torus $\mathbf{T}$ of $\mathbf{G}_A$. By assumption, there is a set $\mathcal{S} \subseteq \Sigma_K$ with density 1 such that an element $F_v \in \mathrm{Conj}(\mathbf{G}_A)(\mathbb{Q})$ as in Conjecture 2.8 exists for all $v \in \mathcal{S}$. Let $\mathcal{S}_A$ be the density 1 subset of Σ_K from §2.4. Without loss of generality, we may assume that $\mathcal{S} \subseteq \mathcal{S}_A$.

Take a place $v \in \mathcal{S}$, and define the set

$$\mathcal{J}_v := \big\{t \in \mathbf{T}(\overline{\mathbb{Q}}) : \mathrm{cl}_{\mathbf{G}_A}(t) = F_v\big\}.$$

Choose an element $t_v \in \mathcal{J}_v$; it satisfies $\det(xI - t_v) = P_{A_v}(x)$. By Lemma 6.2, the map $\gamma_v \colon X(\mathbf{T}) \to \Phi_{A_v}$, $\alpha \mapsto \alpha(t_v)$ is an isomorphism of free abelian groups (this uses our assumption that the Mumford–Tate conjecture for A holds). There is thus a unique homomorphism $\psi_v \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{Aut}(X(\mathbf{T}))$ such that $\sigma(\alpha(t_v)) = \big(\psi_v(\sigma)\alpha\big)(t_v)$ for all $\sigma \in \mathrm{Gal}_\mathbb{Q}$ and $\alpha \in X(\mathbf{T})$.

We will now show that the image of ψ_v lies in $\Pi(\mathbf{G}_A, \mathbf{T})$. Conjugation induces an action of $W(\mathbf{G}_A, \mathbf{T})$ on $\mathcal{J}_v$; this action is simply transitive (the group $W(\mathbf{G}_A, \mathbf{T})$ acts faithfully on $\mathbf{T}_{\overline{\mathbb{Q}}}$ since the subgroup generated by each $t \in \mathcal{J}_v$ is Zariski dense in $\mathbf{T}_{\overline{\mathbb{Q}}}$). Since F_v and $\mathrm{cl}_{\mathbf{G}_A}$ are defined over $\mathbb{Q}$, the set $\mathcal{J}_v$ is also stable under the action of $\mathrm{Gal}_\mathbb{Q}$. So for each $\sigma \in \mathrm{Gal}_\mathbb{Q}$, there is a unique $w_\sigma \in W(\mathbf{G}_A, \mathbf{T})$ such that $\sigma(t_v) = w_\sigma^{-1}(t_v)$. For $\alpha \in X(\mathbf{T})$, we have

$$\sigma(\alpha(t_v)) = \sigma(\alpha)(\sigma(t_v)) = \sigma(\alpha)(w_\sigma^{-1}(t_v)) = (\sigma(\alpha) \circ w_\sigma^{-1})(t_v).$$

Therefore,

$$\psi_v(\sigma)\alpha = \sigma(\alpha) \circ w_\sigma \tag{8.1}$$

for all $\sigma \in \mathrm{Gal}_\mathbb{Q}$ and $\alpha \in X(\mathbf{T})$. Since $w_\sigma \in W(\mathbf{G}_A, \mathbf{T})$, we find that $\psi_v(\sigma)$ belongs to $\Pi(\mathbf{G}_A, \mathbf{T})$ for all $\sigma \in \mathrm{Gal}_\mathbb{Q}$.

Recall that $W(\mathbf{G}_A, \mathbf{T})$ is a normal subgroup of $\Pi(\mathbf{G}_A, \mathbf{T})$. Define the homomorphism

$$\overline{\psi}_v \colon \mathrm{Gal}_\mathbb{Q} \xrightarrow{\psi_v} \Pi(\mathbf{G}_A, \mathbf{T}) \twoheadrightarrow \Pi(\mathbf{G}_A, \mathbf{T})/W(\mathbf{G}_A, \mathbf{T}).$$

From (8.1), we see that $\overline{\psi}_v$ agrees with the composition of the homomorphism $\varphi_\mathbf{T} \colon \mathrm{Gal}_\mathbb{Q} \to \Pi(\mathbf{G}_A, \mathbf{T})$ from §3 with the quotient map $\Pi(\mathbf{G}_A, \mathbf{T}) \to \Pi(\mathbf{G}_A, \mathbf{T})/W(\mathbf{G}_A, \mathbf{T})$. In particular, we find that $\overline{\psi}_v$ is surjective. Therefore, we have $\psi_v(\mathrm{Gal}_\mathbb{Q}) = \Pi(\mathbf{G}_A, \mathbf{T})$ if and only if $\psi_v(\mathrm{Gal}_\mathbb{Q}) \supseteq W(\mathbf{G}_A, \mathbf{T})$.

Using Proposition 6.6, we deduce that $\psi_v(\mathrm{Gal}_\mathbb{Q}) = \Pi(\mathbf{G}_A, \mathbf{T})$ for all $v \in \mathcal{S}$ away from a set of density 0 (in fact, it would be much easier to prove Proposition 6.6 in the current setting since we do not have the extraneous group Γ to deal with) . Using that $\mathcal{W}_{A_v}$ generates Φ_{A_v}, we find that ψ_v factors through an injective homomorphism $\mathrm{Gal}(\mathbb{Q}(\mathcal{W}_{A_v})/\mathbb{Q}) \hookrightarrow \Pi(\mathbf{G}_A, \mathbf{T}) \cong \Pi(\mathbf{G}_A)$; the theorem follows immediately.

9. Effective bounds

For each place $v \in \Sigma_K$, we define $N(v)$ to be the cardinality of the field $\mathbb{F}_v$. For each subset $\mathscr{S}$ of Σ_K and real number x, we define $\mathscr{S}(x)$ to be the set of $v \in \mathscr{S}$ that satisfy $N(v) \leq x$.

Let A be an absolutely simple abelian variety defined over a number field K such that $K_A^{\mathrm{conn}} = K$. Define the integer $m = [\mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q} : E]^{1/2}$, where E is the center of the division algebra $\mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q}$. Let d and r be the dimension and rank, respectively, of $\mathbf{G}_A$. The following makes Theorem 1.2(i) effective.

Proposition 9.1. *Let $\mathscr{S}$ be the set of places $v \in \Sigma_K$ such that A_v is* not *isogenous to B^m for some abelian variety B over $\mathbb{F}_v$. Then $|\mathscr{S}(x)| \ll \frac{x}{(\log x)^{1+1/d}} \cdot ((\log\log x)^2 \log\log\log x)^{1/d}$. If the Generalized Riemann Hypothesis (GRH) is true, then $|\mathscr{S}(x)| \ll x^{1-\frac{1}{2d}} (\log x)^{-1+2/d}$.*

We can also state an effective version of Theorems 1.2(ii) and 1.5.

Theorem 9.2. *Suppose that the representations $\{\rho_{A,\ell}\}_\ell$ are* independent*, that is, $\big(\prod_\ell \rho_{A,\ell}\big)(\mathrm{Gal}_K) = \prod_\ell \rho_{A,\ell}(\mathrm{Gal}_K)$ (by Proposition 2.11 this can be achieved by replacing K with a finite extension). Assume that the Mumford–Tate conjecture for A holds.*

Let $\mathscr{S}_1$ be the set of places $v \in \Sigma_K$ for which A_v is not *isogenous to B^m for some absolutely simple abelian variety $B/\mathbb{F}_v$. Fix a finite extension L of $k_{\mathbf{G}_A}$ and let $\mathscr{S}_2$ be the set of places $v \in \Sigma_K$ for which $\mathrm{Gal}(L(\mathcal{W}_{A_v})/L)$ is* not *isomorphic to $W(\mathbf{G}_A)$.*

Then

$$|\mathscr{S}_i(x)| \ll \frac{x(\log\log x)^{1+1/(3d)}}{(\log x)^{1+1/(6d)}}.$$

If the GRH is true, then

$$|\mathscr{S}_i(x)| \ll x^{1-\frac{1}{4d+2r+2}} (\log x)^{\frac{2}{2d+r+1}}.$$

These bounds will be an application of the large sieve as developed in [Zyw08]. Cases where $\mathbf{G}_A \cong \mathbf{GSp}_{2\dim(A),\mathbb{Q}}$ were handled in [Zyw08, §1.4] and many other cases were proved by Achter, see [Ach11, Theorem B]. For comparison, note that $|\Sigma_K(x)| \sim x/\log x$ as $x \to +\infty$.

9.1. ℓ-adic subvarieties.

Lemma 9.3. *Fix a prime ℓ and a proper subvariety V of $\mathbf{G}_{A,\ell}$ that is stable under conjugation. Let $\mathscr{S}$ be the set of place $v \in \Sigma_K$ for which A has good reduction, $v \nmid \ell$, and $\rho_{A,\ell}(\mathrm{Frob}_v) \subseteq V(\mathbb{Q}_\ell)$. Then*

$$|\mathscr{S}(x)| \ll \frac{x}{(\log x)^{1+1/d}} \cdot ((\log\log x)^2 \log\log\log x)^{1/d}.$$

If GRH holds, then $|\mathscr{S}(x)| \ll x^{1-\frac{1}{2d}} (\log x)^{-1+2/d}$.

Proof. Let d' be the dimension of $\mathbf{G}_{A,\ell}$. The variety V has dimension at most $d'-1$ since it is a proper subvariety of the connected group $\mathbf{G}_{A,\ell}$. By Proposition 2.3, $\rho_{A,\ell}(\mathrm{Gal}_K)$ has dimension d' as an ℓ-adic Lie group. As an ℓ-adic analytic variety, $V(\mathbb{Q}_\ell) \cap \rho_{A,\ell}(\mathrm{Gal}_K)$ has dimension at most $d'-1$. By Serre [Ser81, Théorème 10(i)], we have

$$|\mathscr{S}(x)| \ll \frac{x}{\log x}\Big(\frac{(\log\log x)^2 \log\log\log x}{\log x}\Big)^{1/d'} = \frac{x}{(\log x)^{1+1/d'}} \cdot ((\log\log x)^2 \log\log\log x)^{1/d'}$$

Assuming GRH, [Ser81, Théorème 10(ii)] implies that

$$|\mathscr{S}(x)| \ll \frac{x}{\log x}\Big(\frac{(\log x)^2}{x^{1/2}}\Big)^{1/d'} = x^{1-\frac{1}{2d'}} (\log x)^{-1+2/d'}.$$

We have $d' \le d$ by Proposition 2.7; the lemma then quickly follows. □

We can now consider our set $\mathcal{S}_A$ from §2.4.

Lemma 9.4. *We have $|\Sigma_K(x) - \mathcal{S}_A(x)| \ll \frac{x}{(\log x)^{1+1/d}} \cdot ((\log\log x)^2 \log\log\log x)^{1/d}$. If GRH holds, then $|\Sigma_K(x) - \mathcal{S}_A(x)| \ll x^{1-\frac{1}{2d}} (\log x)^{-1+2/d}$.*

Proof. There are only finitely many places v for which A has bad reduction. If $v \in \Sigma_K(x)$ satisfies $N(v) = p^e$ with $e > 1$, then $p \le \sqrt{x}$. Using that at most $[K : \mathbb{Q}]$ places of K lie over a given prime p, we find that $|\{v \in \Sigma_K(x) : N(v) \text{ not prime}\}| \le [K : \mathbb{Q}]\sqrt{x}$.

Fix a prime ℓ. It thus suffices to consider the set $\mathscr{S}$ of places $v \in \Sigma_K$ for which A has good reduction and $v \nmid \ell$ such that Φ_{A_v} is *not* a free abelian group with rank equal to the common rank of the groups $\mathbf{G}_{A,\ell}$. Pink and Larsen [LP97a, §2] show that there is a proper subvariety V of $\mathbf{G}_{A,\ell}$ stable under conjugation such that if $\rho_{A,\ell}(\mathrm{Frob}_v) \notin V(\mathbb{Q}_\ell)$, then $v \in \mathscr{S}$. [Let $\mathbf{T}_v$ be the algebraic subgroup of $\mathbf{G}_{A,\ell}$ generated by a representative of $\rho_{A,\ell}(\mathrm{Frob}_v)$. Then Φ_{A_v} is a free abelian group with rank equal to the rank of $\mathbf{G}_{A,\ell}$ if and only if $\mathbf{T}_v$ is a maximal torus of $\mathbf{G}_{A,\ell}$ and $\rho_{A,\ell}(\mathrm{Frob}_v)$ is "neat".] The required bounds for $|\mathscr{S}(x)|$ then follow from Lemma 9.3. □

Proof of Proposition 9.1. The proposition follows from Lemmas 6.3 and 9.4. □

9.2. **Proof of Theorem 9.2.** For a finite group G, we denote its set of conjugacy classes by $G^\sharp$.

Lemma 9.5. *Let $\mathbf{G}$ be a split and connected reductive group defined over a finite field $\mathbb{F}_q$. Let d and r be the dimension and rank of $\mathbf{G}$, respectively.*

((i)) *We have $|\mathbf{G}(\mathbb{F}_q)| \le q^d$.*

((ii)) *There is a constant $\kappa \ge 1$, depending only on d and r, such that $|\mathbf{G}(\mathbb{F}_q)^\sharp| \le \kappa q^r$.*

Proof. The reductive group $\mathbf{G}$ is the almost direct product of a split torus and a split semisimple group. We can then reduce (i) and (ii) to the case where $\mathbf{G}$ is a split torus or $\mathbf{G}$ is a connected and split semisimple group. If $\mathbf{G}$ is a split torus, then $r = d$ and we have $|\mathbf{G}(\mathbb{F}_q)| = |\mathbf{G}(\mathbb{F}_q)^\sharp| = (q-1)^d \le q^d$.

Now suppose that $\mathbf{G}$ is semisimple. We first prove (i). The cardinality $|\mathbf{G}(\mathbb{F}_q)|$ does not change under isogeny, so we may assume that $\mathbf{G}$ is simply connected. The group $\mathbf{G}$ is then a product of simple, simply connected, and split semisimple groups (the number of factors being bounded in terms of d); so we may further assume that $\mathbf{G}$ is simple. There are positive integers a_i such that $|\mathbf{G}(\mathbb{F}_q)| = q^d \prod_{i=1}^r \left(1 - \frac{1}{q^{a_i}}\right)$; this can be deduced from [Ste68, Theorem 25(a)]. Therefore, $|\mathbf{G}(\mathbb{F}_q)| \le q^d$.

We now prove (ii). If H is a proper subgroup of a finite group G, then we have inequalities $|H^\sharp| \le [G : H]|G^\sharp|$ and $|G^\sharp| \le [G : H]|H^\sharp|$, cf. [Ern61]. Using these inequalities, we can reduce part (ii) to showing that if G is a finite simple group of Lie type over $\mathbb{F}_q$ which arises from a simple algebraic group of rank r, then $|G^\sharp| \le \kappa q^r$ for some constant $\kappa \ge 1$ depending only on r; this follows from [LP97b, Theorem 1]. □

Proposition 9.6. *Fix a set Λ of rational primes with positive density such that $\mathcal{G}_{A,\ell}$ is a split reductive group scheme over $\mathbb{Z}_\ell$ for all $\ell \in \Lambda$. For each prime $\ell \in \Lambda$, fix a subset U_ℓ of $\bar\rho_{A,\ell}(\mathrm{Gal}_K)$ that is stable under conjugation and satisfies $|U_\ell|/|\bar\rho_{A,\ell}(\mathrm{Gal}_K)| = \delta + O(1/\ell)$ for some $0 < \delta < 1$, where δ and the implicit constant do not depend on ℓ. Let $\mathcal{V}$ be the set of place $v \in \Sigma_K$ for which A has good reduction and for which $\bar\rho_{A,\ell}(\mathrm{Frob}_v) \not\subseteq U_\ell$ for all $\ell \in \Lambda$ that satisfy $v \nmid \ell$.*

((a)) *Then*

$$|\mathcal{V}(x)| \ll \frac{x(\log\log x)^{1+1/(3d)}}{(\log x)^{1+1/(6d)}}.$$

((b)) *If GRH holds, then*

$$|\mathcal{V}(x)| \ll x^{1-\frac{1}{4d+2r+2}} (\log x)^{\frac{2}{2d+r+1}}.$$

Proof. For each $\ell \in \Lambda$, we set $H_\ell := \bar\rho_{A,\ell}(\mathrm{Gal}_K)$. Take any prime $\ell \in \Lambda$, and let $\mathbf{G}/\mathbb{F}_\ell$ be the special fiber of $\mathcal{G}_{A,\ell}$. By Lemma 9.5(i), we have $|H_\ell| \le |\mathbf{G}(\mathbb{F}_\ell)| \le \ell^d$. We have an inequality $|H_\ell^\sharp| \le$

$[\mathbf{G}(\mathbb{F}_\ell) : H_\ell] \cdot |\mathbf{G}(\mathbb{F}_\ell)^\sharp|$ (see the comments following [Ern61, Theorem 2]). By Proposition 2.10(ii) and Lemma 9.5(ii), there is a constant $\kappa \geq 1$ which does not depend on ℓ such that $|H_\ell^\sharp| \leq \kappa \ell^r$.

We now set some notation so that we may apply the large sieve as presented in [Zyw08]. After possibly removing a finite number of primes from Λ, there will be a constant $\delta' > 0$ such that $|U_\ell|/|\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)| \geq \delta'$ for all $\ell \in \Lambda$. Let Λ_Q be the set of $\ell \in \Lambda$ that satisfy $\ell \leq Q$ and let $\mathcal{Z}(Q)$ be the set of subsets D of Λ_Q that satisfy $\prod_{\ell \in D} \kappa\ell \leq Q$. Define the function

$$L(Q) := \sum_{D \in \mathcal{Z}(Q)} \prod_{\ell \in D} \frac{\delta'}{1-\delta'}.$$

For Q large enough, we have $L(Q) \geq \sum_{\ell \in \Lambda, \ell \leq Q/\kappa} \delta'/(1-\delta') \gg Q/\log Q$ where the implicit constant does not depend on Q; this uses that Λ has positive density. For each $D \in \mathcal{Z}(Q)$, we define the group $H_D := \prod_{\ell \in D} H_\ell$. For $D \in \mathcal{Z}(Q)$, we have

$$|H_D| \leq \prod_{\ell \in D} \ell^d \leq Q^d \quad \text{and } |H_D^\sharp| \leq \prod_{\ell \in D} \kappa\ell^r \leq \big(\prod_{\ell \in D} \kappa\ell\big)^r \leq Q^r. \tag{9.1}$$

We first consider the unconditional case. Theorem 3.3(i) of [Zyw08] implies that for a sufficiently small positive constant c, we have

$$|\mathcal{V}(x)| \ll \frac{x}{\log x} \cdot L\big(c(\log x/(\log\log x)^2)^{1/(6d)}\big)^{-1}.$$

Using our bound $L(Q) \gg Q/\log Q$, we obtain

$$|\mathcal{V}(x)| \ll \frac{x}{(\log x)^{1+1/(6d)}} (\log\log x)^{1+1/(3d)}.$$

Now suppose that GRH holds. Theorem 3.3(ii) of [Zyw08] implies that

$$|\mathcal{V}(x)| \ll \big(\frac{x}{\log x} + \max_{D' \in \mathcal{Z}(Q)} |H_{D'}| \cdot \sum_{D \in \mathcal{Z}(Q)} |H_D^\sharp||H_D| \cdot x^{1/2} \log x\big) L(Q)^{-1}.$$

Using (9.1), $L(Q) \gg Q/\log Q$ and $|\mathcal{Z}(Q)| \leq Q$, we obtain the bound

$$|\mathcal{V}(x)| \ll \Big(\frac{x}{\log x} + Q^d \cdot |\mathcal{Z}(Q)| Q^r Q^d x^{1/2} \log x\Big)(\log Q)/Q \leq \Big(\frac{x}{\log x} + Q^f x^{1/2} \log x\Big)(\log Q)/Q$$

where we have set $f := 2d + r + 1$. Setting Q equal to $(x^{1/2}/(\log x)^2)^{1/f}$, we deduce that

$$|\mathcal{V}(x)| \ll \frac{x}{\log x}(\log Q)/Q \ll x/Q = x^{1-\frac{1}{2f}} (\log x)^{2/f}.$$

Note that Theorem 3.3 of [Zyw08] required our assumption that the representations $\{\rho_{A,\ell}\}_\ell$ are independent. □

We finally begin the proof of Theorem 9.2. Fix a maximal torus $\mathbf{T}$ of $\mathbf{G}_A$. In §6.2, we defined a homomorphism $\psi_v \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{Aut}(X(\mathbf{T}))$ for every place $v \in \mathcal{S}_A$. The following is an effective version of Proposition 6.6.

Proposition 9.7. *Fix a finite extension L of $k_{\mathbf{G}_A}$. Let $\mathscr{S}$ be the set of places $v \in \mathcal{S}_A$ for which $\psi_v(\mathrm{Gal}_L) \neq W(\mathbf{G}_A, \mathbf{T})$. Then*

$$|\mathscr{S}(x)| \ll \frac{x(\log\log x)^{1+1/(3d)}}{(\log x)^{1+1/(6d)}}.$$

If GRH holds, then

$$|\mathscr{S}(x)| \ll x^{1-\frac{1}{4d+2r+2}} (\log x)^{\frac{2}{2d+r+1}}.$$

Proof. The proof is the same as that of Proposition 6.6 with a few extra remarks. After replacing L by a finite extension, we may assume that $\mathbf{T}_L$ is split. In the proof of Proposition 6.6 we chose a certain set of primes Λ with positive density such that $\mathcal{G}_{A,\ell}/\mathbb{Z}_\ell$ is a split reductive group scheme for all $\ell \in \Lambda$. For a fixed non-empty subset C of $W(\mathbf{G}_A, \mathbf{T})$, which is stable under conjugation by Γ, we defined the set $\mathcal{V}_C$ consisting of those places $v \in \mathcal{S}_A$ for which $\bar{\rho}_{A,\ell}(\mathrm{Frob}_v) \not\subseteq U_\ell$ for all $\ell \in \Lambda$ that satisfy $v \nmid \ell$, where the sets U_ℓ of $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ are stable under conjugation and satisfy $|U_\ell|/|\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)| = |C|/|W(\mathbf{G}_A, \mathbf{T})| + O(1/\ell)$. We can then apply Proposition 9.6 to bound $|\mathcal{V}_C(x)|$. The proposition then follows in the same manner as before; note that the number of such subsets C can be bounded in terms of A. □

The proof of Theorem 9.2 is now identical to §6 where we make use of Lemma 9.4 and Proposition 9.7 instead of using that certain sets have density 0.

Acknowledgements. Thanks to J. Achter for rekindling the author's interest in the conjecture of Murty and Patankar. Thanks to F. Jouve and E. Kowalski; many of the techniques and strategies used here were first worked out in the joint paper [JKZ11]. Thanks also to the referees for their useful suggestions.

References

[Ach09] Jeffrey D. Achter, *Split reductions of simple abelian varieties*, Math. Res. Lett. **16** (2009), no. 2, 199–213. ↑1.2

[Ach11] ———, *Explicit bounds for split reductions of simple abelian varieties*, 2011. preprint. ↑1.2, 8.1, 9

[BGK06] Grzegorz Banaszak, Wojciech Gajda, and Piotr Krasoń, *On the image of l-adic Galois representations for abelian varieties of type I and II*, Doc. Math. **Extra Vol.** (2006), 35–75. ↑1.2

[BGK10] ———, *On the image of Galois l-adic representations for abelian varieties of type III*, Tohoku Math. J. (2) **62** (2010), no. 2, 163–189. ↑1.2

[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. ↑2.3

[Bog81] F A Bogomolov, *Points of finite order on an abelian variety*, Mathematics of the USSR-Izvestiya **17** (1981), no. 1, 55. ↑2.3

[Bor91] Armand Borel, *Linear algebraic groups*, Second, Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991. ↑4.3

[Car85] Roger W. Carter, *Finite groups of Lie type*, Pure and Applied Mathematics (New York), John Wiley & Sons Inc., New York, 1985. Conjugacy classes and complex characters, A Wiley-Interscience Publication. ↑3.3

[Cha97] Nick Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180. ↑1.2

[DG70] Michel Demazure and Alexandre Grothendieck, *Séminaire de Géométrie Algébrique du Bois Marie - 1962–64 - Schémas en groupes (SGA 3)*, Lecture Notes in Mathematics **151**, **152**, **153**, Springer-Verlag, New York, 1970. ↑5, 5

[DMOS82] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin, 1982. ↑2.6

[Ern61] John A. Ernest, *Central intertwining numbers for representations of finite groups*, Trans. Amer. Math. Soc. **99** (1961), 499–508. ↑9.2, 9.2

[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]. ↑2.3

[JKZ11] Florent Jouve, Emmanuel Kowalski, and David Zywina, *Splitting fields of characteristic polynomials of random elements in arithmetic groups* (2011). arXiv:1008.3662 (to appear, Israel J. Math.) ↑3.2, 3.3, 3.3, 9.2

[Lar95] Michael Larsen, *Maximality of Galois actions for compatible systems*, Duke Math. J. **80** (1995), no. 3, 601–630. ↑3.3

[LP95] Michael Larsen and Richard Pink, *Abelian varieties, l-adic representations, and l-independence*, Math. Ann. **302** (1995), no. 3, 561–579. ↑1, 2.6, 2.8, 6.1

[LP97a] ———, *A connectedness criterion for l-adic Galois representations*, Israel J. Math. **97** (1997), 1–10. ↑2.3, 9.1

[LP97b] Martin W. Liebeck and László Pyber, *Upper bounds for the number of conjugacy classes of a finite group*, J. Algebra **198** (1997), no. 2, 538–562. ↑9.2

[Mil86] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 103–150. ↑2

[Mum69] D. Mumford, *A note of Shimura's paper "Discontinuous groups and abelian varieties"*, Math. Ann. **181** (1969), 345–351. ↑8.1

[MP08] V. Kumar Murty and Vijay M. Patankar, *Splitting of abelian varieties*, Int. Math. Res. Not. IMRN **12** (2008). ↑1, 1, 1.2

[Noo00] Rutger Noot, *Abelian varieties with l-adic Galois representation of Mumford's type*, J. Reine Angew. Math. **519** (2000), 155–169. ↑8.1

[Noo09] ———, *Classe de conjugaison du Frobenius d'une variété abélienne sur un corps de nombres*, J. Lond. Math. Soc. (2) **79** (2009), no. 1, 53–71. ↑4.2

[Pin98] Richard Pink, *l-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture*, J. Reine Angew. Math. **495** (1998), 187–237. ↑1.2, 6.1, 8.1

[Rib76] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. ↑6.4

[Ser77] Jean-Pierre Serre, *Représentations l-adiques*, Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), 1977, pp. 177–193. ↑2, 2.6

[Ser79] ———, *Groupes algébriques associés aux modules de Hodge-Tate*, Journées de Géométrie Algébrique de Rennes. (Rennes, 1978), Vol. III, 1979, pp. 155–188. ↑6.1, 6.1

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. ↑9.1

[Ser94] ———, *Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques*, Motives (Seattle, WA, 1991), 1994, pp. 377–400. ↑2, 2.7

[Ser00] ———, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000. 1985–1998. ↑2.3, 2.8, 2.11

[Ser03] ———, *On a theorem of Jordan*, Bull. Amer. Math. Soc. (N.S.) **40** (2003), no. 4, 429–440 (electronic). ↑4.3

[Shi67] Goro Shimura, *Algebraic number fields and symplectic discontinuous groups*, Ann. of Math. (2) **86** (1967), 503–592. ↑6.4

[Ste68] Robert Steinberg, *Lectures on Chevalley groups*, Yale University, New Haven, Conn., 1968. Notes prepared by John Faulkner and Robert Wilson. ↑9.2

[Vas08] Adrian Vasiu, *Some cases of the Mumford-Tate conjecture and Shimura varieties*, Indiana Univ. Math. J. **57** (2008), no. 1, 1–75. ↑1.2, 2.6

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. ↑2.1

[Win02] J.-P. Wintenberger, *Démonstration d'une conjecture de Lang dans des cas particuliers*, J. Reine Angew. Math. **553** (2002), 1–16. ↑2.8, 5, (ii)

[WM71] W. C. Waterhouse and J. S. Milne, *Abelian varieties over finite fields*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), 1971, pp. 53–64. ↑2.1

[Zyw08] David Zywina, *The large sieve and Galois representations* (2008). arXiv:0812.2222. ↑9, 9.2, 9.2

School of Mathematics, Institute for advanced study, Princeton, NJ 08540
E-mail address: zywina@math.ias.edu