# AN EFFECTIVE OPEN IMAGE THEOREM FOR ABELIAN VARIETIES

DAVID ZYWINA

Abstract. Fix a nonzero abelian variety $A$ of dimension $g$ defined over a number field $K$. For each prime $\ell$, the Galois action on the $\ell$-power torsion points of $A$ induces a representation $\rho_{A,\ell}\colon \mathrm{Gal}_K \to \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. The $\ell$-adic monodromy group of $A$ is the Zariski closure $G_{A,\ell}$ of the image of $\rho_{A,\ell}$ in $\mathrm{GL}_{2g,\mathbb{Q}_\ell}$. The image of $\rho_{A,\ell}$ is open in $G_{A,\ell}(\mathbb{Q}_\ell)$ with respect to the $\ell$-adic topology and hence the index $[G_{A,\ell}(\mathbb{Q}_\ell)\cap \mathrm{GL}_{2g}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)]$ is finite. We prove that this index can be bounded in terms of $g$ for all $\ell$ larger then some constant depending on certain invariants of $A$.

## 1. Introduction

Let $A$ be an abelian variety of dimension $g \geq 1$ defined over a number field $K$. Fix an algebraic closure $\overline{K}$ of $K$ and define the absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K)$.

Take any rational prime $\ell$. For each positive integer $n$, we denote by $A[\ell^n]$ the $\ell^n$-torsion subgroup of $A(\overline{K})$. The group $A[\ell^n]$ is a free $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank $2g$ and comes with a natural $\mathrm{Gal}_K$-action that respects the group structure. The $\ell$-adic Tate module of $A$ is

$$T_\ell(A) := \varprojlim_n A[\ell^n],$$

where the transition maps $A[\ell^{n+1}] \to A[\ell^n]$ are multiplication by $\ell$; it is a free $\mathbb{Z}_\ell$-module of rank $2g$. The induced Galois action on $T_\ell(A)$ can be expressed in terms of a continuous representation

$$\rho_{A,\ell}\colon \mathrm{Gal}_K \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A)) = \mathrm{GL}_{T_\ell(A)}(\mathbb{Z}_\ell),$$

where $\mathrm{GL}_{T_\ell(A)}$ is the group scheme over $\mathbb{Z}_\ell$ for which $\mathrm{GL}_{T_\ell(A)}(R) = \mathrm{Aut}_R(T_\ell(A)\otimes_{\mathbb{Z}_\ell} R)$ for all $\mathbb{Z}_\ell$-algebras $R$ with the obvious functoriality. After choosing a basis for $T_\ell(A)$, one could have $\rho_{A,\ell}$ mapping to $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$; it will make our arguments easier not to make such an arbitrary choice.

To study the group $\rho_{A,\ell}(\mathrm{Gal}_K)$, we consider a related algebraic group defined over $\mathbb{Q}_\ell$. Define $V_\ell(A) := T_\ell(A)\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$; it is a $\mathbb{Q}_\ell$-vector space of dimension $2g$ and inherits the Galois action from $T_\ell(A)$. We can define a group scheme $\mathrm{GL}_{V_\ell(A)}$ over $\mathbb{Q}_\ell$ as above; it is the generic fiber of $\mathrm{GL}_{T_\ell(A)}$. We can view $\mathrm{GL}_{T_\ell(A)}(\mathbb{Z}_\ell)$, and hence also $\rho_{A,\ell}(\mathrm{Gal}_K)$, as a subgroup of $\mathrm{GL}_{V_\ell(A)}(\mathbb{Q}_\ell) = \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$.

**Definition 1.1.** The $\ell$-adic monodromy group of $A$ is the algebraic group $G_{A,\ell}$ defined over $\mathbb{Q}_\ell$ obtained by taking the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}_K)$ in $\mathrm{GL}_{V_\ell(A)}$. Let $\mathcal{G}_{A,\ell}$ be the algebraic group over $\mathbb{Z}_\ell$ obtained by taking the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}_K)$ in $\mathrm{GL}_{T_\ell(A)}$.

Note that the group schemes $G_{A,\ell}$ and $\mathcal{G}_{A,\ell}$ determine each other; $G_{A,\ell}$ is the generic fiber of $\mathcal{G}_{A,\ell}$ and $\mathcal{G}_{A,\ell}$ is the Zariski closure of $G_{A,\ell}$ in $\mathrm{GL}_{T_\ell(A)}$.

The group $\rho_{A,\ell}(\mathrm{Gal}_K)$ is open in $G_{A,\ell}(\mathbb{Q}_\ell)$ with respect to the $\ell$-adic topology, cf. [Bog80]. In particular, $\rho_{A,\ell}(\mathrm{Gal}_K)$ is an open, and hence finite index, subgroup of $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) = G_{A,\ell}(\mathbb{Q}_\ell)\cap \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(A))$. An effective version would ask for effective bounds for $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)]$. As a special case of our work, we will see that

$$[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] \ll_g 1$$

for all sufficiently large primes $\ell$. The notation "$\ll_g$" indicates that the index can be bounded in terms of a constant that depends only on $g$, cf. §1.3. For applications, in particular [Zyw19], we are interested in describing how large $\ell$ needs to be in terms of invariants of $A$.

*Date*: January 1, 2022.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F80.

1.1. **Some quantities.** Before stating our main results, we need to define some quantities that will show up in the bounds. See §2 for further details and references.

For each prime $\ell$, let $G_{A,\ell}^{\circ}$ be the neutral component of $G_{A,\ell}$, i.e., the algebraic subgroup of $G_{A,\ell}$ that is the connected component of the identity. The algebraic group $G_{A,\ell}^{\circ}$ is reductive and its rank $r$ is independent of $\ell$. Let $\mathcal{G}_{A,\ell}^{\circ}$ be the $\mathbb{Z}_\ell$-group subscheme of $\mathcal{G}_{A,\ell}$ that is the Zariski closure of $G_{A,\ell}^{\circ}$. Let $K_A^{\mathrm{conn}}$ be the minimal extension of $K$ in $\overline{K}$ for which $\rho_{A,\ell}(\mathrm{Gal}_{K_A^{\mathrm{conn}}}) \subseteq G_{A,\ell}^{\circ}(\mathbb{Q}_\ell)$. The field $K_A^{\mathrm{conn}}$ is a number field that is independent of $\ell$. The extension $K_A^{\mathrm{conn}}/K$ is unramified at all primes ideals for which $A$ has good reduction and the degree $[K_A^{\mathrm{conn}} : K]$ can be bounded in terms of $g$.

Let $\mathfrak{p}$ be any non-zero prime ideal of $\mathcal{O}_K$ for which $A$ has good reduction. Denote by $P_{A,\mathfrak{p}}(x)$ the Frobenius polynomial of $A$ at $\mathfrak{p}$; it is a monic polynomial of degree $2g$ with integer coefficients. For a prime $\ell$ satisfying $\mathfrak{p} \nmid \ell$, the representation $\rho_{A,\ell}$ is unramified at $\mathfrak{p}$ and we have

$$P_{A,\mathfrak{p}}(x) = \det(xI - \rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})).$$

Let $\Phi_{A,\mathfrak{p}}$ be the subgroup of $\mathbb{C}^\times$ generated by the roots of $P_{A,\mathfrak{p}}(x)$. If $\Phi_{A,\mathfrak{p}}$ is a free abelian group, then it has rank at most $r$. Moreover, the set of primes $\mathfrak{p}$ for which $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank $r$ has positive density.

Denote by $h(A)$ the (logarithmic absolute semistable) Faltings height of $A$.

1.2. **Main results.** We can now state the main theorem of the paper. As before, $A$ is an abelian variety of dimension $g \geq 1$ defined over a number field $K$. Let $\mathfrak{q}$ be a non-zero prime ideal of $\mathcal{O}_K$ for which $\Phi_{A,\mathfrak{q}}$ is a free abelian group of rank $r$, where $r$ is the common rank of the reductive groups $G_{A,\ell}^{\circ}$.

**Theorem 1.2.** *There are positive constants $c$ and $\gamma$, depending only on $g$, such that for any prime $\ell$ satisfying*

$$\ell \geq c \cdot \max(\{[K : \mathbb{Q}], h(A), N(\mathfrak{q})\})^{\gamma} \tag{1.1}$$

*the following hold:*

(a) $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] \ll_{g,[K:\mathbb{Q}]} 1$,
(b) *if $\ell$ is unramified in $K_A^{\mathrm{conn}}$, then* $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] \ll_g 1$.
(c) *$\mathcal{G}_{A,\ell}^{\circ}$ is a reductive group scheme over $\mathbb{Z}_\ell$,*
(d) *the commutator subgroups of $\rho_{A,\ell}(\mathrm{Gal}_{K_A^{\mathrm{conn}}})$ and $\mathcal{G}_{A,\ell}^{\circ}(\mathbb{Z}_\ell)$ agree.*

*Remark* 1.3. Building on the work of Serre, Wintenberger proved that parts (c) and (d) of Theorem 1.2 hold for all primes $\ell \geq C$ with $C$ a constant depending on $A$, cf. [Win02, §2.1]. Using results of Serre, it is then easy to show that $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] \ll_A 1$ holds for all $\ell$.

In §2.2 of [Win02], Wintenberger discusses how one could make the bound $\ell \geq C$ effective. He mentioned that it should be possible to consider $\ell$ large enough in terms of the Faltings height $h(A)$, a related field $K$, the prime ideal $\mathfrak{q}$, and the finite set $S$ of prime ideals of $\mathcal{O}_K$ for which $A$ has bad reduction. We tried to work this out following Wintenberger's approach but the dependencies on the set $S$ were not appropriate for our applications where we vary $A$ in a geometric family.

Note that, except for possibly part (b), the set $S$ of bad primes of $A$ do not occur in our theorem. This was achieved by using the effective bounds of Masser–Wüstholz (Theorem 2.4) to give a new streamlined proof. In particular, our proof of (c) and (d) does not require inertia groups which is a key ingredient in the work of Serre and Wintenberger (for example, see §§3.1–3.3 of [Win02]).

Assuming the Generalized Riemann Hypothesis (GRH) for number fields, we can give a version of Theorem 1.2 that does not involve the prime ideal $\mathfrak{q}$. Let $D$ be the product of primes $p$ that ramify in $K$ or are divisible by a prime ideal for which $A$ has bad reduction.

**Theorem 1.4.** *Suppose that GRH holds. Theorem 1.2 holds with (1.1) replaced by*

$$\ell \geq c \cdot \max(\{[K : \mathbb{Q}], h(A), \log D\})^{\gamma},$$

*where $c$ and $\gamma$ are positive constants depending only on $g$.*

*Remark* 1.5. The difficulty with bounding the minimal possible $N(\mathfrak{q})$ is that the most natural way to do this is via the Chebotarev density theorem, and this requires knowledge about the image of a representation $\rho_{A,\ell}$ (which is the thing we are trying to study in the first place!). Our proof of Theorem 1.4 uses a variant of

Theorem 1.2 along with an effective version of the Chebotarev density theorem. Unfortunately, unconditional versions of the Chebotarev density theorem did not produce upper bounds for $N(\mathfrak{q})$.

For $\ell$ sufficiently large, one can show that $T_\ell(A)$ has a basis over $\mathbb{Z}_\ell$ such that, with respect to this basis, $\rho_{A,\ell}(\mathrm{Gal}_K) \subseteq \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$.

**Corollary 1.6.** *Suppose that* $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$ *and that there is a non-zero prime ideal* $\mathfrak{q}$ *of* $\mathcal{O}_K$ *for which* $A$ *has good reduction and for which* $\Phi_{A,\mathfrak{q}}$ *is a free abelian group of rank* $g+1$*. Then there are positive constants* $c$ *and* $\gamma$*, depending only on* $g$*, such that*

$$\rho_{A,\ell}(\mathrm{Gal}_K) = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$$

*holds for all primes* $\ell \geq c \cdot \max(\{[K:\mathbb{Q}], h(A), N(\mathfrak{q})\})^\gamma$ *that are unramified in* $K$*.*

Corollary 1.6 recovers the main result of Lombardo in [Lom15] except that he gives explicit numerical values of $c$ and $\gamma$ (he also gives another condition on a prime ideal $\mathfrak{q}$ that implies ours). In principle our constants can be made explicit, but working them out in the full generality of Theorem 1.2 would be quite a chore. Note that Lombardo's methods are different than ours; he studies the maximal proper subgroups of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ and makes use of inertia groups.

*Remark* 1.7. Suppose that we have $\rho_{A,\ell}(\mathrm{Gal}_K) = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ for all sufficiently large $\ell$. In this case, one can show that $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$ and that $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank $g+1$ for all prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ away from a set of density 0. This justifies the assumptions of Corollary 1.6.

1.3. **Notation.** For two real quantities $f$ and $g$, we write that $f \ll_{\alpha_1,\ldots,\alpha_n} g$ if the inequality $|f| \leq C|g|$ holds for some positive constant $C$ depending only on $\alpha_1, \ldots, \alpha_n$. In particular, $f \ll g$ means that the implicit constant is absolute. We denote by $O_{\alpha_1,\ldots,\alpha_n}(g)$ a quantity $f$ satisfying $f \ll_{\alpha_1,\ldots,\alpha_n} g$.

Fix a number field $F$. We denote the ring of integers of $F$ by $\mathcal{O}_F$. For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, we denote by $F_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of $F$ and let $\mathcal{O}_\mathfrak{p}$ be the valuation ring of $F_\mathfrak{p}$. The residue field of $\mathcal{O}_\mathfrak{p}$ agrees with $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. For a field $F$, let $\overline{F}$ be a fixed algebraic closure of $F$ and define $\mathrm{Gal}_F := \mathrm{Gal}(\overline{F}/F)$.

For a scheme $X$ over a commutative ring $R$ and a commutative $R$-algebra $S$, we denote by $X_S$ the base extension of $X$ by $\operatorname{Spec} S$.

Let $M$ be a free module of finite rank over a commutative ring $R$. Denote by $\mathrm{GL}_M$ the $R$-scheme such that $\mathrm{GL}_M(S) = \mathrm{Aut}_S(M \otimes_R S)$ for any commutative $R$-algebra $S$ with the obvious functoriality.

For an algebraic group $G$ over a field $F$, we denote by $G^\circ$ the neutral component of $G$ (i.e., the connected component of the identity of $G$); it is an algebraic subgroup of $G$. For an algebraic group $T$ of multiplicative type defined over $F$, let $X(T)$ be the group of characters $T_{\overline{F}} \to \mathbb{G}_{m,\overline{F}}$; it has a natural $\mathrm{Gal}_F$-action. If $T$ is a torus, then the group $X(T)$ is free abelian whose rank is equal to the dimension of $T$.

Consider a topological group $G$. Note that profinite groups, will always be considered with their profinite topology. The commutator subgroup of $G$ is the closed subgroup generated by the commutators of $G$; we denote it by $G'$.

1.4. **Overview.** In §2, we recall several fundamental results about the Galois representations $\rho_{A,\ell}$ and their $\ell$-adic monodromy group $G_{A,\ell}$. We also state the *Mumford–Tate conjecture* for $A$ in §2.6 which says that $G^\circ_{A,\ell}$ arises from a certain reductive group defined over $\mathbb{Q}$ that is independent of $\ell$. In §2.7, we show that it suffices to prove Theorem 1.2 in the special case where all the groups $G_{A,\ell}$ are connected.

In §4, we prove parts (c) and (d) of Theorem 1.2. Our new proof makes key use of theorems of Masser–Wüstholz and Larsen–Pink. Some of the needed group theory is described in §3.

In §5, assuming the $\ell$-adic monodromy groups $G_{A,\ell}$ are connected, we construct abelian representations $\beta_{A,\ell}\colon \mathrm{Gal}_K \to Y(\mathbb{Q}_\ell)_c$, where $Y$ is a certain torus over $\mathbb{Q}$ and $Y(\mathbb{Q}_\ell)_c$ is the maximal compact subgroup of $Y(\mathbb{Q}_\ell)$ with respect to the $\ell$-adic topology. We show that the image of $\beta_{A,\ell}(\mathrm{Gal}_K)$ is open in $Y(\mathbb{Q}_\ell)_c$. Moreover, we show that the index $[Y(\mathbb{Q}_\ell)_c : \beta_{A,\ell}(\mathrm{Gal}_K)]$ can be bounded in terms of $g$ if $\ell$ is unramified in $K$ and in terms of $g$ and $[K:\mathbb{Q}]$ otherwise. This bound is key in deducing Theorem 1.2(a) and (b) from Theorem 1.2(d).

In §6, we complete the proof of Theorem 1.2. In §7 and §8, we prove Theorem 1.4 and Corollary 1.6, respectively.

1.5. **Acknowledgements.** Special thanks to David Zureick-Brown; this article is spun off from earlier work with him. Thanks also to Chun Yin Hui.

## 2. Background: $\ell$-adic monodromy groups

Fix an abelian variety $A$ of dimension $g \geq 1$ defined over a number field $K$.

2.1. **Compatibility.** Take any non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ for which $A$ has good reduction. Denote by $A_\mathfrak{p}$ the abelian variety over $\mathbb{F}_\mathfrak{p}$ obtained by reducing $A$ modulo $\mathfrak{p}$. There is a unique polynomial $P_{A,\mathfrak{p}}(x) \in \mathbb{Z}[x]$ such that $P_{A,\mathfrak{p}}(n)$ is the degree of the isogeny $n-\pi$ for each integer $n$, where $\pi$ is the Frobenius endomorphism of $A_\mathfrak{p}/\mathbb{F}_\mathfrak{p}$. The polynomial $P_{A,\mathfrak{p}}(x)$ is monic of degree $2g$. For each rational prime $\ell$ for which $\mathfrak{p} \nmid \ell$, the representation $\rho_{A,\ell}$ is unramified at $\mathfrak{p}$ and satisfies

$$\det(xI - \rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})) = P_{A,\mathfrak{p}}(x).$$

In the notation of [Ser98], the Galois representations $\{\rho_{A,\ell}\}_\ell$ form a *strictly compatible* family.

Note that $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ is semisimple in $\mathrm{GL}_{V_\ell(A)}$; this can be seen by noting that $\pi$ acts semisimply on the $\ell$-adic Tate module of $A_\mathfrak{p}$. From Weil, we know that all of the roots of $P_{A,\mathfrak{p}}(x)$ in $\mathbb{C}$ have absolute value $N(\mathfrak{p})^{1/2}$.

2.2. **Neutral component.** Let $G^\circ_{A,\ell}$ be the neutral component of $G_{A,\ell}$, i.e., the connected component of $G_{A,\ell}$ containing the identity. Define $\mathcal{G}^\circ_{A,\ell}$ to be the $\mathbb{Z}_\ell$-group subscheme of $\mathcal{G}_{A,\ell}$ that is the Zariski closure of $G^\circ_{A,\ell}$.

Define $K_A^{\mathrm{conn}}$ to be the subfield of $\overline{K}$ fixed by the kernel of the homomorphism

$$\mathrm{Gal}_K \xrightarrow{\rho_{A,\ell}} G_{A,\ell}(\mathbb{Q}_\ell) \to G_{A,\ell}(\mathbb{Q}_\ell)/G^\circ_{A,\ell}(\mathbb{Q}_\ell). \tag{2.1}$$

Equivalently, $K_A^{\mathrm{conn}}$ is the smallest extension of $K$ in $\overline{K}$ that satisfies $\rho_{A,\ell}(\mathrm{Gal}_{K_A^{\mathrm{conn}}}) \subseteq G^\circ_{A,\ell}(\mathbb{Q}_\ell)$.

**Proposition 2.1.**

(i) *The field $K_A^{\mathrm{conn}}$ depends only on $A$, i.e., it is independent of $\ell$.*
(ii) *The degree $[K_A^{\mathrm{conn}} : K]$ can be bounded in terms of $g$ only.*
(iii) *We have*

$$[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] = [\mathcal{G}_{A',\ell}(\mathbb{Z}_\ell) : \rho_{A',\ell}(\mathrm{Gal}_{K_A^{\mathrm{conn}}})],$$

*where $A'$ is the base change of $A$ to $K_A^{\mathrm{conn}}$.*

*Proof.* Part (i) was proved by Serre [Ser00, 133]; see also [LP97]. From (i), we find that $K_A^{\mathrm{conn}}$ is a subfield of $K(A[\ell^\infty])$ and hence $[K_A^{\mathrm{conn}} : K]$ divides $[K(A[\ell]) : K]\ell^{e_\ell}$ for some integer $e_\ell$. Since $[K(A[\ell]) : K]$ divides $|\mathrm{GL}_{2g}(\mathbb{F}_\ell)|$, we deduce that $[K_A^{\mathrm{conn}} : K]$ divides $|\mathrm{GL}_{2g}(\mathbb{F}_\ell)|\ell^{e_\ell}$. Therefore, $[K_A^{\mathrm{conn}} : K]$ must divide $|\mathrm{GL}_{2g}(\mathbb{F}_2)| \cdot |\mathrm{GL}_{2g}(\mathbb{F}_3)|$ which completes the proof of (ii).

Note that the homomorphism (2.1) is surjective since $G_{A,\ell}$ is the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}_K)$. Therefore, $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \mathcal{G}^\circ_{A,\ell}(\mathbb{Z}_\ell)] = [G_{A,\ell}(\mathbb{Q}_\ell) : G^\circ_{A,\ell}(\mathbb{Q}_\ell)] = [K_A^{\mathrm{conn}} : K]$. Part (iii) follows since $[\rho_{A,\ell}(\mathrm{Gal}_K) : \rho_{A,\ell}(\mathrm{Gal}_{K_A^{\mathrm{conn}}})] = [K_A^{\mathrm{conn}} : K]$. □

2.3. **Tate conjecture.** The following, which was conjectured by Tate, is an important result of Faltings, cf. [Fal86].

**Theorem 2.2** (Faltings)**.**

(i) *The $\mathbb{Q}_\ell[\mathrm{Gal}_K]$-module $V_\ell(A)$ is semisimple.*
(ii) *The natural map $\mathrm{End}(A) \otimes_\mathbb{Z} \mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_K]}(V_\ell(A))$ is an isomorphism.*

Here are some basic properties of the groups $G^\circ_{A,\ell}$.

**Proposition 2.3.**

(i) *The group $G^\circ_{A,\ell}$ is reductive.*
(ii) *For any number field $L$ containing $K_A^{\mathrm{conn}}$, the group $\rho_{A,\ell}(\mathrm{Gal}_L)$ is Zariski dense in $G^\circ_{A,\ell}$.*
(iii) *The commutant of $G^\circ_{A,\ell}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ agrees with $\mathrm{End}(A_{\overline{K}}) \otimes_\mathbb{Z} \mathbb{Q}_\ell$.*
(iv) *All of the endomorphisms of $A$ over $\overline{K}$ are defined over $K_A^{\mathrm{conn}}$, i.e., $\mathrm{End}(A_{\overline{K}}) = \mathrm{End}(A_{K_A^{\mathrm{conn}}})$.*

*Proof.* Part (i) can be deduced from Theorem 2.2.

Take any number field $L \supseteq K_A^{\mathrm{conn}}$. We have $\rho_{A,\ell}(\mathrm{Gal}_L) \subseteq G_{A,\ell}^\circ(\mathbb{Q}_\ell)$, so $G_{A_L,\ell}$ is a finite index subgroup of $G_{A,\ell}^\circ$. Since $G_{A,\ell}^\circ$ is connected, we have $G_{A_L,\ell} = G_{A,\ell}^\circ$. This proves (ii).

From part (ii) and Theorem 2.2(ii), we find that $\mathrm{End}(A_L) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ is naturally isomorphic to the subring of $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ that commutes with $G_{A_L,\ell} = G_{A,\ell}^\circ$. Since this holds for all $L \supseteq K_A^{\mathrm{conn}}$, we deduce that

$$\mathrm{End}(A_{K_A^{\mathrm{conn}}}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell = \mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell. \tag{2.2}$$

This proves part (iii). Since $\mathrm{End}(A_{\overline{K}})$ is a free abelian group and $\mathrm{Gal}_{K_A^{\mathrm{conn}}}$ acts trivially on $\mathrm{End}(A_{\overline{K}}) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ by (2.2), we deduce that $\mathrm{Gal}_{K_A^{\mathrm{conn}}}$ acts trivially on $\mathrm{End}(A_{\overline{K}})$. This proves (iv). □

We will also need the following effective modulo $\ell$ version of Faltings' theorem due to Masser and Wüstholz. We denote by $h(A)$ the (logarithmic absolute) Faltings height of $A$ obtained after base extending to any finite extension of $K$ over which $A$ has semistable reduction (see §5 of [Cha86]). In particular, note that $h(A_L) = h(A)$ for any finite extension $L/K$.

**Theorem 2.4** (Masser-Wüstholz)**.** *Let $L$ be a finite extension of $K$. There are positive constants $c$ and $\gamma$, depending only on the dimension of $A$, such that if $\ell \geq c(\max\{[L:\mathbb{Q}], h(A)\})^\gamma$, then the following hold:*

- *the $\mathbb{F}_\ell[\mathrm{Gal}_L]$-module $A[\ell]$ is semisimple,*
- *the natural map $\mathrm{End}(A_L) \otimes_{\mathbb{Z}} \mathbb{F}_\ell \to \mathrm{End}_{\mathbb{F}_\ell[\mathrm{Gal}_L]}(A[\ell])$ is an isomorphism,*
- *$\mathrm{End}(A_L) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ is a semisimple $\mathbb{F}_\ell$-algebra.*

*Proof.* Since $h(A) = h(A_L)$, it suffices to prove the theorem in the special case $L = K$.

The first two conclusions of the theorem follow from Corollaries 1 and 2 in §1 of [MW95]; see the last remark of their paper for the stated dependence on $K$. By Lemmas 2.3 and 5.2 of [MW95], we deduce $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ is semisimple after suitable increasing $c$ and $\gamma$; as before, see the last remark of loc. cit. for the stated dependence on $K$. □

2.4. **Computing $\Phi_{A,\mathfrak{p}}$.** Fix a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ for which $A$ has good reduction. Let $\Phi_{A,\mathfrak{p}}$ be the subgroup of $\mathbb{C}^\times$ generated by the roots of $P_{A,\mathfrak{p}}(x)$.

Let $\pi_1, \ldots, \pi_{2g} \in \mathbb{C}$ be the roots of $P_{A,\mathfrak{p}}(x)$ with multiplicity. Define the number field $L = \mathbb{Q}(\pi_1, \ldots, \pi_{2g})$. We have a surjective homomorphism

$$\varphi \colon \mathbb{Z}^{2g} \to \Phi_{A,\mathfrak{p}}, \quad e \mapsto \prod_{i=1}^{2g} \pi_i^{e_i}.$$

To compute the group $\Phi_{A,\mathfrak{p}}$, we need to describe the kernel of $\varphi$. We first describe the $e \in \mathbb{Z}^{2g}$ for which $\varphi(e)$ is a root of unity. For each non-zero prime $\lambda$ of $\mathcal{O}_L$, let $v_\lambda \colon L^\times \twoheadrightarrow \mathbb{Z}$ be the $\lambda$-adic valuation.

**Lemma 2.5.** *Take any $e \in \mathbb{Z}^{2g}$. The following are equivalent:*

(a) *$\varphi(e)$ is a root of unity,*
(b) *$\sum_{i=1}^{2g} v_\lambda(\pi_i) \cdot e_i = 0$ holds for all prime ideals $\lambda | N(\mathfrak{p})$ of $\mathcal{O}_L$,*

*Proof.* For a fixed $e \in \mathbb{Z}^{2g}$, define $\alpha := \varphi(e) = \prod_{i=1}^{2g} \pi_i^{e_i} \in L^\times$. Observe that for a non-zero prime $\lambda$ of $\mathcal{O}_L$, we have $v_\lambda(\alpha) = \sum_{i=1}^{2g} v_\lambda(\pi_i) \cdot e_i$. If $\alpha$ is a root of unity, then we have $v_\lambda(\alpha) = 0$ for all $\lambda$. Therefore, (a) implies (b).

We now assume that (b) holds, i.e., $v_\lambda(\alpha) = 0$ for all prime ideals $\lambda | N(\mathfrak{p})$ of $\mathcal{O}_L$. We need to show that $\varphi(e)$ is a root of unity.

Take any non-zero prime ideal $\lambda \nmid N(\mathfrak{p})$ of $\mathcal{O}_L$. For each $\pi_i$, we have $\pi_i \overline{\pi}_i = N(\mathfrak{p})$, where $\overline{\pi}_i$ is the complex conjugate of $\pi_i$ under any complex embedding. So $v_\lambda(\pi_i) + v_\lambda(\overline{\pi}_i) = 0$. Since $\pi_i$ and $\overline{\pi}_i$ are algebraic integers, we have $v_\lambda(\pi_i) \geq 0$ and $v_\lambda(\overline{\pi}_i) \geq 0$, and hence $v_\lambda(\pi_i) = 0$. Therefore, $v_\lambda(\alpha) = 0$. Combing this with our assumption, we deduce that $v_\lambda(\alpha) = 0$ for all non-zero prime ideals $\lambda$ of $\mathcal{O}_L$. This implies that $\alpha \in \mathcal{O}_L^\times$.

Take any embedding $\iota \colon L \hookrightarrow \mathbb{C}$. From Weil, we know that each $\iota(\pi_i)$ has absolute value $N(\mathfrak{p})^{1/2}$. Therefore, $|\iota(\alpha)| = N(\mathfrak{p})^{(e_1+\cdots+e_{2g})/2}$ for any $\iota$ and hence $|N_{L/\mathbb{Q}}(\alpha)| = N(\mathfrak{p})^{[L:\mathbb{Q}]\,(e_1+\cdots+e_{2g})/2}$. We have $N_{L/\mathbb{Q}}(\alpha) = \pm 1$ since $\alpha \in \mathcal{O}_L^\times$, so $e_1 + \cdots + e_{2g} = 0$. Therefore, $\alpha$ has absolute value 1 under any embedding into $\mathbb{C}$. Since $\alpha$ is a unit in $\mathcal{O}_L$ with absolute value 1 under any embedding into $\mathbb{C}$, we conclude that $\alpha$ is a root of unity. □

We now describe how to compute the kernel of $\varphi$. Let $M \subseteq \mathbb{Z}^{2g}$ be the group of $e \in \mathbb{Z}^{2g}$ for which $\sum_{i=1}^{2g} v_\lambda(\pi_i) \cdot e_i = 0$ for all prime ideals $\lambda | N(\mathfrak{p})$ of $\mathcal{O}_L$. By Lemma 2.5, we have $\varphi^{-1}(\mu_L) = M$, where $\mu_L$ is the (finite) group of roots of unity in $L^\times$. Define the homomorphism

$$\varphi|_M \colon M \to \mu_L, \quad e \mapsto \prod_{i=1}^{2g} \pi^{e_i}.$$

Computing $\varphi$ on a basis of $M$, one can then explicitly compute $\ker \varphi = \ker(\varphi|_M) \subseteq \mathbb{Z}^{2g}$.

The following finiteness result will be used multiple times in our proofs.

**Proposition 2.6.** *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$ for which $A$ has good reduction. Let $\pi_1, \dots, \pi_{2g} \in \mathbb{C}$ be the roots of $P_{A,\mathfrak{p}}(x)$ with multiplicity. Let $M$ be the group of $e \in \mathbb{Z}^{2g}$ for which $\prod_{i=1}^{2g} \pi_i^{e_i} = 1$. There are a finite number of subgroups $M_1, \dots, M_s$ of $\mathbb{Z}^{2g}$, depending only on $g$ (and not on $A$ and $\mathfrak{p}$), such that $M$ equals one of the $M_i$.*

*Proof.* Define the number field $L := \mathbb{Q}(\pi_1, \dots, \pi_{2g})$. Let $N$ be the group of $e \in \mathbb{Z}^{2g}$ for which $\prod_{i=1}^{2g} \pi_i^{e_i}$ is a root of unity. Take any $e \in \mathbb{Z}^{2g}$. By Lemma 2.5, we have $e \in N$ if and only if $\sum_{i=1}^{2g} v_\lambda(\pi_i) \cdot e_i = 0$ holds for prime ideals $\lambda | \ell$ of $\mathcal{O}_L$. We have $[L : \mathbb{Q}] \ll_g 1$ since $L$ is the splitting field of a degree $2g$ polynomial and hence $0 \leq v_\lambda(\pi_i) \leq [L : \mathbb{Q}] \ll_g 1$. So $N$ is defined in $\mathbb{Z}^{2g}$ by a finite number of linear equations with integer coefficients, where the number of equations and size of the coefficients can be bounded in terms of $g$. So $N$ is one of a finite number of subgroups $N_1, \dots, N_m$ of $\mathbb{Z}^{2g}$ that depend only on $g$.

The group $M$ is the kernel of $N \to \mu_L$, $e \to \prod_{i=1}^{2g} \pi_i^{e_i}$, where $\mu_L$ is the group of roots of unity in $L^\times$. We have $|\mu_L| \ll_g 1$ since $[L : \mathbb{Q}] \ll_g 1$. So we have $[N : M] \leq C$ for some constant $C$ depending only on $g$. The proposition thus holds where $M_1, \dots, M_s$ are the subgroups of $N_1, \dots, N_m$ of index at most $C$. □

2.5. **Common rank.** The results in this section are due to Serre and details can be found in [LP97]. Fix a prime $\ell$ and denote by $r$ the rank of the reductive group $G^\circ_{A,\ell}$.

**Lemma 2.7.**

(i) *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$ for which $A$ has good reduction. If $\Phi_{A,\mathfrak{p}}$ is a free abelian group, then $\mathfrak{p}$ splits completely in $K_A^{\mathrm{conn}}$ and $\Phi_{A,\mathfrak{p}}$ has rank at most $r$.*

(ii) *There is a set $S$ of prime ideals of $\mathcal{O}_K$ with density 0 such that $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank $r$ for all $\mathfrak{p} \notin S$ that split completely in $K_A^{\mathrm{conn}}$.*

*Proof.* Take any non-zero prime ideal $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_K$ for which $A$ has good reduction. Let $T_\mathfrak{p}$ be the Zariski closure in $G_{A,\ell}$ of the subgroup generated by the semisimple element $t_\mathfrak{p} := \rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$. Note that $T_\mathfrak{p}$ is a commutative algebraic subgroup of $G_{A,\ell}$ and $T_\mathfrak{p}^\circ$ is a torus. Let $X(T_\mathfrak{p})$ be the group of characters $(T_\mathfrak{p})_{\overline{\mathbb{Q}}_\ell} \to \mathbb{G}_{m,\overline{\mathbb{Q}}_\ell}$.

We claim that the groups $X(T_\mathfrak{p})$ and $\Phi_{A,\mathfrak{p}}$ are isomorphic. Let $\Omega \subseteq X(T_\mathfrak{p})$ be the weights of $T_\mathfrak{p} \subseteq \mathrm{GL}_{V_\ell(A)}$ acting on $V_\ell(A)$. The set $\Omega$ generates $X(T_\mathfrak{p})$ since this action is faithful. Since $T_\mathfrak{p}$ is generated by $t_\mathfrak{p}$, the homomorphism $f \colon X(T_\mathfrak{p}) \to \overline{\mathbb{Q}}_\ell^\times$, $\alpha \mapsto \alpha(t_\mathfrak{p})$ is injective. The elements $\{\alpha(t_\mathfrak{p}) : \alpha \in \Omega\}$ are the roots of $P_{A,\mathfrak{p}}(x)$ in $\overline{\mathbb{Q}}_\ell$ and generate the image of $f$. Therefore, we have an isomorphism $X(T_\mathfrak{p}) \to \Phi_{A,\mathfrak{p}}$, $\alpha \mapsto \tau(\alpha(t_\mathfrak{p}))$, where $\tau \colon \overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$ is a fixed embedding. This proves the claim.

Suppose that $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank $s$. From the above claim, $X(T_\mathfrak{p})$ is free abelian of rank $s$ and hence $T_\mathfrak{p}$ is a torus of rank $s$. Since $T_\mathfrak{p}$ is connected, we have $T_\mathfrak{p} \subseteq G^\circ_{A,\ell}$. We have $s \leq r$ since $G^\circ_{A,\ell}$ has rank $r$. We have $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \in T_\mathfrak{p}(\mathbb{Q}_\ell) \subseteq G^\circ_{A,\ell}(\mathbb{Q}_\ell)$, so $\mathfrak{p}$ splits completely in $K_A^{\mathrm{conn}}$ since $K_A^{\mathrm{conn}}$ is the fixed field in $\overline{K}$ of (2.1). This proves (i) for $\mathfrak{p} \nmid \ell$.

The set of prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ that split completely in $K_A^{\mathrm{conn}}$ for which $T_\mathfrak{p}$ is *not* a maximal torus of $G^\circ_{A,\ell}$ has density 0; this follows from Theorem 1.2 of [LP97] which shows it under the assumption $K_A^{\mathrm{conn}} = K$. Part (ii) is a direct consequence of the claim.

Finally, from (ii) we find that $r$ does not depend on the choice of $\ell$. Therefore, (i) holds for the primes $\mathfrak{p} | \ell$ that were excluded above. □

**Proposition 2.8.** *The rank $r$ of the reductive group $G^\circ_{A,\ell}$ does not depend on the prime $\ell$.*

*Proof.* This follows from Lemma 2.7(ii) which gives a characterization of $r$ that does not depend on $\ell$. □

2.6. **The Mumford–Tate group.** Fix a field embedding $\overline{K} \subseteq \mathbb{C}$. The homology group $V := H_1(A(\mathbb{C}), \mathbb{Q})$ is a vector space of dimension $2g$ 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

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

be the cocharacter such that for each $z \in \mathbb{C}^\times = \mathbb{G}_m(\mathbb{C})$, $\mu(z)$ is the automorphism of $V \otimes_{\mathbb{Q}} \mathbb{C}$ that is multiplication by $z$ on $V^{-1,0}$ and the identity on $V^{0,-1}$.

**Definition 2.9.** The Mumford–Tate group of $A$ is the smallest algebraic subgroup of $\mathrm{GL}_V$ defined over $\mathbb{Q}$ that contains $\mu(\mathbb{G}_{m,\mathbb{C}})$. We will denote the Mumford–Tate group of $A$ by $\mathrm{MT}_A$.

The endomorphism ring $\mathrm{End}(A_{\mathbb{C}})$ acts on $V$; this action preserves the Hodge decomposition, and hence commutes with $\mu$ and thus also $\mathrm{MT}_A$. Moreover, the ring $\mathrm{End}(A_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is naturally isomorphic to the commutant of $\mathrm{MT}_A$ in $\mathrm{End}_{\mathbb{Q}}(V)$. The group $\mathrm{MT}_A$ is reductive since the $\mathbb{Q}$-Hodge structure for $V$ is pure and polarizable. Using our fixed embedding $\overline{K} \subseteq \mathbb{C}$ and Proposition 2.3(iv), we have a natural isomorphism $\mathrm{End}(A_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}(A_{K_A^{\mathrm{conn}}}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

The comparison isomorphism $V_\ell(A) \cong V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ induces an isomorphism $\mathrm{GL}_{V_\ell(A)} \cong \mathrm{GL}_{V,\mathbb{Q}_\ell}$; we will use the comparison isomorphism as an identification. The following conjecture says that $G_{A,\ell}^\circ$ and $(\mathrm{MT}_A)_{\mathbb{Q}_\ell}$ are the same algebraic group under the comparison isomorphism, cf. [Ser77, §3].

**Conjecture 2.10** (Mumford–Tate conjecture)**.** *For each prime $\ell$, we have $G_{A,\ell}^\circ = (\mathrm{MT}_A)_{\mathbb{Q}_\ell}$.*

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 2.11.** *For each prime $\ell$, we have $G_{A,\ell}^\circ \subseteq (\mathrm{MT}_A)_{\mathbb{Q}_\ell}$.*

One consequence of the Mumford–Tate conjecture is the central torus of the reductive group $G_{A,\ell}^\circ$ (i.e., the neutral component of the center) is independent of $\ell$. This has been proved unconditionally.

**Proposition 2.12.** *The central tori of $G_{A,\ell}^\circ$ and $(\mathrm{MT}_A)_{\mathbb{Q}_\ell}$ agree for all $\ell$.*

*Proof.* See [Vas08, Theorem 1.3.1] or [UY13, Corollary 2.11]. □

2.7. **Reduction to the connected case.** We now show that to prove our main theorem, we may assume that all the $\ell$-adic monodromy groups are connected.

**Lemma 2.13.** *To prove Theorem 1.2, it suffices to consider the case where all the groups $G_{A,\ell}$ are connected; equivalently, $K_A^{\mathrm{conn}} = K$.*

*Proof.* Assume that Theorem 1.2 holds in the case where all the $\ell$-adic monodromy groups are connected.

Define $L := K_A^{\mathrm{conn}}$ and let $A'$ be the base change of $A$ to $L$. Note that $K_{A'}^{\mathrm{conn}} = L$. By Proposition 2.1(ii), we have $[L:\mathbb{Q}] \ll_g [K:\mathbb{Q}]$. We also have $h(A') = h(A)$. The prime ideal $\mathfrak{q} \subseteq \mathcal{O}_K$ splits completely in $L$ by Lemma 2.7(i). Let $\mathfrak{q}'$ be a prime ideal of $\mathcal{O}_L$ that divides $\mathfrak{q}$. The natural map $\mathbb{F}_{\mathfrak{q}} \to \mathbb{F}_{\mathfrak{q}'}$ is an isomorphism and in particular $N(\mathfrak{q}) = N(\mathfrak{q}')$. Under this isomorphism, the abelian varieties $A_{\mathfrak{q}}$ and $A'_{\mathfrak{q}'}$ agree and hence $\Phi_{A',\mathfrak{q}'}$ is also a free abelian group of rank $r$. The assumption (1.1) thus implies that

$$\ell \geq c \cdot \max(\{[L:\mathbb{Q}], h(A'), N(\mathfrak{q}')\})^\gamma,$$

where $c$ is a possibly larger positive constant that depends only on $g$. By the assumed connected case of Theorem 1.2 and Proposition 2.1(iii), we have

$$[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] = [\mathcal{G}_{A',\ell}(\mathbb{Z}_\ell) : \rho_{A',\ell}(\mathrm{Gal}_L)] \ll_{g,[L:\mathbb{Q}]} 1.$$

Since $[L:\mathbb{Q}] \ll_g [K:\mathbb{Q}]$, we have $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] \ll_{g,[K:\mathbb{Q}]} 1$. This shows that Theorem 1.2(a) holds for $A/K$.

By the assumed connected case of Theorem 1.2, the group $\mathcal{G}^\circ_{A',\ell} = \mathcal{G}_{A',\ell}$ is reductive. So $\mathcal{G}^\circ_{A,\ell} = \mathcal{G}_{A',\ell}$ is reductive which shows that Theorem 1.2(c) holds for $A/K$. By the assumed connected case of Theorem 1.2, we have $\rho_{A',\ell}(\mathrm{Gal}_L)' = \mathcal{G}^\circ_{A',\ell}(\mathbb{Z}_\ell)'$. Therefore, $\rho_{A,\ell}(\mathrm{Gal}_L)' = \mathcal{G}^\circ_{A,\ell}(\mathbb{Z}_\ell)'$ and so Theorem 1.2(d) holds for $A/K$.

Now assume further that $\ell$ is unramified in $K_A^{\mathrm{conn}}$. So $\ell$ is unramified in $K_{A'}^{\mathrm{conn}} = L = K_A^{\mathrm{conn}}$. By the assumed connected case of Theorem 1.2 and Proposition 2.1(iii), we have

$$[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] = [\mathcal{G}_{A',\ell}(\mathbb{Z}_\ell) : \rho_{A',\ell}(\mathrm{Gal}_L)] \ll_g 1.$$

Therefore, Theorem 1.2(b) holds for $A/K$. □

## 3. Some group theory

We now review group theoretic results of Nori, Larsen and Pink. They will be needed for the proofs in the next section.

3.1. **Nori theory.** Fix a positive integer $m$ and a prime $\ell \geq m$; we will later apply this theory with $m = 2g$, where $g \geq 1$ is the dimension of our abelian variety.

Fix a subgroup $\Gamma$ of $\mathrm{GL}_m(\mathbb{F}_\ell)$. Let $\Gamma_u$ be the set of elements in $\Gamma$ of order $\ell$; it is also the set of non-trivial unipotent elements in $\Gamma$ since $\ell \geq m$. Let $\Gamma^+$ be the subgroup of $\Gamma$ generated by $\Gamma_u$. The group $\Gamma^+$ is normal in $\Gamma$ and the quotient $\Gamma/\Gamma^+$ has cardinality relatively prime to $\ell$.

For each $x \in \Gamma_u$, define the homomorphism

$$\varphi_x \colon \mathbb{G}_a \to \mathrm{GL}_m, \quad t \mapsto \exp(t \cdot \log x)$$

of algebraic groups over $\mathbb{F}_\ell$ where we use the truncated series

$$\exp z = \sum\nolimits_{i=0}^{m-1} z^i/i! \quad \text{and} \quad \log z = -\sum\nolimits_{i=1}^{m-1} (1-z)^i/i.$$

To show that $\varphi_x$ is a homomorphism, note that $\log x$ is nilpotent and that $\exp(y+z) = \exp(y)\exp(z)$ for commuting nilpotent $y, z \in M_m(\mathbb{F}_\ell)$.

Let $\mathbf{G}_\Gamma$ be the algebraic subgroup of $\mathrm{GL}_{m,\mathbb{F}_\ell}$ generated by the groups $\varphi_x(\mathbb{G}_a)$ with $x \in \Gamma_u$. The following theorem says that, for $\ell$ sufficiently large, we can recover $\Gamma^+$ from $\mathbf{G}_\Gamma$.

**Theorem 3.1** (Nori)**.** [Nor87, Theorem B] *There is a constant $c_1(m) \geq 2m-2$, depending only on $m$, such that if $\ell > c_1(m)$ and $\Gamma$ is a subgroup of $\mathrm{GL}_m(\mathbb{F}_\ell)$, then $\Gamma^+ = \mathbf{G}_\Gamma(\mathbb{F}_\ell)^+$.*

We now consider the case where $\Gamma$ is a semisimple subgroup of $\mathrm{GL}_m(\mathbb{F}_\ell)$, i.e., the group $\Gamma$ acts semisimply on $\mathbb{F}_\ell^m$ via the natural action. The following lemma is shown during the proof of Corollary B.4 in [EHK12].

**Lemma 3.2.** *Suppose that $\ell > c_1(m)$ and that $\Gamma$ is a semisimple subgroup of $\mathrm{GL}_m(\mathbb{F}_\ell)$. Then $\Gamma^+ \subseteq \mathrm{GL}_m(\mathbb{F}_\ell)$ is semisimple and $\mathbf{G}_\Gamma$ is a semisimple algebraic subgroup of $\mathrm{GL}_{m,\mathbb{F}_\ell}$.*

For a semisimple algebraic group $G$ defined over $\mathbb{F}_\ell$, let $G^{\mathrm{sc}} \to G$ be its simply connected cover.

**Lemma 3.3.** *There is a finite collection $\{\varrho_i \colon G_i \to \mathrm{GL}_m\}_{i \in I}$ of $\mathbb{Z}$-representations of split simply connected Chevalley groups and a constant $c_2(m) \geq c_1(m)$ such that if $\ell > c_2(m)$ and $\Gamma \subseteq \mathrm{GL}_m(\mathbb{F}_\ell)$ is a semisimple subgroup, then the representation*

$$(\mathbf{G}_\Gamma^{sc})_{\overline{\mathbb{F}}_\ell} \to (\mathbf{G}_\Gamma)_{\overline{\mathbb{F}}_\ell} \hookrightarrow \mathrm{GL}_{m,\overline{\mathbb{F}}_\ell}$$

*is isomorphic to the fiber of $\varrho_i$ over $\overline{\mathbb{F}}_\ell$ for some $i \in I$.*

*Proof.* This is Theorem B.7 in [EHK12]; by Lemma 3.2, there is no harm in replacing $\Gamma$ by $\Gamma^+$. □

Finally consider a subgroup $H$ of $\mathrm{GL}_m(\mathbb{Z}_\ell)$ that is closed in the $\ell$-adic topology. Let $S$ be the Zariski closure of $H$ in $\mathrm{GL}_{m,\mathbb{Q}_\ell}$ and let $S^\circ$ be the connected component of the identity. We define the Nori dimension of $H$, which we denote by $\mathrm{Ndim}(H)$, to be the dimension of $\mathbf{G}_\Gamma$, where $\Gamma$ is the image of $H$ in $\mathrm{GL}_m(\mathbb{F}_\ell)$. The following is a special case of a theorem of Larsen, cf. [Lar10, Theorem 7].

**Theorem 3.4** (Larsen)**.** *There are constants $c_3(m)$ and $c_4(m)$, depending only $m$, such that the following hold if $\ell \geq c_3(m)$.*

(i) *We have $\mathrm{Ndim}(H) \leq \dim S$.*
(ii) *If $S^\circ$ is semisimple and $\mathrm{Ndim}(H) = \dim S$, then $[S(\mathbb{Q}_\ell) \cap \mathrm{GL}_m(\mathbb{Z}_\ell) : H] \leq c_4(m)$.*

3.2. **A theorem of Larsen and Pink.** A classic theorem of Jordan say that every finite subgroup $\Gamma$ of $\mathrm{GL}_m(\mathbb{C})$ has a normal abelian subgroup whose index can be bounded by some constant depending only on $m$. Larsen and Pink have given a generalized version that holds for all finite subgroups of $\mathrm{GL}_m(k)$, where $k$ is an arbitrary field. The following is [LP11, Theorem 0.2] specialized to the subgroups of $\mathrm{GL}_m(\mathbb{F}_\ell)$.

**Theorem 3.5** (Larsen-Pink)**.** *Let $\Gamma$ be a subgroup of $\mathrm{GL}_m(\mathbb{F}_\ell)$. Then there are normal subgroups $\Gamma_3 \subseteq \Gamma_2 \subseteq \Gamma_1$ of $\Gamma$ such that the following hold:*

(a) $[\Gamma : \Gamma_1] \leq J(m)$*, where $J(m)$ is a constant depending only on $m$.*
(b) $\Gamma_1/\Gamma_2$ *is a direct product of finite simple groups of Lie type in characteristic $\ell$.*
(c) $\Gamma_2/\Gamma_3$ *is abelian and its order is relatively prime to $\ell$.*
(d) $\Gamma_3$ *is an $\ell$-group.*

## 4. Proof of Theorem 1.2(c) and (d)

Fix an abelian variety $A$ of dimension $g \geq 1$ defined over a number field $K$. For each prime $\ell$, we have a representation

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

By Lemma 2.13, we may assume that all the $\ell$-adic monodromy groups $G_{A,\ell}$ are connected. In particular, $\mathcal{G}^\circ_{A,\ell} = \mathcal{G}_{A,\ell}$.

We can identify the special fiber of the $\mathbb{Z}_\ell$-group scheme $\mathrm{GL}_{T_\ell(A)}$ with the $\mathbb{F}_\ell$-group scheme $\mathrm{GL}_{A[\ell]}$. Denote by

$$\bar{\rho}_{A,\ell} \colon \mathrm{Gal}_K \to \mathcal{G}_{A,\ell}(\mathbb{F}_\ell) = \mathrm{GL}_{A[\ell]}(\mathbb{F}_\ell)$$

the representation obtain by composing $\rho_{A,\ell}$ with reduction modulo $\ell$; equivalently, it describes the natural Galois action on $A[\ell]$.

We fix a non-zero prime ideal $\mathfrak{q} \subseteq \mathcal{O}_K$ for which $\Phi_{A,\mathfrak{q}}$ is a free abelian group of rank $r$, where $r$ is the common rank of the reductive groups $G^\circ_{A,\ell}$. Now consider any prime satisfying

$$\ell \geq c \cdot \max(\{[K : \mathbb{Q}], h(A), N(\mathfrak{q})\})^\gamma,$$

where $c \geq 1$ and $\gamma \geq 1$ are positive constants that depend only on $g$. Throughout this section, we will repeatedly increase the constants $c$ and $\gamma$ to make sure that certain condition hold while always maintaining that they depend only on $g$. In particular, the statement of all lemmas and propositions may require increasing $c$ and $\gamma$.

4.1. **Proof of Theorem 1.2(c).** We will make use of the following criterion of Wintenberger.

**Lemma 4.1.** [Win02, Thérème 1] *Let $L$ be a free $\mathbb{Z}_\ell$-module of rank at most $\ell$ and define the $\mathbb{Q}_\ell$-vector space $V := L \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Let $G$ be a reductive group over $\mathbb{Q}_\ell$, $G \hookrightarrow \mathrm{GL}_V$ a faithful representation and $T$ a maximal torus of $G$. Let $\mathcal{T}$ and $\mathcal{G}$ be the schematic closure of $T$ and $G$, respectively, in $\mathrm{GL}_L$. Suppose further that $\mathcal{T}$ is a torus over $\mathbb{Z}_\ell$. Then $\mathcal{G}$ is a smooth group scheme over $\mathbb{Z}_\ell$. If also $\mathcal{G}_{\mathbb{F}_\ell}$ acts semisimply on $L/\ell L$, then $\mathcal{G}$ is a reductive group scheme over $\mathbb{Z}_\ell$.*

We will apply Lemma 4.1 with $L := T_\ell(A)$, $V := V_\ell(A)$ and $G := G_{A,\ell} \subseteq \mathrm{GL}_{V_\ell(A)}$. The group $G$ is connected by assumption and it is reductive by Proposition 2.3(i). Let $T$ be the Zariski closure in $G_{A,\ell}$ of the subgroup generated by the semisimple element $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{q})$. Observe that $T$ is a maximal torus of $G_{A,\ell}$ if and only if $\Phi_{A,\mathfrak{q}}$ is a free abelian group whose rank equals the rank of $G_{A,\ell}$. Therefore, $T$ is a maximal torus of $G_{A,\ell}$ by our choice of $\mathfrak{q}$.

Denote by $\mathcal{T}$ the Zariski closure of $T$ in $\mathrm{GL}_{T_\ell(A)}$; it is a $\mathbb{Z}_\ell$-group scheme. It is straightforward to verify that $\mathcal{T}$ and $\mathcal{G} := \mathcal{G}_{A,\ell}$ are also the scheme-theoretic closures of $T$ and $G_{A,\ell}$, respectively, in $\mathrm{GL}_{T_\ell(A)}/\mathbb{Z}_\ell$.

**Lemma 4.2.** *The group $\mathcal{G}_{\mathbb{F}_\ell}$ acts semisimply on $L/\ell L = A[\ell]$.*

*Proof.* Theorem 2.4 implies (after appropriately increasing $c$ and $\gamma$) that $A[\ell]$ is a semisimple $\mathbb{F}_\ell[\mathrm{Gal}_K]$-module and that the commutant $R_1$ of $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ in $\mathrm{End}_{\mathbb{F}_\ell}(A[\ell])$ is naturally isomorphic to $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$. Let $R_2$ be the commutant of $\mathcal{G}_{\mathbb{F}_\ell}$ in $\mathrm{End}_{\mathbb{F}_\ell}(A[\ell])$.

We have $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K) \subseteq \mathcal{G}(\mathbb{F}_\ell)$, so to prove that $\mathcal{G}_{\mathbb{F}_\ell}$ acts semisimply on $A[\ell]$, it suffices to show that $R_2 = R_1$. We have $R_2 \subseteq R_1 = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ since $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K) \subseteq \mathcal{G}(\mathbb{F}_\ell)$. To prove the other inclusion, it

thus suffices to show that $\mathcal{G}_{\mathbb{F}_\ell}$ and $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{F}_\ell$ commute. This is immediate since $\mathcal{G}$ is the Zariski closure of $\rho_{A,\ell}(\mathrm{Gal}_K)$ and the actions of $\mathrm{Gal}_K$ and $\mathrm{End}(A)$ on $T_\ell(A)$ commute. □

By increasing $c$, we may assume that $\ell > 2g = \mathrm{rank}_{\mathbb{Z}_\ell} T_\ell(A)$. By the criterion of Lemma 4.1, it thus suffices to show that $\mathcal{T}$ is a torus.

Let $F$ be a splitting field of $P_{A,\mathfrak{q}}(x)$ over $\mathbb{Q}_\ell$ and denote by $\lambda_1,\dots,\lambda_m \in F$ the distinct roots of $P_{A,\mathfrak{q}}(x)$. Let $R$ be the valuation ring of the local field $F$ and denote its residue field by $\mathbb{F}$. Define $D := \prod_{1\le i<j\le m}(\lambda_i-\lambda_j)^2 \neq 0$; it is an integer since $P_{A,\mathfrak{q}}(x)$ has coefficients in $\mathbb{Z}$. Since the roots of $P_{A,\mathfrak{q}}(x)$ have absolute value $N(\mathfrak{q})^{1/2}$ under any embedding $F\hookrightarrow\mathbb{C}$, we find that $|D| < cN(\mathfrak{q})^\gamma$ after increasing $c$ and $\gamma$ appropriately. If $\mathfrak{q}$ divides $\ell$, then $\ell \le N(\mathfrak{q})$. So by increasing $c$ and $\gamma$ appropriately, we may assume that $\mathfrak{q}\nmid\ell$ and $D\not\equiv 0 \pmod{\ell}$. This implies that $F/\mathbb{Q}_\ell$ is an unramified extension.

Since $\operatorname{Spec} R\to\operatorname{Spec}\mathbb{Z}_\ell$ is faithfully flat, it suffices to prove that $\mathcal{T}_R$ is a torus. To show this we will use the following lemma.

**Lemma 4.3.** *Take any matrix $B\in\mathrm{GL}_{2g}(R)$ that is semisimple in $\mathrm{GL}_{2g,F}$ and has characteristic polynomial $P_{A,\mathfrak{q}}(x)$. Then the Zariski closure in $\mathrm{GL}_{2g,R}$ of the subgroup generated by $B$ is a split torus over $R$.*

*Proof.* Take any $1\le i\le m$. Let $L_i$ be the $R$-submodule of $R^{2g}$ consisting of those $v\in R^{2g}$ that satisfy $Bv=\lambda_i v$. Since $B$ is semisimple, it acts on $L_i$ as multiplication by $\lambda_i$. Let $d_i$ be the rank of the $R$-module $L_i$. By the assumption of the lemma, $B$ is diagonalizable in $\mathrm{GL}_{2g}(F)$ and hence $F^{2g}=\oplus_{i=1}^m L_i\otimes_R F$. In particular, we have $2g=\sum_{i=1}^m d_i$ by taking dimensions.

Let $\varphi\colon R^{2g}\to\mathbb{F}^{2g}$ be the reduction map. For each $1\le i\le m$, define the $\mathbb{F}$-vector space $V_i:=\varphi(L_i)$.

We claim that $\dim_{\mathbb{F}} V_i = d_i$. By the structure theorem for finitely generated modules over a PID, there is a basis $e_1,\dots,e_{2g}$ of the $R$-module $R^{2g}$ such that

$$L_i = R\pi^{a_1}\cdot e_1\oplus\cdots\oplus R\pi^{a_{d_i}}\cdot e_{d_i}$$

with integers $a_j\ge 0$, where $\pi$ is a uniformizer of $R$. Note that if $\pi^a b$ is in $L_i$ for some $b\in R^{2g}$ and $a\ge 0$, then we have $b\in L_i$. Therefore, $a_1=\cdots=a_{d_i}=0$. The claim follows since we find that $V_i=\varphi(L_i)$ is a vector space over $\mathbb{F}$ with basis $\varphi(e_1),\dots,\varphi(e_{d_i})$.

Let $\overline{B}\in\mathrm{GL}_{2g}(\mathbb{F})$ be the reduction of $B$. The matrix $\overline{B}$ acts on $V_i$ as scalar multiplication by $\bar\lambda_i$, where $\bar\lambda_i$ is the image of $\lambda_i$ in $\mathbb{F}$ (we have $\lambda_i\in R$ since it is a root of the monic polynomial $P_{A,\mathfrak{q}}(x)\in\mathbb{Z}[x]$). For distinct $1\le i<j\le m$, we have $\bar\lambda_i\neq\bar\lambda_j$ since otherwise the image of $D=\prod_{1\le i<j\le m}(\lambda_i-\lambda_j)^2$ in $\mathbb{F}$ is 0 which contradicts that $\ell\nmid D$. Since $\bar\lambda_1,\dots,\bar\lambda_m$ are distinct eigenvalues of $\overline{B}$ and $\sum_{i=1}^m\dim_{\mathbb{F}}V_i=\sum_{i=1}^m d_i=2g$, we deduce that $\oplus_{i=1}^m V_i=\mathbb{F}^{2g}$. Therefore, $\varphi(\oplus_{i=1}^m L_i)=\mathbb{F}^{2g}$. By Nakayama's lemma, we have $\oplus_{i=1}^m L_i=R^{2g}$. Therefore, $B$ is conjugate in $\mathrm{GL}_2(R)$ to a diagonal matrix.

So without loss of generality, we may assume that $B$ is a diagonal matrix. In particular, we can view $B$ as an $R$-point of the diagonal subgroup $\mathbb{G}_{m,R}^{2g}$ of $\mathrm{GL}_{2g,R}$. Let $\mathcal{T}$ be the Zariski closure in $\mathbb{G}_{m,R}^{2g}$ of the subgroup generated by $B$. The fiber $\mathcal{T}_F$ is a torus of rank $r$ since the eigenvalues in $F^\times$ of $B$ generate a free abelian group of rank $r$ (this uses that the characteristic polynomial of $B$ is $P_{A,\mathfrak{q}}(x)$ and our choice of $\mathfrak{q}$). There is thus a set of equations of the form $\prod_{i=1}^{2g}x_i^{a_i}=1$, with integers $a_i$, that cut out $\mathcal{T}_F$ in $\mathbb{G}_{m,F}^{2g}$. These equations thus define $\mathcal{T}$ and hence it is a subtorus of $\mathbb{G}_{m,R}^{2g}$. □

We now complete the proof by verifying that $\mathcal{T}_R$ is a torus. Set $B:=\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{q}})$; it semisimple and has characteristic polynomial $P_{A,\mathfrak{q}}(x)$. From our choice of $\mathfrak{q}$, the Zariski closure in $\mathrm{GL}_{V_\ell(A)}$ of the group generated by $B$ is a maximal torus of $G_{A,\ell}$. The group $\mathcal{T}_R$ is the Zariski closure in $(\mathrm{GL}_{T_\ell(A)})_R=\mathrm{GL}_{T_\ell(A)\otimes_{\mathbb{Z}_\ell}R}$ of the group generated by $B$. By choosing an $R$-basis of $T_\ell(A)\otimes_{\mathbb{Z}_\ell}R$, Lemma 4.3 implies that $\mathcal{T}_R$ is a torus.

4.2. **The reductive group $H_{A,\ell}$ of Serre.** Recall that $\mathcal{G}_{A,\ell}$ is reductive by §4.1. Let $\mathcal{C}_{A,\ell}$ be the central torus $\mathcal{G}_{A,\ell}$ and denote by $C_{A,\ell}\subseteq\mathrm{GL}_{A[\ell]}$ the torus obtained by base changing $\mathcal{C}_{A,\ell}$ to $\mathbb{F}_\ell$. Since $\mathcal{C}_{A,\ell}$ commutes with $\rho_{A,\ell}(\mathrm{Gal}_K)\subseteq\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$, we find that $C_{A,\ell}$ commutes with $\bar\rho_{A,\ell}(\mathrm{Gal}_K)$. Let $\mathcal{S}_{A,\ell}$ be the derived subgroup of $\mathcal{G}_{A,\ell}$; it is semisimple group scheme over $\mathbb{Z}_\ell$.

We now consider the algebraic subgroup $\mathbf{G}_\Gamma\subseteq\mathrm{GL}_{A[\ell]}$ constructed as in §3.1 with $\Gamma:=\bar\rho_{A,\ell}(\mathrm{Gal}_K)$. Note that after possibly increasing the constants $c$ and $\gamma$, Theorem 2.4 implies that $A[\ell]$ is a semisimple $\Gamma$-module.

**Lemma 4.4.** *The group $\mathbf{G}_\Gamma$ is semisimple and commutes with $C_{A,\ell}$.*

*Proof.* After possibly increasing $c$, Lemma 3.2 implies that $\mathbf{G}_\Gamma$ is a semisimple subgroup of $\mathrm{GL}_{A[\ell]}$. That $\mathbf{G}_\Gamma$ commutes with $C_{A,\ell}$ is an easy consequence of $\Gamma$ commuting with $C_{A,\ell}$. □

Define the algebraic subgroup

$$H_{A,\ell} := C_{A,\ell} \cdot \mathbf{G}_\Gamma$$

of $\mathrm{GL}_{A[\ell]}$. The group $H_{A,\ell}$, for $\ell$ sufficiently large, was first defined by Serre [Ser00, 136].

The group $H_{A,\ell}$ is reductive by Lemma 4.4. From the image of the representation $\rho_{A,\ell}$, we have constructed two reductive subgroups $H_{A,\ell}$ and $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ of $\mathrm{GL}_{A[\ell]}$. We now prove that they agree; this is the main result of this section.

**Theorem 4.5.** *We have $H_{A,\ell} = (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$. In particular, we have $\mathbf{G}_\Gamma = (\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$.*

We will use the following criterion to verify that the reductive groups $H_{A,\ell}$ and $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ are equal.

**Lemma 4.6.** [Win02, Lemma 7] *Let $F$ be a perfect field whose characteristic is $0$ or at least $5$. Let $G_1 \subseteq G_2$ be reductive groups defined over $F$ that have the same rank. Suppose we have a faithful linear representation $G_2 \hookrightarrow \mathrm{GL}_V$, where $V$ is a finite dimension $F$-vector space, such that the centers of the commutants of $G_1$ and $G_2$ in $\mathrm{End}_F(V)$ are the same $F$-algebra $R$. Suppose further that the commutative $F$-algebra $R$ is semisimple. Then $G_1 = G_2$.* □

We first show that one of our reductive groups is a subgroup of the other.

**Lemma 4.7.** *There is an inclusion $H_{A,\ell} \subseteq (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$.*

*Proof.* The reductive groups $H_{A,\ell}$ and $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ both have the same central torus $C_{A,\ell}$, so it suffices to prove that $\mathbf{G}_\Gamma \subseteq (\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$. After possibly increasing $c$, we may assume that $\ell \geq 2g$. Take any $x \in \Gamma$ of order $\ell$ and let $\varphi_x \colon \mathbb{G}_a \to \mathrm{GL}_{A[\ell]}$ be the homomorphism $t \mapsto \exp(t \cdot \log x)$ as in §3.1. Using that $\mathcal{S}_{A,\ell}$ is semisimple and by possibly increasing $c$, Lemma 6 of [Win02] implies that the image of $\varphi_x$ is contained in $(\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$. Since $x$ is an arbitrary element of $\Gamma$ of order $\ell$, we deduce that $\mathbf{G}_\Gamma$ is contained in $(\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$. □

The following lemma, which we will prove in §4.3, shows that $H_{A,\ell}(\mathbb{F}_\ell)$ contains a large subgroup of $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$.

**Lemma 4.8.** *There is a constant $b \geq 1$, depending only on $g$, such that $\bar{\rho}_{A,\ell}(\mathrm{Gal}_L) \subseteq H_{A,\ell}(\mathbb{F}_\ell)$ for some extension $L/K$ with $[L : K] \leq b$.*

The following lemma, which we will prove in §4.5, shows that our groups have the same rank.

**Lemma 4.9.** *The reductive groups $H_{A,\ell}$ and $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ have the same rank.*

**Lemma 4.10.** *The commutants of $H_{A,\ell}$ and $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ in $\mathrm{End}_{\mathbb{F}_\ell}(A[\ell])$ agree and their common center is a semisimple $\mathbb{F}_\ell$-algebra.*

*Proof.* Let $L$ be the extension of $K$ from Lemma 4.8. After possibly increasing $c$, Theorem 2.4 and $[L : K] \ll_g 1$ implies that the commutant $R$ of $\bar{\rho}_{A,\ell}(\mathrm{Gal}_L)$ in $\mathrm{End}(A[\ell])$ is naturally isomorphic to $\mathrm{End}(A_L) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ and that $R$ is a semisimple $\mathbb{F}_\ell$-algebra. In fact, we have a natural isomorphism $R = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ since $\mathrm{End}(A) = \mathrm{End}(A_{\overline{K}})$ by Proposition 2.3 and our assumption that $G_{A,\ell}$ is connected. Since $R$ is semisimple, the center of $R$ is semisimple.

Let $R_1$ and $R_2$ be the commutants of $H_{A,\ell}$ and $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$, respectively, in $\mathrm{End}_{\mathbb{F}_\ell}(A[\ell])$. We have inclusion $R_2 \subseteq R_1 \subseteq R$ since $\bar{\rho}_{A,\ell}(\mathrm{Gal}_L) \subseteq H_{A,\ell}(\mathbb{F}_\ell)$ by our choice of $L$ and since $H_{A,\ell} \subseteq (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ by Lemma 4.7. So it suffices to show that $R = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ is a subring of $R_2$. Equivalently, it suffices to show that $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ commutes with $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$; this is immediate since the actions of $\mathrm{Gal}_K$ and $\mathrm{End}(A)$ on $T_\ell(A)$ commute. □

*Proof of Theorem 4.5.* We may assume that $\ell \geq 5$ after possibly increasing $c$. Set $G_1 := H_{A,\ell}$ and $G_2 := (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$. Using Lemma 4.6 with Lemmas 4.7, 4.9 and 4.10, we deduce that $G_1 = G_2$. □

4.3. **Proof of Lemma 4.8.** Let $\Gamma_3 \subseteq \Gamma_2 \subseteq \Gamma_1$ be the normal subgroups of $\Gamma := \bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ as in Theorem 3.5 with $m = 2g$. By increasing $c$, we may assume that $\ell > \max\{J(2g), 2g, 7\}$.

Since $\Gamma = \bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ acts semisimply on the $\mathbb{F}_\ell$-vector space $A[\ell]$ and $\Gamma_3$ is a normal subgroup of $\Gamma$, we deduce by Clifford's theorem [CR81, 11.1] that $\Gamma_3$ also acts semisimply on $A[\ell]$. Since $\ell > 2g$ and $\Gamma_3$ is an $\ell$-group, the action of $\Gamma_3$ on $A[\ell]$ is unipotent. Since the action of $\Gamma_3$ on $A[\ell]$ is unipotent and semisimple, we must have $\Gamma_3 = 1$. In particular, $\Gamma_2$ is an abelian group with cardinality relatively prime to $\ell$.

**Lemma 4.11.** *The group $\Gamma_2$ has a set of generators with cardinality at most $2g$.*

*Proof.* Since $\Gamma_2$ is abelian and has order relatively prime to $\ell$, it must lie in a maximal torus T of $\mathrm{GL}_{A[\ell]} \cong \mathrm{GL}_{2g,\mathbb{F}_\ell}$. Let $\mathbb{F}$ be a finite extension of $\mathbb{F}_\ell$ over which T is split. So $\Gamma_2$ is a subgroup of $\mathrm{T}(\mathbb{F}) \cong (\mathbb{F}^\times)^{2g}$. Since $\mathbb{F}^\times$ is cyclic, $\Gamma_2$ lies in a finite abelian group generated by $2g$ elements. The lemma is now easy from the structure theorem for finite abelian groups. □

**Lemma 4.12.** *The center of $\Gamma_1$ is $\Gamma_2$.*

*Proof.* Since $\Gamma_1/\Gamma_2$ is a product of non-abelian simple groups, we find that the cardinality of the center of $\Gamma_1$ divides $|\Gamma_2|$. It thus suffices to show that $\Gamma_2$ lies in the center of $\Gamma_1$; equivalently, that the homomorphism $\varphi\colon \Gamma_1/\Gamma_2 \to \mathrm{Aut}(\Gamma_2)$ arising from conjugation is trivial.

Suppose that $\varphi \neq 1$. Then for some prime $p$ dividing $|\Gamma_2|$, there is a finite simple group $S$ of Lie type in characteristic $\ell$ that acts non-trivially on the $p$-Sylow subgroup $W$ of $\Gamma_2$. We view $W$ as an additive group. Define $\mathcal{W} := p^i W$, where $i \geq 0$ is the largest integer such that $S$ acts nontrivially on $\mathcal{W}$ and trivially on $p\mathcal{W}$.

Suppose that $S$ acts trivially on the quotient group $\mathcal{W}/p\mathcal{W}$. Take any $w \in \mathcal{W}$. We thus have a well-defined map $\xi_w\colon S \to p\mathcal{W}$, $h \mapsto h(w) - w$. Using that $S$ acts trivially on $p\mathcal{W}$, we find that

$$\xi_w(h_1h_2) = h_1h_2(w) - w = h_1(w + \xi_w(h_2)) - w = h_1(w) - w + \xi_w(h_2) = \xi_w(h_1) + \xi_w(h_2)$$

for all $h_1, h_2 \in S$. Therefore, $\xi_w\colon S \to p\mathcal{W}$ is a homomorphism. Since the group $S$ is nonabelian and simple and $p\mathcal{W}$ is abelian, we must have $\xi_w = 0$. Since $w \in \mathcal{W}$ was arbitrary, we deduce that $S$ acts trivially on $\mathcal{W}$ which contradicts our choice of $\mathcal{W}$.

Therefore, $S$ acts non-trivially on the $\mathbb{F}_p$-vector space $\mathcal{W}/p\mathcal{W}$. From Lemma 4.11, the dimension of $\mathcal{W}/p\mathcal{W}$ as an $\mathbb{F}_p$-vector space is at most $2g$. Since $S$ is simple, we deduce that $S$ is isomorphic to a subgroup of $\mathrm{GL}_{2g}(\mathbb{F}_p)$.

Since $\ell$ divides $|S|$ and $\ell > J(2g)$, Theorem 3.5 (with $m = 2g$ and $\ell$ replaced by $p$) implies that $S$ is a finite simple group of Lie type in characteristic $p$. However, there is no finite simple group $S$ that is of Lie type in two distinct characteristics $p$ and $\ell > 7$. (We need $\ell > 7$ to avoid the exceptional isomorphism $\mathrm{PSL}_2(\mathbb{F}_7) \cong \mathrm{PSL}_3(\mathbb{F}_2)$.) This contradiction ensures that $\varphi = 1$. □

Let $\psi\colon \mathrm{Gal}_K \to \bar{\rho}_{A,\ell}(\mathrm{Gal}_K)/\Gamma_1$ be the homomorphism obtained by composing $\bar{\rho}_{A,\ell}$ with the obvious quotient map. We define $L$ to be the fixed field in $\overline{K}$ of $\ker(\psi)$; we have $\bar{\rho}_{A,\ell}(\mathrm{Gal}_L) = \Gamma_1$. The field $L$ is a Galois extension of $K$ which satisfies $[L : K] \leq J(2g)$. Since $\ell > J(2g)$, we have $\bar{\rho}_{A,\ell}(\mathrm{Gal}_L)^+ = \Gamma^+$.

**Lemma 4.13.** *The group $\Gamma_1$ is generated by $\Gamma_2$ and $\Gamma^+$.*

*Proof.* The group $\Gamma^+ = \bar{\rho}_{A,\ell}(\mathrm{Gal}_L)^+$ is a contained in $\Gamma_1 = \bar{\rho}_{A,\ell}(\mathrm{Gal}_L)$. The homomorphism $\Gamma^+ \to \Gamma_1/\Gamma_2$ is surjective since $\ell \nmid |\Gamma_2|$ and since any finite simple group of Lie type in characteristic $\ell$ is generated by its elements of order $\ell$. Therefore, $\Gamma_1$ is generated by $\Gamma^+$ and $\Gamma_2$. □

Let $Z$ be the center of $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$; we have $Z^\circ = C_{A,\ell}$.

**Lemma 4.14.** *The group $\Gamma_2$ is contained in $Z(\mathbb{F}_\ell)$.*

*Proof.* After possibly increasing $c$ and $\gamma$, Theorem 2.4 implies that the centralizer of $\Gamma_1 = \bar{\rho}_{A,\ell}(\mathrm{Gal}_L)$ in $\mathrm{End}_{\mathbb{F}_\ell}(A[\ell])$ is $\mathrm{End}(A_L) \otimes_{\mathbb{Z}} \mathbb{F}_\ell = \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{F}_\ell$ (recall that $[L : k] \leq J(2g)$). The group $\Gamma_2$ is contained in the center of $\Gamma_1$ by Lemma 4.12, so we can identify $\Gamma_2$ with a subgroup of $(\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{F}_\ell)^\times$. The group $(\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{F}_\ell)^\times$, and hence also $\Gamma_2$, commutes with $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$. Since $\Gamma_2 \subseteq \bar{\rho}_{A,\ell}(\mathrm{Gal}_k) \subseteq \mathcal{G}_{A,\ell}(\mathbb{F}_\ell)$, we deduce that $\Gamma_2$ lies in the center of $(\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$. □

Let $\widetilde{H}$ be the algebraic subgroup of $\mathrm{GL}_{A[\ell]}$ generated by $Z$ and $\mathbf{G}_\Gamma$; note that $Z$ and $\mathbf{G}_\Gamma$ commute since $\overline{\rho}_{A,\ell}(\mathrm{Gal}_k)$ commutes with $Z$. Observe that the neutral component of $\widetilde{H}$ is precisely our reductive group $H_{A,\ell}$. By Lemma 4.14, we have $\Gamma_2 \subseteq \widetilde{H}(\mathbb{F}_\ell)$. Since $\mathbf{G}_\Gamma(\mathbb{F}_\ell)^+ = \Gamma^+$ by Theorem 3.1, after possibly increasing $c$, we find that $\Gamma^+$ is contained $\widetilde{H}(\mathbb{F}_\ell)$. Therefore, $\Gamma_1$ is a subgroup of $\widetilde{H}(\mathbb{F}_\ell)$ by Lemma 4.13.

**Lemma 4.15.** *The index of $H_{A,\ell}$ in $\widetilde{H}$ can be bounded by a constant depending only on $g$.*

*Proof.* Equivalently, we need to bound the index of $C_{A,\ell}$ in $Z$. It suffices to bound the cardinality of the center of the semisimple group $G := (\mathcal{G}_{A,\ell})_{\overline{\mathbb{F}}_\ell}/(C_{A,\ell})_{\overline{\mathbb{F}}_\ell}$. This is clear since $G$ is a semisimple group whose rank is bounded in terms of $g$; the cardinality of the center can be bounded in terms of the root datum of $G$ and there are only finitely many root datum for semisimple groups of bounded rank. (Moreover, the cardinality of the center of a semisimple group of rank $r$ is bounded above by $2^r$.) □

We have shown that $\Gamma_1 = \overline{\rho}_{A,\ell}(\mathrm{Gal}_L)$ is a subgroup of $\widetilde{H}(\mathbb{F}_\ell)$. Let $L'$ be the smallest extension of $L$ for which $\overline{\rho}_{A,\ell}(\mathrm{Gal}_{L'}) \subseteq H_{A,\ell}(\mathbb{F}_\ell)$. By Lemma 4.15, the degree $[L' : L]$ can be bounded in terms of $g$. We have already seen that $[L : K]$ can be bounded in terms of $g$. Therefore, we have $\overline{\rho}_{A,\ell}(\mathrm{Gal}_{L'}) \subseteq H_{A,\ell}(\mathbb{F}_\ell)$ with $[L' : K] \ll_g 1$.

4.4. **Complexity of $H_{A,\ell}$.** Define the $\mathbb{Z}$-torus $D := \mathbb{G}_m^{2g}$; we will identify it with the diagonal torus of $\mathrm{GL}_{2g,\mathbb{Z}}$. Let $X(D)$ be the group of characters $D \to \mathbb{G}_m$. We have an isomorphism

$$\mathbb{Z}^{2g} \xrightarrow{\sim} X(D), \quad m \mapsto \alpha_m,$$

where $\alpha_m$ is the character given by $(x_1, \dots, x_{2g}) \mapsto \prod_i x_i^{m_i}$.

Consider a field $F$ and a connected and reductive subgroup $G$ of $\mathrm{GL}_{2g,F}$. Choose an algebraically closed extension $F'/F$ and a torus $T$ in the diagonal torus $D_{F'} \subseteq \mathrm{GL}_{2g,F'}$ that is conjugate to a maximal torus of $G_{F'}$ by some element of $\mathrm{GL}_{2g}(F')$. We define the complexity of $G$ to be the smallest integer $\mathscr{F}(G) \geq 1$ satisfying

$$T = \bigcap_{m \in M} \ker \alpha_m$$

in $D_{F'}$ for some subset $M \subseteq \mathbb{Z}^{2g}$ with $|m_i| \leq \mathscr{F}(G)$ for all $m \in M$ and $1 \leq i \leq 2g$. We can identify the character group of $T$ with $\mathbb{Z}^{2g}/\mathbb{Z}M$. Note that $\mathscr{F}(G)$ does not depend on the choice of $F'$ or $T$.

The goal of this section is to show that $\mathscr{F}(H_{A,\ell}) \ll_g 1$.

**Lemma 4.16.** *We have $\mathscr{F}(G_{A,\ell}) \ll_g 1$.*

*Proof.* Let $T$ be the Zariski closure in $G_{A,\ell}$ of the group generated by $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{q})$. As observed in §4.1, $T$ is a maximal torus of $G_{A,\ell}$. Take $t \in D(\overline{\mathbb{Q}}_\ell)$ that is conjugate to $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{q})$. We have $t = (\pi_1, \dots, \pi_{2g})$, where the $\pi_i$ are the roots of $P_{A,\mathfrak{q}}(x)$ in $\overline{\mathbb{Q}}_\ell$ with multiplicity. Let $N \subseteq \mathbb{Z}^{2g}$ be the group of $m \in \mathbb{Z}^{2g}$ for which $\prod_{i=1}^{2g} \pi_i^{m_i} = 1$. Choose a finite set $M$ of generators for $N$ with $B := \max\{|m_i| : m \in M, 1 \leq i \leq 2g\}$ minimal. We have $\mathscr{F}(G_{A,\ell}) = \mathscr{F}(T) \leq B$. Proposition 2.6 says that there are only finitely many possibilities for the group $N$ in terms of $g$. We can thus bound $B$ in terms of $g$. □

**Lemma 4.17.** *We have $\mathscr{F}(C_{A,\ell}) \ll_g 1$.*

*Proof.* Define $C := (\mathcal{C}_{A,\ell})_{\mathbb{Q}_\ell}$; it is the central torus of $G_{A,\ell}$. Since $\mathcal{C}_{A,\ell}$ is a torus with special fiber $C_{A,\ell}$, we have $\mathscr{F}(C_{A,\ell}) = \mathscr{F}(C)$. So it suffices to prove $\mathscr{F}(C) \ll_g 1$.

The center of $G_{A,\ell}$ is the intersection of all of its maximal tori. Since $G_{A,\ell}$ has rank $r$, there are maximal tori $T_0, \dots, T_r$ of $G$ such that the neutral component of $Z := T_0 \cap \cdots \cap T_r$ is $C$.

Using that $\mathscr{F}(T_i) = \mathscr{F}(G_{A,\ell}) \ll_g 1$ by Lemma 4.16, we find that there an integer $B \geq 1$ depending only on $g$ and subset $M \subseteq \mathbb{Z}^{2g}$ such that

$$Z = \bigcap_{m \in M} \ker \alpha_m$$

and $|m_i| \leq B$ for all $m \in M$ and $1 \leq i \leq 2g$. We thus have $C = \cap_{m \in M'} \ker \alpha_m$, where $M'$ is any finite set that generates the smallest group $\mathbb{Z}M \subseteq N \subseteq \mathbb{Z}^{2g}$ for which $\mathbb{Z}^{2g}/N$ is torsion-free. We can choose $M'$ so

that $B' := \max\{|m_i| : m \in M', 1 \le i \le 2g\}$ is minimal. Since there are only finitely many possible $M$ for a given $g$, we find that $B' \ll_g 1$. Therefore, $\mathscr{F}(C) \le B' \ll_g 1$. □

**Lemma 4.18.** *We have $\mathscr{F}(\mathbf{G}_\Gamma) \ll_g 1$.*

*Proof.* After possibly increasing $c$, we may assume that $\ell > c_2(2g)$, with $c_2(2g)$ as in Lemma 3.3. Let $\{\varrho_i \colon G_i \to \mathrm{GL}_{2g}\}_{i\in I}$ be the representations of Lemma 3.3 with $m = 2g$; they depend only on $g$.

Fix a split maximal torus $T_i$ of $G_i$ and define $H_i := \varrho_i(T_i)_{\overline{\mathbb{F}}_\ell}$. We have $\mathscr{F}(H_i) = \mathscr{F}(\varrho_i(G_i)_{\overline{\mathbb{Q}}}) =: f_i$, which does not depend on $\ell$. Lemma 3.3 implies that any maximal torus $T \subseteq (\mathbf{G}_\Gamma)_{\overline{\mathbb{F}}_\ell}$ is conjugate in $\mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell}$ to $H_i$ for some $i \in I$. Therefore,

$$\mathscr{F}(\mathbf{G}_\Gamma) = \mathscr{F}(T) = \mathscr{F}(H_i) = f_i.$$

Since $I$ is finite, we have $\mathscr{F}(\mathbf{G}_\Gamma) \le \max\{f_i : i \in I\} \ll_g 1$. □

Combining the previous two lemmas, we deduce the following.

**Lemma 4.19.** *We have $\mathscr{F}(H_{A,\ell}) \le B$, where $B$ is a positive integer depending only on $g$.*

*Proof.* Let $T$ be a subtorus of $D_{\overline{\mathbb{F}}_\ell}$ that is conjugate in $\mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell} \cong \mathrm{GL}_{A[\ell],\overline{\mathbb{F}}_\ell}$ to a maximal torus of $(H_{A,\ell})_{\overline{\mathbb{F}}_\ell}$. We have $T = T_1 \cdot T_2$, where $T_1$ and $T_2$ are conjugate to $(C_{A,\ell})_{\overline{\mathbb{F}}_\ell}$ and to a maximal torus of $(\mathbf{G}_\Gamma)_{\overline{\mathbb{F}}_\ell}$, respectively. By Lemmas 4.17 and 4.18, we have $\mathcal{F}(T_1) \ll_g 1$ and $\mathcal{F}(T_2) \ll_g 1$.

So there are subsets $M_1$ and $M_2$, with $\max\{|m_i| : m \in M_1 \cup M_2, 1 \le i \le 2g\} \ll_g 1$ such that $T_i = \cap_{m\in M_i} \ker \alpha_m$ for $1 \le i \le 2$. We then have $T = \cap_{m\in M} \ker \alpha_m$, where $M$ is a finite set of generators of the subgroup $\mathbb{Z}M_1 \cap \mathbb{Z}M_2$ of $\mathbb{Z}^{2g}$. We can choose $M$ so that $B := \max\{|m_i| : m \in M, 1 \le i \le 2g\}$ is minimal. Since there are only finitely many possible $M_1$ and $M_2$ for a given $g$, we find that $B \ll_g 1$. Therefore, $\mathscr{F}(H_{A,\ell}) = \mathscr{F}(T) \le B \ll_g 1$. □

4.5. **Proof of Lemma 4.9.** Take $B$ as in Lemma 4.19. With our fixed prime $\mathfrak{q}$, let $\pi_1, \dots, \pi_{2g} \in \overline{\mathbb{Q}}$ be the roots of $P_{A,\mathfrak{q}}(x)$ with multiplicity and define the number field $F := \mathbb{Q}(\pi_1, \dots, \pi_{2g})$. Let $\mathcal{M}$ be the (finite) set of subsets $M \subseteq \mathbb{Z}^{2g}$ such that

$$\max\{|m_i| : m \in M, 1 \le i \le 2g\} \le B$$

and such that $\mathrm{rank}_{\mathbb{Z}}(\mathbb{Z}M) > 2g - r$. For each $M \in \mathcal{M}$, define

$$\beta_M := \sum_{m\in M} N_{F/\mathbb{Q}}\Big( \prod_{1\le i\le 2g,\, m_i>0} \pi_i^{m_i} - \prod_{1\le i\le 2g,\, m_i<0} \pi_i^{-m_i} \Big)^2;$$

it is an integer since all the $\pi_i$ are algebraic integers.

**Lemma 4.20.** *If $\mathrm{rank}(H_{A,\ell}) \ne r$, then $\beta_M \equiv 0 \pmod{\ell}$ for some $M \in \mathcal{M}$.*

*Proof.* Suppose that $\mathrm{rank}(H_{A,\ell}) \ne r$. From Lemma 4.7, we have an inclusion $H_{A,\ell} \subseteq (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ in $\mathrm{GL}_{A[\ell]}$ of reductive groups. Therefore,

$$\mathrm{rank}(H_{A,\ell}) \le \mathrm{rank}((\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}) = \mathrm{rank}(G_{A,\ell}) = r.$$

Our assumption implies that $\mathrm{rank}(H_{A,\ell}) < r$.

Let $T$ be a subtorus of $D_{\overline{\mathbb{F}}_\ell}$ that is conjugate in $\mathrm{GL}_{2g,\overline{\mathbb{F}}_\ell} \cong \mathrm{GL}_{A[\ell],\overline{\mathbb{F}}_\ell}$ to a maximal torus of $(H_{A,\ell})_{\overline{\mathbb{F}}_\ell}$. By Lemma 4.19, there is a set $M \subseteq \mathbb{Z}^{2g}$ such that $T = \cap_{m\in M} \ker \alpha_m$ and such that $|m_i| \le B$ for all $m \in M$ and $1 \le i \le 2g$. We have $X(T) \cong \mathbb{Z}^{2g}/M$ and hence $\dim T = 2g - \mathrm{rank}_{\mathbb{Z}}(\mathbb{Z}M)$. Therefore,

$$\mathrm{rank}_{\mathbb{Z}}(\mathbb{Z}M) = 2g - \dim T = 2g - \mathrm{rank}(H_{A,\ell}) > 2g - r,$$

and hence $M \in \mathcal{M}$.

After possibly increasing $c$ and $\gamma$, we may assume that $\ell > N(\mathfrak{q})$ and hence $\mathfrak{q} \nmid \ell$. So $\overline{\rho}_{A,\ell}$ is unramified at $\mathfrak{q}$ and $\overline{\rho}_{A,\ell}(\mathrm{Frob}_{\mathfrak{q}})$ has characteristic polynomial $P_{A,\mathfrak{q}}(x)$ modulo $\ell$. The semisimple component of $\overline{\rho}_{A,\ell}(\mathrm{Frob}_{\mathfrak{q}})$ is conjugate in $\mathrm{GL}_{2g}(\overline{\mathbb{F}}_\ell)$ to an element $t \in T(\overline{\mathbb{F}}_\ell)$. Let $b_1, \dots, b_{2g} \in \overline{\mathbb{F}}_\ell$ be the diagonal entries of $t$. Let $\lambda$ be a prime ideal of $\mathcal{O}_F$ dividing $\ell$ and choose an embedding $\mathbb{F}_\lambda \hookrightarrow \overline{\mathbb{F}}_\ell$. After first possibly conjugating $T$ and $t$ by some element of $\mathrm{GL}_{2g}(\overline{\mathbb{F}}_\ell)$, we may assume that the image of $\pi_i$ modulo $\lambda$ is $b_i$.

Take any $m \in M$. We have $t \in T(\overline{\mathbb{F}}_\ell)$, so $\prod_i b_i^{m_i} = 1$ and hence

$$\prod_{i,\, m_i>0} b_i^{m_i} - \prod_{i,\, m_i<0} b_i^{-m_i} = 0.$$

Therefore,

$$\prod_{1\le i\le 2g,\, m_i>0} \pi_i^{m_i} - \prod_{1\le i\le 2g,\, m_i<0} \pi_i^{-m_i} \equiv 0 \pmod{\lambda}$$

for all $m \in M$. The lemma is now clear since $\beta_M$ is the sum of integers divisible by $\ell$. □

**Lemma 4.21.** *The integer $\beta_M$ is nonzero for all $M \in \mathcal{M}$.*

*Proof.* Suppose that there is a set $M \in \mathcal{M}$ such that $\beta_M = 0$. We thus have $\prod_i \pi_i^{m_i} = 1$ for all $m \in M$. Therefore, the subgroup $\Phi_{A,\mathfrak{q}}$ of $\overline{\mathbb{Q}}^\times$ generated by $\pi_1, \dots, \pi_{2g}$ is an abelian group of rank at most $2g - \operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}M)$. By our definition of $\mathcal{M}$, $\Phi_{A,\mathfrak{q}}$ has rank strictly less than $r$. This is a contradiction since $\Phi_{A,\mathfrak{q}}$ has rank $r$ by our initial choice of $\mathfrak{q}$. Therefore, $\beta_M$ is nonzero for all $M \in \mathcal{M}$. □

From Weil, we know that each $\pi_i$ has complex absolute value $N(\mathfrak{q})^{1/2}$ under any embedding $F \subseteq \mathbb{C}$. We can bound $[F : \mathbb{Q}]$ in terms of $g$, so there are positive constants $c'$ and $\gamma'$, depending only on $g$, such that

$$|\beta_M| < c' N(\mathfrak{q})^{\gamma'}$$

for all $M \in \mathcal{M}$. We may thus assume that $c$ and $\gamma$ are taken so that $|\beta_M| < cN(\mathfrak{q})^\gamma$ holds for all $M \in \mathcal{M}$.

Now suppose that $\operatorname{rank}(H_{A,\ell}) < r$. By Lemmas 4.20 and 4.21, we have $\ell \le |\beta_M|$ for some $M \in \mathcal{M}$. Therefore, $\ell < cN(\mathfrak{q})^\gamma$. However, this contradicts $\ell \ge c \cdot \max(\{[K : \mathbb{Q}], h(A), N(\mathfrak{q})\})^\gamma \ge cN(\mathfrak{q})^\gamma$, so we must have $\operatorname{rank}(H_{A,\ell}) = r$.

4.6. **The derived subgroup of $\mathcal{G}_{A,\ell}$.** We have already proved that the $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell}$ is reductive. Let $\mathcal{S}_{A,\ell}$ be the derived subgroup of $\mathcal{G}_{A,\ell}$; it is semisimple group scheme over $\mathbb{Z}_\ell$.

By Theorem 4.5, there is a subgroup $\Gamma$ of $\mathrm{GL}_{A[\ell]}(\mathbb{F}_\ell)$ that acts semisimply on $A[\ell]$ such that $\mathbf{G}_\Gamma = (\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$, where $\mathbf{G}_\Gamma$ is defined as in §3.1. By Theorem 3.1, we have $\Gamma^+ = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$. Since $\Gamma^+$ is a normal subgroup of $\Gamma$, we find that $\Gamma^+$ acts semisimply on $A[\ell]$ by Clifford's theorem [CR81, 11.1]. We have $\mathbf{G}_\Gamma = \mathbf{G}_{\Gamma^+}$, so we may take $\Gamma := \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$.

**Lemma 4.22.**

(i) *Every simple quotient of $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ is a finite simple group of Lie type in characteristic $\ell$. In particular, $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ is perfect.*

(ii) *The quotient group $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)/\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ is abelian and its cardinality can be bounded in terms of $g$.*

(iii) *The group $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ is the commutator subgroup of $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$.*

*Proof.* Let $G$ be a finite simple quotient of $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$. By increasing $c$, we may assume that $\ell > J(2g)$ with $J(2g)$ as in Theorem 3.5. The group $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$, and hence also $G$, is generated by elements of order $\ell$, so Theorem 3.5 implies that $G$ is either a finite (nonabelian) simple group of Lie type in characteristic $\ell$ or a cyclic group of order $\ell$.

Suppose that $G$ is a cyclic group of order $\ell$. Theorem 3.5 implies that $\Gamma = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ contains a normal subgroup $U \ne 1$ that is an $\ell$-group. So $U$ is a unipotent subgroup of $\mathrm{GL}_{A[\ell]}(\mathbb{F}_\ell)$. Since $U$ is a normal subgroup of $\Gamma$, we find that $U$ acts semisimply on $A[\ell]$ by Clifford's theorem [CR81, 11.1]. Since the action of $U$ on $A[\ell]$ is unipotent and semisimple, we must have $U = 1$. This contradiction proves part (i).

Since $(\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$ is of the form $\mathbf{G}_\Gamma$, part (ii) follows from statement 3.6(v) of [Nor87].

From (ii), we find that $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)' \subseteq \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ and that $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+/\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ is abelian. Since $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ has no abelian quotients by (i), we deduce that $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+ = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$. This proves (iii). □

Let $\mathcal{B}$ be the inverse image of $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ under the reduction modulo $\ell$ map $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell) \to \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$.

**Lemma 4.23.** *Let $H$ be a closed subgroup of $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)$ whose image in $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$ contains $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$. Then $H \supseteq \mathcal{B}$.*

*Proof.* Without loss of generality, we may assume that the image of $H$ in $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$ is $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+ = \Gamma$. We have $\mathbf{G}_\Gamma = (\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$, so $\mathrm{Ndim}(H) = \dim(\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$.

Let $S$ be the Zariski closure of $H$ in $G_{A,\ell}$. We have $S \subseteq (\mathcal{S}_{A,\ell})_{\mathbb{Q}_\ell}$. By Theorem 3.4(i), we have $\mathrm{Ndim}(H) \leq \dim S \leq \dim(\mathcal{S}_{A,\ell})_{\mathbb{Q}_\ell}$. So we have

$$\mathrm{Ndim}(H) \leq \dim S \leq \dim(\mathcal{S}_{A,\ell})_{\mathbb{Q}_\ell} = \dim(\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell} = \mathrm{Ndim}(H).$$

Therefore, $\dim S = \dim(\mathcal{S}_{A,\ell})_{\mathbb{Q}_\ell}$ and hence $S = (\mathcal{S}_{A,\ell})_{\mathbb{Q}_\ell}$ since $(\mathcal{S}_{A,\ell})_{\mathbb{Q}_\ell}$ is connected. In particular, $S$ is connected and semisimple. Applying Theorem 3.4(ii), we find that

$$[S(\mathbb{Q}_\ell) \cap \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : H] \leq c_4(2g).$$

After possibly increasing $c$, we may assume that $\ell > c_4(2g)$ and thus $[\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell) : H] < \ell$. Therefore, $H$ contains the pro-$\ell$ group that is the kernel of the reduction map $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell) \to \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$. It is now clear that $H$ is equal to $\mathcal{B}$. □

**Lemma 4.24.** *The group $\mathcal{B}$ is perfect and is equal to $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$.*

*Proof.* Let $H$ be the group $\mathcal{B}'$ or $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$. By Lemma 4.22, we find that the image of $H$ in $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$ is $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$. Therefore, $H = \mathcal{B}$ by Lemma 4.23. This proves the lemma. □

We now summarize some important properties of the groups $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)$.

**Proposition 4.25.**

(i) *The group $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ agrees with the inverse image of $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ under the reduction modulo $\ell$ homomorphism $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell) \to \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$.*
(ii) *The groups $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ and $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ are perfect.*
(iii) *The cardinality of the group $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)/\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)' \cong \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)/\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ can be bounded in terms of $g$.*
(iv) *The finite simple quotients of $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ are groups of Lie type in characteristic $\ell$.*
(v) *We have $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)' = \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$.*

*Proof.* By Lemma 4.22, $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$ is perfect and equals $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$. Parts (i) and (ii) are immediate consequences of Lemma 4.24. Since $\mathcal{S}_{A,\ell}$ is smooth, the reduction modulo $\ell$ map $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell) \to \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$ is surjective; part (iii) now follows from part (i) and Lemma 4.22(ii).

Let $G$ be a finite simple quotient of $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$; it is nonabelian since $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ is perfect. The kernel of the reduction modulo $\ell$ map $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)' \twoheadrightarrow \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$ is a pro-$\ell$ group. Since pro-$\ell$ groups are prosolvable, we find that $G$ must be a quotient of $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$. By Lemma 4.22(i), the group $G$ is a finite simple group of Lie type in characteristic $\ell$.

Define $H := \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)'$; it is a closed subgroup of $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)$. With $G := (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$, the quotient $G(\mathbb{F}_\ell)/G(\mathbb{F}_\ell)^+$ is abelian by [Pet16, Proposition 1.1]. This implies that $H$ modulo $\ell$ is a subgroup of $\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)^+ = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$. Since $H \supseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$, we find by Lemma 4.24 that $H$ modulo $\ell$ contains the group $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$. Therefore, $H = \mathcal{B}$. By Lemma 4.24, we deduce that $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)' = \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$. □

*Remark* 4.26. There is an alternate description of the commutator subgroups of $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)$ and $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$. Let $\pi\colon \mathcal{S}^{\mathrm{sc}}_{A,\ell} \to \mathcal{S}_{A,\ell}$ be the simply connected cover of $\mathcal{S}_{A,\ell}$. We have $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)' = \pi(\mathcal{S}^{\mathrm{sc}}_{A,\ell}(\mathbb{Z}_\ell))$ and $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)' = \pi(\mathcal{S}^{\mathrm{sc}}_{A,\ell}(\mathbb{F}_\ell))$; as noted in §1.2 of [Win02], $\pi(\mathcal{S}^{\mathrm{sc}}_{A,\ell}(\mathbb{F}_\ell))$ is the commutator subgroup of $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)$ and $\pi(\mathcal{S}^{\mathrm{sc}}_{A,\ell}(\mathbb{Z}_\ell))$ is the subgroup of $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)$ whose reduction modulo $\ell$ lies in $\pi(\mathcal{S}^{\mathrm{sc}}_{A,\ell}(\mathbb{F}_\ell))$.

4.7. **Proof of Theorem 1.2(d).** With $\Gamma := \bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$, we have $\mathbf{G}_\Gamma = (\mathcal{S}_{A,\ell})_{\mathbb{F}_\ell}$ by Theorem 4.5. By Theorem 3.1, we have $\Gamma^+ = \mathbf{G}_\Gamma(\mathbb{F}_\ell)^+ = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ and hence $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ is a subgroup of $\Gamma = \bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$.

Since $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$ is perfect by Lemma 4.22(i), we have $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+ \subseteq \bar{\rho}_{A,\ell}(\mathrm{Gal}_K)'$. Therefore, $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)' \subseteq \mathcal{G}_{A,\ell}(\mathbb{F}_\ell)' = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)'$, where the last equality follows from Lemma 4.25(v). By Lemma 4.22(iii), we deduce that

$$\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)' = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)' = \mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+.$$

So $\rho_{A,\ell}(\mathrm{Gal}_K)'$ is a closed subgroup of $\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)$ whose reduction modulo $\ell$ is equal to $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell)^+$. By Lemmas 4.23 and 4.24, we have $\rho_{A,\ell}(\mathrm{Gal}_K)' = \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$. Therefore, $\rho_{A,\ell}(\mathrm{Gal}_K)' = \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)'$ by Lemma 4.25(v).

## 5. Abelian representations

Fix an abelian variety $A$ of dimension $g \geq 1$ defined over a number field $K$. Assume that all the $\ell$-adic monodromy groups $G_{A,\ell}$ are connected; equivalently, $K_A^{\mathrm{conn}} = K$.

Fix an isogeny

$$\iota\colon A \to \prod_{i=1}^{s} A_i,$$

where $A_i = B_i^{e_i}$ with $e_i \geq 1$ and the $B_i$ are simple abelian varieties over $K$ that are pairwise non-isogenous. By Proposition 2.3(iv), each $B_i$ is geometrically simple and they are pairwise non-isogenous. The isogeny $\iota$ induces an isomorphism $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} = \prod_{i=1}^{s} \mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Q}$. Note that none of the results of this section will depend on the choice of $\iota$.

Let $L$ be the center of $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$. Let $L_i$ be the center of $\mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Q}$; we can also identify it with the center of $\mathrm{End}(B_i) \otimes_{\mathbb{Z}} \mathbb{Q}$. We have $L = \prod_{i=1}^{s} L_i$ and each $L_i$ is a number field.

Let $T_L$ be the torus defined over $\mathbb{Q}$ for which $T_L(R) = (L \otimes_{\mathbb{Q}} R)^\times$ for any $\mathbb{Q}$-algebra $R$ with the obvious functoriality. We have $T_L = \prod_{i=1}^{s} T_{L_i}$, where $T_{L_i}$ is equal to the restriction of scalars $\mathrm{Res}_{L_i/\mathbb{Q}}(\mathbb{G}_{m,L_i})$.

5.1. **The homomorphism $\beta_{A,\ell}$.** Take any prime $\ell$. The isogeny $\iota$ induces an isomorphism $V_\ell(A) = \oplus_{i=1}^{s} V_\ell(A_i)$ of $\mathbb{Q}_\ell[\mathrm{Gal}_K]$-modules. Note that each $V_\ell(A_i)$ is a free $L_i \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module of rank $d_i := 2 \dim A_i / [L_i : \mathbb{Q}]$, cf. [Rib76, II Theorem 2.1.1]. Since the $\mathrm{Gal}_K$ and $L$ actions on $V_\ell(A)$ commute, we have

$$\rho_{A,\ell}(\mathrm{Gal}_K) \subseteq \mathrm{Aut}_{L \otimes_{\mathbb{Q}} \mathbb{Q}_\ell}(V_\ell(A)) = \prod_{i=1}^{s} \mathrm{Aut}_{L_i \otimes_{\mathbb{Q}} \mathbb{Q}_\ell}(V_\ell(A_i)) \cong \prod_{i=1}^{s} \mathrm{GL}_{d_i}(L_i \otimes_{\mathbb{Q}} \mathbb{Q}_\ell).$$

By taking determinants, we obtain from $\rho_{A,\ell}$ a homomorphism

$$\beta_{A,\ell}\colon \mathrm{Gal}_K \to \prod_{i=1}^{s} (L_i \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^\times = \prod_{i=1}^{s} T_{L_i}(\mathbb{Q}_\ell) = T_L(\mathbb{Q}_\ell).$$

Using $\prod_{i=1}^{s} T_{L_i} = T_L$, we clearly have $\prod_{i=1}^{s} \beta_{A_i,\ell} = \beta_{A,\ell}$. The homomorphism $\beta_{A,\ell}\colon \mathrm{Gal}_K \to T_L(\mathbb{Q}_\ell)$ is unramified at all non-zero prime ideals $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_K$ for which $A$ has good reduction since $\rho_{A,\ell}$ has this property.

**Lemma 5.1.** *There is a field extension $F/K$ with $[F : K] \ll_g 1$ such that for all primes $\ell$, the homomorphism $\beta_{A,\ell}|_{\mathrm{Gal}_F}\colon \mathrm{Gal}_F \to T_L(\mathbb{Q}_\ell)$ is unramified at all non-zero prime ideals $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_F$.*

*Proof.* Define the number field $F = K(A[12])$; we have $[F : K] \leq 12^{(2g)^2} \ll_g 1$. By a criterion of Raynaud (see Proposition 4.7 of [SGA7 I, Expose IX]), the abelian variety $A_F$ has semistable reduction at all non-zero prime ideals of $\mathcal{O}_F$.

Take any prime $\ell$. Take any non-zero prime ideal $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_F$ and denote by $I_\mathfrak{p}$ an inertia subgroup of $\mathrm{Gal}_F$ at $\mathfrak{p}$. Since $A$ has semistable reduction at $\mathfrak{p}$, we know from Grothendieck (Proposition 3.5 of [SGA7 I, Expose IX]) that the group $\rho_{A,\ell}(I_\mathfrak{p})$ consists of unipotent elements in $\mathrm{GL}_{V_\ell}(\mathbb{Q}_\ell)$. Since $T_L$ is a torus, we deduce that $\beta_{A,\ell}(I_\mathfrak{p}) = 1$. Therefore, $\beta_{A,\ell}|_{\mathrm{Gal}_F}$ is unramified at $\mathfrak{p}$. □

5.2. **The torus $Y$.** Fix notation as in §2.6 and let $V_i$ be the homology group of $A_i$. The isogeny $\iota$ induces an isomorphism $V = \oplus_{i=1}^{s} V_i$. Since $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ acts faithfully on $V$, we have a faithful action of $T_L$ on $V$ and we may thus identify $T_L$ with an algebraic subgroup of $\mathrm{GL}_V$.

Let $\mathscr{G}$ be the algebraic subgroup of $\mathrm{GL}_V$ over $\mathbb{Q}$ that satisfies

$$\mathscr{G}(R) = \prod_{i=1}^{s} \mathrm{Aut}_{L_i \otimes_{\mathbb{Q}} R}(V_i \otimes_{\mathbb{Q}} R)$$

for any $\mathbb{Q}$-algebra $R$ with the obvious functoriality. Since $V = \oplus_{i=1}^{s} V_i$, we find that $T_L \subseteq \mathscr{G} \subseteq \mathrm{GL}_V$. The $L_i$-vector space $V_i$ has dimension $d_i = 2 \dim A_i / [L_i : \mathbb{Q}]$. We define

$$\det{}_L\colon \mathscr{G} \to T_L$$

to be the homomorphism that for each $\mathbb{Q}$-algebra $R$ takes $(g_1, \dots, g_s) \in \mathscr{G}(R) \cong \prod_{i=1}^{s} \mathrm{GL}_{d_i}(L_i \otimes_{\mathbb{Q}} R)$ to $(\det g_1, \dots, \det g_s) \in \prod_{i=1}^{s} (L_i \otimes_{\mathbb{Q}} R)^\times = (L \otimes_{\mathbb{Q}} R)^\times = T_L(R)$. In particular, $\det_L$ gives an isogeny $T_L \to T_L$ of tori of degree $d_1 \cdots d_s$.

Observe that $\mathrm{MT}_A \subseteq \mathcal{G}$ since the Mumford–Tate group $\mathrm{MT}_A$ commutes with the action of $L$ on $V$. Let $C_A$ be the central torus of the reductive group $\mathrm{MT}_A$. One knows that the commutant of $\mathrm{MT}_A$ in $\mathrm{End}_{\mathbb{Q}}(V)$ is

naturally isomorphic to $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$. We have $C_A \subseteq T_L$ since $C_A$ commutes with $\mathrm{MT}_A$ and $\mathrm{End}(A)\otimes_{\mathbb{Z}}\mathbb{Q}$. Define the algebraic group

$$Y := \det_L(C_A);$$

it is a subtorus of $T_L$ defined over $\mathbb{Q}$. Observe that $\det_L|_{C_A}\colon C_A \to Y$ is an isogeny of degree at most $d_1\cdots d_s$. For later, note that $d_1\cdots d_s \ll_g 1$.

The following gives some important information on the image of $\beta_{A,\ell}$.

**Proposition 5.2.** *We have $\beta_{A,\ell}(\mathrm{Gal}_K) \subseteq Y(\mathbb{Q}_\ell)$. Moreover, $\beta_{A,\ell}(\mathrm{Gal}_K)$ is Zariski dense in $Y_{\mathbb{Q}_\ell}$ and $\det_L(G_{A,\ell}) = Y_{\mathbb{Q}_\ell}$.*

*Proof.* Using comparison isomorphisms, we have

$$\mathscr{G}(\mathbb{Q}_\ell) = \prod_{i=1}^{s} \mathrm{Aut}_{L_i\otimes_{\mathbb{Q}}\mathbb{Q}_\ell}(V_\ell(A_i)) = \mathrm{Aut}_{L\otimes_{\mathbb{Q}}\mathbb{Q}_\ell}(V_\ell(A))$$

and hence $\rho_{A,\ell}(\mathrm{Gal}_K) \subseteq \mathscr{G}(\mathbb{Q}_\ell)$. In particular, $G_{A,\ell} \subseteq \mathscr{G}_{\mathbb{Q}_\ell}$. The homomorphism

$$\beta_{A,\ell}\colon \mathrm{Gal}_K \to T_L(\mathbb{Q}_\ell)$$

can be obtained by composing $\rho_{A,\ell}\colon \mathrm{Gal}_K \to \mathscr{G}(\mathbb{Q}_\ell)$ with $\det_L\colon \mathscr{G}(\mathbb{Q}_\ell) \to T_L(\mathbb{Q}_\ell)$.

We have $\beta_{A,\ell}(\mathrm{Gal}_K) = \det_L(\rho_{A,\ell}(\mathrm{Gal}_K)) \subseteq \det_L(G_{A,\ell}(\mathbb{Q}_\ell))$. By Proposition 2.11, we have $\beta_{A,\ell}(\mathrm{Gal}_K) \subseteq \det_L(\mathrm{MT}_A(\mathbb{Q}_\ell))$. Since $\mathrm{MT}_A$ is reductive and $T_L$ is a torus, we have $\det_L(\mathrm{MT}_A) = \det_L(C_A) = Y$. Therefore, $\beta_{A,\ell}(\mathrm{Gal}_K) \subseteq Y(\mathbb{Q}_\ell)$.

By Proposition 2.12, $(C_A)_{\mathbb{Q}_\ell}$ is the central torus of the reductive group $G_{A,\ell}$. Since $G_{A,\ell}$ is reductive, we have $\det_L(G_{A,\ell}) = \det_L((C_A)_{\mathbb{Q}_\ell}) = Y_{\mathbb{Q}_\ell}$. Since $\rho_{A,\ell}(\mathrm{Gal}_K)$ is Zariski dense in $G_{A,\ell}$, we deduce that $\beta_{A,\ell}(\mathrm{Gal}_K) = \det_L(\rho_{A,\ell}(\mathrm{Gal}_K))$ is Zariski dense in $Y_{\mathbb{Q}_\ell}$. □

Since $\beta_{A,\ell}$ is continuous and $\mathrm{Gal}_K$ is compact, we have $\beta_{A,\ell}(\mathrm{Gal}_K) \subseteq Y(\mathbb{Q}_\ell)_c$, where $Y(\mathbb{Q}_\ell)_c$ is the maximal compact subgroup of $Y(\mathbb{Q}_\ell)$ with respect to the $\ell$-adic topology. That $Y(\mathbb{Q}_\ell)$ has a unique maximal compact subgroup uses that $Y(\mathbb{Q}_\ell)$ is abelian. The following theorem, which we will prove in §5.6, is the main result of §5.

**Theorem 5.3.**

(i) *For any prime $\ell$, we have $[Y(\mathbb{Q}_\ell)_c : \beta_{A,\ell}(\mathrm{Gal}_K)] \ll_{g,[K:\mathbb{Q}]} 1$.*
(ii) *For any prime $\ell$ that is unramified in $K$, we have $[Y(\mathbb{Q}_\ell)_c : \beta_{A,\ell}(\mathrm{Gal}_K)] \ll_g 1$.*

5.3. **$\lambda$-adic representations.** Throughout §5.3, we shall further assume that $A$ is a power of a simple abelian variety and hence $L$ is a number field.

We have $L_\ell := L\otimes_{\mathbb{Q}}\mathbb{Q}_\ell = \prod_{\lambda|\ell} L_\lambda$, where $\lambda$ runs over the prime ideals of $\mathcal{O}_L$ dividing $\ell$ and $L_\lambda$ is the $\lambda$-adic completion of $L$. For each $\lambda$, define $V_\lambda(A) := V_\ell(A)\otimes_{L_\ell} L_\lambda$; it is a $L_\lambda$-vector space of dimension $d = 2g/[L:\mathbb{Q}]$. We have an isomorphism $V_\ell(A) = \oplus_{\lambda|\ell} V_\lambda(A)$ of $\mathbb{Q}_\ell[\mathrm{Gal}_K]$-algebras. The Galois action on $V_\lambda(A)$ gives a representation

$$\rho_{A,\lambda}\colon \mathrm{Gal}_K \to \mathrm{Aut}_{L_\lambda}(V_\lambda(A)) \cong \mathrm{GL}_d(L_\lambda).$$

By composing $\rho_{A,\lambda}$ with the determinant map, we obtain a homomorphism

$$\beta_{A,\lambda}\colon \mathrm{Gal}_K \to L_\lambda^\times.$$

Using $T_L(\mathbb{Q}_\ell) = (L\otimes_{\mathbb{Q}}\mathbb{Q}_\ell)^\times = \prod_{\lambda|\ell} L_\lambda^\times$, we find that $\beta_{A,\ell} = \prod_{\lambda|\ell}\beta_{A,\lambda}$.

**Lemma 5.4.** *Take any non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ for which $A$ has good reduction. Then there is an element $F_\mathfrak{p} \in L^\times$ such that $\beta_{A,\lambda}$ is unramified at $\mathfrak{p}$ and satisfies*

$$\beta_{A,\lambda}(\mathrm{Frob}_\mathfrak{p}) = F_\mathfrak{p}$$

*for all non-zero prime ideals $\lambda$ of $\mathcal{O}_F$ that do not divide the characteristic of $\mathbb{F}_\mathfrak{p}$.*

*Proof.* Let $\lambda$ be a non-zero prime ideal of $\mathcal{O}_F$ that does not divide the characteristic of $\mathbb{F}_\mathfrak{p}$. Theorem 2.1.1 of [Rib76, II §1] says that there is a polynomial $Q_\mathfrak{p}(x) \in L[x]$ such that $\det(xI - \rho_{A,\lambda}(\mathrm{Frob}_\mathfrak{p})) = Q_\mathfrak{p}(x)$; the polynomial $Q_\mathfrak{p}(x)$ does not depend on the choice of $\lambda$. Therefore, $\beta_{A,\lambda}(\mathrm{Frob}_\mathfrak{p}) = \det(\rho_{A,\lambda}(\mathrm{Frob}_\mathfrak{p})) = (-1)^d Q_\mathfrak{p}(0)$ which is an element of $L^\times$ that does not depend on $\lambda$. □

For each prime $\ell$, let $\chi_\ell\colon \mathrm{Gal}_K \to \mathbb{Z}_\ell^\times$ be the $\ell$-adic cyclotomic character; we have $\sigma(\zeta) = \zeta^{\chi_\ell(\sigma) \bmod \ell^n}$ for any $\ell^n$-th root of unity $\zeta \in \overline{K}$ and $\sigma \in \mathrm{Gal}_K$. Reducing modulo $\ell$, we obtain a homomorphism $\overline{\chi}_\ell\colon \mathrm{Gal}_K \to \mathbb{F}_\ell^\times$.

For any non-zero prime ideal $\lambda$ of $\mathcal{O}_L$, the image of $\beta_{A,\lambda}$ is compact so it lies in $\mathcal{O}_\lambda^\times$. Reducing gives a homomorphism

$$\overline{\beta}_{A,\lambda}\colon \mathrm{Gal}_K \to \mathbb{F}_\lambda^\times.$$

**Lemma 5.5.** *Fix a prime $\ell \geq 5$ that splits completely in $L$ and is unramified in $K$ and let $\lambda$ be a prime ideal of $\mathcal{O}_L$ dividing $\ell$. Let $\mathfrak{p}|\ell$ be a prime ideal of $\mathcal{O}_K$ for which $A$ has good reduction at $\mathfrak{p}$ and let $I_\mathfrak{p}$ be an inertia subgroup of $\mathrm{Gal}_K$ for the prime $\mathfrak{p}$. Then there is an integer $0 \leq b \leq 2g/[L:\mathbb{Q}]$ such that $\overline{\beta}_{A,\lambda}(\sigma) = \overline{\chi}_\ell(\sigma)^b$ holds for all $\sigma \in I_\mathfrak{p}$.*

*Proof.* Since $\ell$ splits completely in $L$, we have $\mathbb{F}_\lambda = \mathbb{F}_\ell$ and hence $\overline{\beta}_{A,\lambda}\colon \mathrm{Gal}_K \to \mathbb{F}_\lambda^\times = \mathbb{F}_\ell^\times$.

There is a $\mathcal{O}_\lambda$-submodule $M$ of $V_\lambda(A)$ of rank $\dim_{L_\lambda} V_\lambda(A)$ that is stable under the action of $I_\mathfrak{p}$. Let $W$ be the semi-simplification of $M/\lambda M$ as a module over $\mathbb{F}_\lambda[I_\mathfrak{p}] = \mathbb{F}_\ell[I_\mathfrak{p}]$. The character $\overline{\beta}_{A,\lambda}|_{I_\mathfrak{p}}$ thus arises by taking the determinant of the action of $I_\mathfrak{p}$ on the vector space $W$ over $\mathbb{F}_\lambda = \mathbb{F}_\ell$.

Take any irreducible $\mathbb{F}_\ell[I_\mathfrak{p}]$-submodule $\mathcal{V}$ of $W$ and set $n = \dim_{\mathbb{F}_\ell} \mathcal{V}$. Let $Z$ be the ring of endomorphisms of $\mathcal{V}$ as an $\mathbb{F}_\ell[I_\mathfrak{p}]$-module. Since $\mathcal{V}$ is irreducible, $Z$ is a division algebra of finite dimension over $\mathbb{F}_\ell$. Therefore, $Z$ is a finite field and $\mathcal{V}$ is a vector space of dimension 1 over $Z$. Choose an isomorphism $Z \cong \mathbb{F}_{\ell^n}$ of fields. The action of $I_\mathfrak{p}$ on $\mathcal{V}$ corresponds to a character $\alpha\colon I_\mathfrak{p} \to Z^\times \cong \mathbb{F}_{\ell^n}^\times$. Let $\varepsilon_1, \ldots, \varepsilon_n\colon I_\mathfrak{p} \to \mathbb{F}_{\ell^n}^\times$ be the fundamental character of level $n$, cf. [Ser72, §1.7]. There are unique integers $e_i \in \{0, 1, \ldots, \ell-1\}$ such that $\alpha = \varepsilon_1^{e_1} \cdots \varepsilon_n^{e_n}$. These integers $e_1, \ldots, e_n$ are called the tame inertia weights of $\mathcal{V}$.

Note that $\mathcal{V}$ will arise in the semi-simplification of $A[\ell]$ as an $\mathbb{F}_\ell[I_\mathfrak{p}]$-module since $V_\lambda(A) \subseteq V_\ell(A)$. From [Car08, Théorème 1.2], we find that all of the integers $e_i$ are either 0 or 1 (this uses that $A[\ell]$ is isomorphic as an $\mathbb{F}_\ell[\mathrm{Gal}_K]$-module to the dual of $H^1_{\text{ét}}(A_{\overline{K}}, \mathbb{Z}/\ell\mathbb{Z})$ and the conditions on $\ell$ and $\mathfrak{p}$ in the statement of the lemma).

Take any $\sigma \in I_\mathfrak{p}$. The determinant of $\varepsilon_i(\sigma) \in \mathbb{F}_{\ell^n}^\times \subseteq \mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^n})$ is equal to $N_{\mathbb{F}_{\ell^n}/\mathbb{F}_\ell}(\varepsilon_i(\sigma)) = \overline{\chi}_\ell(\sigma)$, where the last equality uses Proposition 8 of [Ser72]. Viewing $\alpha(\sigma)$ as an endomorphism of $\mathcal{V}$, we thus have $\det(\alpha(\sigma)) = \overline{\chi}_\ell(\sigma)^{e_1+\cdots+e_n}$. Since $e_i \in \{0,1\}$, there is an integer $0 \leq b \leq \dim_{\mathbb{F}_\ell} \mathcal{V}$ such that $\det(\sigma|\mathcal{V}) = \det(\alpha(\sigma)) = \overline{\chi}_\ell(\sigma)^b$ for all $\sigma \in I_\mathfrak{p}$.

Therefore, there is an integer $0 \leq b \leq \dim_{\mathbb{F}_\ell} W = \dim V_\lambda(A) = 2g/[L:\mathbb{Q}]$ such that $\overline{\beta}_{A,\lambda}(\sigma) = \overline{\chi}_\ell(\sigma)^b$ for all $\sigma \in I_\mathfrak{p}$. □

5.4. **Serre tori.** We now recall the families of compatible abelian Galois representations described by Serre in Chapter II of [Ser98]; for statements generalized to $\lambda$-adic representations see section I of [Rib76]. In Lemma 5.6, we will see how these representations give rise to our $\beta_{A,\ell}$.

Define the torus

$$T_K := \mathrm{Res}_{K/\mathbb{Q}}(\mathbb{G}_{m,K}),$$

where we are taking restriction of scalars from $K$ to $\mathbb{Q}$. Let $I_K$ be the group of ideles of $K$.

Fix a *modulus* $\mathfrak{m}$, i.e., a sequence $\{\mathfrak{m}_v\}_v$ of non-negative integers indexed by the places $v$ of $K$ satisfying $\mathfrak{m}_v = 0$ for all but finitely many places $v$. For a finite place $v$ with $\mathfrak{m}_v = 0$, we define $U_{v,\mathfrak{m}} = \mathcal{O}_v^\times$. For a finite place $v$ with $\mathfrak{m}_v > 0$, we define $U_{v,\mathfrak{m}}$ to be the subgroup of $x \in \mathcal{O}_v^\times$ for which the $v$-adic valuation of $1-x$ is at least $\mathfrak{m}_v$. For an infinite place $v$, let $U_{v,\mathfrak{m}}$ be the connected component of $K_v^\times$ containing the identity if $\mathfrak{m}_v \geq 1$ and $K_v^\times$ otherwise. Define $U_\mathfrak{m} := \prod_v U_{v,\mathfrak{m}}$; it is an open subgroup of $I_K$. Set $I_\mathfrak{m} := I_K/U_\mathfrak{m}$.

Let $E_\mathfrak{m}$ be the group of $x \in K^\times$ for which $x \in U_\mathfrak{m}$. We let $T_\mathfrak{m}$ be the quotient of $T_K$ by the Zariski closure of $E_\mathfrak{m} \subseteq K^\times = T_K(\mathbb{Q})$. In [Ser98, II], Serre constructs a commutative algebraic group $S_\mathfrak{m}$ over $\mathbb{Q}$ whose neutral component is $T_\mathfrak{m}$ and for which the quotient $S_\mathfrak{m}/T_\mathfrak{m}$ equals the finite group $C_\mathfrak{m} := I_K/(I_\mathfrak{m} K^\times)$. He also constructs a homomorphism

$$\varepsilon\colon I_\mathfrak{m} \to S_\mathfrak{m}(\mathbb{Q})$$

for which we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times/E_\mathfrak{m} & \longrightarrow & I_\mathfrak{m} & \longrightarrow & C_\mathfrak{m} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \varepsilon} & & \| & & \\ 1 & \longrightarrow & T_\mathfrak{m}(\mathbb{Q}) & \longrightarrow & S_\mathfrak{m}(\mathbb{Q}) & \longrightarrow & C_\mathfrak{m} & \longrightarrow & 1. \end{array}$$

They are characterized by the following universal property: for any field extension $k/\mathbb{Q}$, homomorphism $f'\colon T_{\mathfrak{m},k} \to A$ of commutative algebraic groups over $k$ and homomorphism $\varepsilon'\colon I_\mathfrak{m} \to A(k)$ such that the following diagram commutes

$$\begin{array}{ccc} K^\times/E_\mathfrak{m} & \longrightarrow & I_\mathfrak{m} \\ \downarrow & & \downarrow{\scriptstyle \varepsilon'} \\ T_\mathfrak{m}(k) & \xrightarrow{f'} & A(k), \end{array}$$

there is a unique homomorphism $g\colon S_{\mathfrak{m},k} \to A$ which induces $f'$ and $\varepsilon'$ (i.e., $f'$ is obtained by composing $T_\mathfrak{m} \hookrightarrow S_\mathfrak{m}$ and $g$ and $\varepsilon'$ is obtained by composing $\varepsilon$ with $S_\mathfrak{m}(\mathbb{Q}) \hookrightarrow S_\mathfrak{m}(k) \xrightarrow{g} A(k)$).

Take any prime $\ell$. Let $\alpha_\ell\colon I_K \to S_\mathfrak{m}(\mathbb{Q}_\ell)$ be the homomorphism obtained by composing the natural projection $I_K \to \prod_{v|\ell} K_v^\times = (K \otimes_\mathbb{Q} \mathbb{Q}_\ell)^\times = T_K(\mathbb{Q}_\ell)$ with the homomorphism $T_K(\mathbb{Q}_\ell) \to S_\mathfrak{m}(\mathbb{Q}_\ell)$. Composing the quotient map $I_K \to I_\mathfrak{m}$ with $\varepsilon$ gives a homomorphism $I_K \to S_\mathfrak{m}(\mathbb{Q})$ that we shall also denote by $\varepsilon$. For all $x \in K^\times$, we have $\alpha_\ell(x) = \varepsilon(x)$, cf. [Ser98, II 2.3]. We thus have a continuous homomorphism

$$\varepsilon_\ell\colon I_K \to S_\mathfrak{m}(\mathbb{Q}_\ell), \quad x \mapsto \varepsilon(x)\alpha_\ell(x)^{-1}$$

that vanishes on $K^\times$. We shall also denote by

$$\varepsilon_\ell\colon \mathrm{Gal}_K \to S_\mathfrak{m}(\mathbb{Q}_\ell)$$

the homomorphism arising from $\varepsilon_\ell$ via class field theory.

We now observe that the homomorphisms $\varepsilon_\ell$ are compatible. Take any non-zero prime $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_K$ such that $\mathfrak{m}_v = 0$, where $v$ is the corresponding place. Let $\pi_\mathfrak{p}$ be an element of $I_K$ that is a uniformizer at the place $v$ and is 1 at the other places. Therefore,

$$\varepsilon_\ell(\mathrm{Frob}_\mathfrak{p}) = \varepsilon_\ell(\pi_\mathfrak{p}) = \varepsilon(\pi_\mathfrak{p})\alpha_\ell(\pi_\mathfrak{p})^{-1} = \varepsilon(\pi_\mathfrak{p});$$

this is an element of $S_\mathfrak{m}(\mathbb{Q})$ that is independent of $\ell$ and the choice of $\pi_\mathfrak{p}$.

We now show that our homomorphisms $\beta_{A,\ell}$ arise from Serre's $\varepsilon_\ell$ for some modulus $\mathfrak{m}$.

**Lemma 5.6.** *There is a modulus $\mathfrak{m}$ and a homomorphism $\phi\colon S_\mathfrak{m} \to T_L$ of algebraic groups over $\mathbb{Q}$ such that each $\beta_{A,\ell}$ is equal to the composition of $\varepsilon_\ell\colon \mathrm{Gal}_K \to S_\mathfrak{m}(\mathbb{Q}_\ell)$ with the homomorphism $S_\mathfrak{m}(\mathbb{Q}_\ell) \xrightarrow{\phi} T_L(\mathbb{Q}_\ell)$.*

*Proof.* Using $T_L = \prod_{i=1}^s T_{L_i}$ and $\beta_{A,\ell} = \prod_{i=1}^s \beta_{A_i,\ell}$, it suffices to prove the lemma for each $A_i$; we can find a common modulus $\mathfrak{m}$ by increasing the values $\mathfrak{m}_v$ appropriately. We may thus assume that $A$ is a power of a simple abelian variety and hence $L$ is a field.

Since $L$ is a number field, we have a natural isomorphism $L \otimes_\mathbb{Q} \mathbb{Q}_\ell = \prod_{\lambda|\ell} L_\lambda$, where the product is over the non-zero prime ideals of $\mathcal{O}_L$ that divide $\ell$. We have a homomorphism

$$\beta_{A,\ell}\colon \mathrm{Gal}_K \to T_L(\mathbb{Q}_\ell) = (L \otimes_\mathbb{Q} \mathbb{Q}_\ell)^\times = \prod\nolimits_{\lambda|\ell} L_\lambda^\times.$$

We thus have $\beta_{A,\ell} := \prod_{\lambda|\ell} \beta_{A,\lambda}$, where $\beta_{A,\lambda}\colon \mathrm{Gal}_K \to L_\lambda^\times$ is obtained by composing $\beta_{A,\ell}$ with the obvious projection. Note that these agree with the representations $\beta_{A,\lambda}$ defined in §5.3. By Lemma 5.4, for every prime $\mathfrak{p}$ for which $A$ has good reduction, there is an element $F_\mathfrak{p} \in L^\times = T(\mathbb{Q})$ such that $\beta_{A,\lambda}(\mathrm{Frob}_\mathfrak{p}) = F_\mathfrak{p}$ for all $\lambda$ that do not divide the characteristic of $\mathbb{F}_\mathfrak{p}$.

Fix a non-zero prime ideal $\lambda'$ of $\mathcal{O}_L$ and let $\ell'$ be the rational prime it divides. Théorèm 2 of [Hen82] now applies and says that $\beta_{A,\lambda'}$ is *locally algebraic*. The main theorem of section I.6 of [Rib76] then implies that

there is a modulus $\mathfrak{m}$ and a homomorphism $\psi\colon S_{\mathfrak{m},L} \to \mathbb{G}_{m,L}$ such that $\beta_{A,\lambda'}$ agrees with the composition

$$\mathrm{Gal}_K \xrightarrow{\varepsilon_{\ell'}} S_{\mathfrak{m}}(\mathbb{Q}_{\ell'}) \subseteq S_{\mathfrak{m}}(L_{\lambda'}) \xrightarrow{\psi} \mathbb{G}_m(L_{\lambda'}) = L_{\lambda'}^{\times}.$$

Now take any non-zero prime ideal $\lambda$ of $\mathcal{O}_L$ dividing a prime $\ell$. Take any non-zero prime $\mathfrak{p} \nmid \ell\ell'$ for which $A$ has good reduction. We have $\varepsilon_\ell(\mathrm{Frob}_\mathfrak{p}) = \varepsilon_{\ell'}(\mathrm{Frob}_\mathfrak{p})$ in $S_\mathfrak{m}(\mathbb{Q})$, so

$$\beta_{A,\lambda}(\mathrm{Frob}_\mathfrak{p}) = F_\mathfrak{p} = \beta_{A,\lambda'}(\mathrm{Frob}_\mathfrak{p}) = \psi(\varepsilon_{\ell'}(\mathrm{Frob}_\mathfrak{p})) = \psi(\varepsilon_\ell(\mathrm{Frob}_\mathfrak{p})).$$

By the Chebotarev density theorem, we deduce that $\beta_{A,\lambda}$ is the composition of $\varepsilon_\ell$ with the homomorphism $S_\mathfrak{m}(\mathbb{Q}_\ell) \subseteq S_\mathfrak{m}(L_\lambda) \xrightarrow{\psi} \mathbb{G}_m(L_\lambda)$. We take $\phi$ to be the composition of the natural morphism $S_\mathfrak{m} \to \mathrm{Res}_{L/\mathbb{Q}}(S_{\mathfrak{m},L})$ with the morphism $\mathrm{Res}_{L/\mathbb{Q}}(S_{\mathfrak{m},L}) \to \mathrm{Res}_{L/\mathbb{Q}}(\mathbb{G}_{m,L}) = T_L$ induced by $\psi$. Since $\beta_{A,\ell} = \prod_\lambda \beta_{A,\lambda}$, one can now check that the lemma holds with this $\phi$. □

We define

$$\varphi\colon T_K \to T_L$$

to be the homomorphism obtained by composing the quotient map $T_K \to T_\mathfrak{m}$ with the homomorphism $\phi$ in Lemma 5.6.

Take any prime $\ell$. We have $T_K(\mathbb{Q}_\ell) = (K \otimes_\mathbb{Q} \mathbb{Q}_\ell)^\times = \prod_{v|\ell} K_v^\times$ and $T_K(\mathbb{Q}_\ell)_c = \prod_{v|\ell} \mathcal{O}_v^\times$, where $T_K(\mathbb{Q}_\ell)_c$ is the maximal compact subgroup of $T_K(\mathbb{Q}_\ell)$ with respect to the $\ell$-adic topology. Let $\pi_\ell\colon T_K(\mathbb{Q}_\ell) \hookrightarrow I_K$ be the homomorphism that extends an element of $\prod_{v|\ell} K_v^\times$ to an idele by setting 1 at the places of $K$ that do not divide $\ell$. Since $\beta_{A,\ell}$ has abelian image, class field theory gives a homomorphism $I_K \to T_L(\mathbb{Q}_\ell)$ corresponding to $\beta_{A,\ell}$; we will also denote it by $\beta_{A,\ell}$.

**Proposition 5.7.** *There is an open subgroup $U \subseteq T_K(\mathbb{Q}_\ell)_c$ with $[T_K(\mathbb{Q}_\ell)_c : U] \ll_g 1$ such that*

$$\beta_{A,\ell}(\pi_\ell(u)) = \varphi(u)^{-1}$$

*holds for all $u \in U$. We can take $U = T_K(\mathbb{Q}_\ell)_c$ when $\ell$ is not divisible by any non-zero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ for which $A$ has bad reduction.*

*Proof.* Define the group $G := (\phi \circ \varepsilon)(\pi_\ell(T_K(\mathbb{Q}_\ell)_c)) \subseteq T_L(\mathbb{Q})$.

Take any prime $\ell' \neq \ell$. By Lemma 5.6, we have $\beta_{A,\ell'} = \phi \circ (\varepsilon \cdot \alpha_{\ell'}^{-1})$. We have $\alpha_{\ell'}(\pi_\ell(T_K(\mathbb{Q}_\ell)_c)) = 1$ since $\ell \neq \ell'$, so

$$\beta_{A,\ell'}(\pi_\ell(T_K(\mathbb{Q}_\ell)_c)) = (\phi \circ \varepsilon)(\pi_\ell(T_K(\mathbb{Q}_\ell)_c)) = G.$$

By class field theory, $G$ is thus the group generated by $\beta_{A,\ell'}(I_\mathfrak{p})$ where $I_\mathfrak{p}$ are inertia groups at primes $\mathfrak{p}|\ell$. By Lemma 5.1 and $\ell \neq \ell'$, we find that $G$ is finite and $|G| \leq [F : K] \ll_g 1$.

There is thus an open subgroup $U \subseteq T_K(\mathbb{Q}_\ell)_c$ with $(\phi \circ \varepsilon)(\pi_\ell(U)) = 1$ and $[T_K(\mathbb{Q}_\ell)_c : U] = |G| \ll_g 1$. For each $u \in U$, we have

$$\beta_{A,\ell}(\pi_\ell(u)) = (\phi \circ \varepsilon_\ell)(\pi_\ell(u)) = (\phi \circ \varepsilon)(\pi_\ell(u)) \cdot \phi(\alpha_\ell(\pi_\ell(u)))^{-1} = \phi(\alpha_\ell(\pi_\ell(u)))^{-1},$$

where we have used Lemma 5.6 in the first equality. The first part of the lemma follows by noting that $\phi(\alpha_\ell(\pi_\ell(u))) = \varphi(u)$ for all $u \in T_K(\mathbb{Q}_\ell)_c$.

Now suppose that $\ell$ is not divisible by any non-zero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ for which $A$ has bad reduction. Take any prime $\ell' \neq \ell$. By our choice of $\ell$, the representation $\rho_{A,\ell'}$, and hence also $\beta_{A,\ell'}$, is unramified at all primes that divide $\ell$. By class field theory, this is equivalent to having $\beta_{A,\ell'}(\pi_1(T_K(\mathbb{Q}_\ell)_c)) = 1$. From the work above, this implies that $1 = \beta_{A,\ell'}(\pi_\ell(T_K(\mathbb{Q}_\ell)_c)) = (\phi \circ \varepsilon)(\pi_\ell(T_K(\mathbb{Q}_\ell)_c)) = G$. Therefore, $U = T_K(\mathbb{Q}_\ell)_c$ since $[T_K(\mathbb{Q}_\ell)_c : U] = |G| = 1$. □

The following lemma, which we will prove in §5.5, gives some additional information on $\varphi$.

**Lemma 5.8.** *Set $d := [K : \mathbb{Q}]$ and $e := [L : \mathbb{Q}]$. There are bases $\alpha_1, \dots, \alpha_d$ of $X(T_K)$ and $\gamma_1, \dots, \gamma_e$ of $X(T_L)$ such that*

$$\gamma_j \circ \varphi = \prod_{i=1}^{d} \alpha_i^{n_{i,j}}$$

*holds for all $1 \leq j \leq e$, where $n_{i,j}$ are integers satisfying $|n_{i,j}| \leq 2g$. Moreover, the two bases are stable under the $\mathrm{Gal}_\mathbb{Q}$-actions on $X(T_K)$ and $X(T_L)$.*

**Lemma 5.9.** *Let $W$ be the kernel of $\varphi\colon T_K \to T_L$. Then $W/W^\circ$ is a finite group scheme whose cardinality can be bounded in terms of $g$.*

*Proof.* Set $d := [K : \mathbb{Q}]$ and $e := [L : \mathbb{Q}]$. Define the homomorphism $\varphi^*\colon X(T_L) \to X(T_K)$, $\gamma \mapsto \gamma \circ \varphi$. The group $X(W)$ is isomorphic to the cokernel of $\varphi^*$. The cardinality $m$ of the finite group scheme $W/W^\circ$ is equal to the cardinality of the torsion subgroup of the cokernel of $\varphi^*$.

Let $A \in M_{d,e}(\mathbb{Z})$ be a matrix that represents $\varphi^*$ with respect to the bases of $X(T_L)$ and $X(T_K)$ from Lemma 5.8. In particular, all the entries of $A$ have absolute value at most $2g$. Let $D \in M_{d,e}(\mathbb{Z})$ be the *Smith Normal Form* of $A$. There is an integer $0 \le k \le \min\{d, e\}$ such that $D_{i,j} > 0$ if $1 \le i = j \le k$ and $D_{i,j} = 0$ otherwise. Moreover, the integer $D_{i,i}$ divides $D_{i+1,i+1}$ for all $1 \le i \le k-1$. Therefore, $m = \prod_{i=1}^k D_{i,i}$.

Note that $m = \prod_{i=1}^k D_{i,i}$ is equal to the greatest common divisor of all determinants of $k \times k$ minors of $A$, cf. [MR09, Proposition 8.1]. Since the entries of $A$ are bounded in terms of $g$ and $k \le e \le 2g$, we conclude that $m \ll_g 1$. □

5.5. **Proof of Lemma 5.8.** We first assume that $L$ is a field.

For a prime $\ell$, we have an isomorphism $(T_K)_{\mathbb{Q}_\ell} = \prod_{\mathfrak{p}|\ell} \mathrm{Res}_{K_\mathfrak{p}/\mathbb{Q}_\ell}(\mathbb{G}_{m,K_\mathfrak{p}})$, where the product is over prime ideals $\mathfrak{p}|\ell$ of $\mathcal{O}_K$. Similarly, we have $(T_L)_{\mathbb{Q}_\ell} = \prod_{\lambda|\ell} \mathrm{Res}_{L_\lambda/\mathbb{Q}_\ell}(\mathbb{G}_{m,L_\lambda})$, where the product is over prime ideals $\lambda|\ell$ of $\mathcal{O}_L$.

Now fix any prime $\ell \ge 5$ that splits completely in the number fields $K$ and $L$ and is not divisible by any prime for which $A$ has bad reduction. For the rest of the proof $\mathfrak{p}$ and $\lambda$ will denote prime ideals of $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively, that divide $\ell$.

The tori $(T_K)_{\mathbb{Q}_\ell}$ and $(T_L)_{\mathbb{Q}_\ell}$ are split since $\ell$ splits completely in $K$ and $L$. In particular, we have isomorphisms $(T_K)_{\mathbb{Q}_\ell} = \prod_{\mathfrak{p}|\ell} \mathbb{G}_{m,\mathbb{Q}_\ell}$ and $(T_L)_{\mathbb{Q}_\ell} = \prod_{\lambda|\ell} \mathbb{G}_{m,\mathbb{Q}_\ell}$. Denote by $\alpha_\mathfrak{p}\colon (T_K)_{\mathbb{Q}_\ell} \to \mathbb{G}_{m,\mathbb{Q}_\ell}$ and $\gamma_\lambda\colon (T_L)_{\mathbb{Q}_\ell} \to \mathbb{G}_{m,\mathbb{Q}_\ell}$ the character obtained by projecting onto the corresponding factor. Note that $\{\alpha_\mathfrak{p}\}_{\mathfrak{p}|\ell}$ and $\{\gamma_\lambda\}_{\lambda|\ell}$ are bases of $X((T_K)_{\mathbb{Q}_\ell})$ and $X((T_L)_{\mathbb{Q}_\ell})$, respectively.

The homomorphism $\varphi\colon (T_K)_{\mathbb{Q}_\ell} \to (T_L)_{\mathbb{Q}_\ell}$ is thus of the form

$$\varphi\Big((x_\mathfrak{p})_{\mathfrak{p}|\ell}\Big) = \Big(\prod_{\mathfrak{p}|\ell} x_\mathfrak{p}^{n_{\mathfrak{p},\lambda}}\Big)_{\lambda|\ell}$$

for unique integers $n_{\mathfrak{p},\lambda}$. In particular, we have

$$\gamma_\lambda \circ \varphi = \prod_{\mathfrak{p}|\ell} \alpha_\mathfrak{p}^{n_{\mathfrak{p},\lambda}} \tag{5.1}$$

for all $\lambda|\ell$. The following lemma gives some constraints on the integers $n_{\mathfrak{p},\lambda}$.

**Lemma 5.10.** *Each integer $n_{\mathfrak{p},\lambda}$ is congruent modulo $\ell - 1$ to an integer that has absolute value at most $2g$.*

*Proof.* Take any prime ideal $\lambda|\ell$ of $\mathcal{O}_L$. We have defined a representation $\beta_{A,\lambda}\colon \mathrm{Gal}_K \to L_\lambda^\times$. The image of $\beta_{A,\lambda}$ is contained in $\mathcal{O}_\lambda$ since it is continuous and $\mathrm{Gal}_K$ is compact. By class field theory, we may view $\beta_{A,\lambda}$ as a homomorphism $I_K \to \mathcal{O}_\lambda^\times$. By Proposition 5.7 and our choice of $\ell$, we have $\beta_{A,\ell}(\pi_\ell(u)) = \varphi(u)^{-1}$ for all $u \in T_K(\mathbb{Q}_\ell)_c$. Therefore, $\beta_{A,\lambda}(\pi_\ell(u)) = \gamma_\lambda(\varphi(u)^{-1}) = \prod_{\mathfrak{p}|\ell} \alpha_\mathfrak{p}(u)^{-n_{\mathfrak{p},\lambda}}$ holds for all $u \in T_K(\mathbb{Q}_\ell)_c$.

Now fix a prime ideal $\mathfrak{p}|\ell$ of $\mathcal{O}_K$. Define the homomorphism

$$\widetilde{\beta}_{A,\lambda}\colon \mathcal{O}_\mathfrak{p}^\times \xrightarrow{i} I_K \xrightarrow{\beta_{A,\lambda}} \mathcal{O}_\lambda^\times,$$

where $i\colon \mathcal{O}_\mathfrak{p}^\times \hookrightarrow I_K$ is the inclusion on the $\mathfrak{p}$-th term of $I_K$ and 1 elsewhere. We have

$$\widetilde{\beta}_{A,\lambda}(a) = a^{-n_{p,\lambda}}$$

for all $a \in \mathcal{O}_\mathfrak{p}^\times$; note that this does makes sense because $\ell$ splits completely in $K$ and $L$ and hence $\mathcal{O}_\mathfrak{p}^\times = \mathbb{Z}_\ell^\times$ and $\mathcal{O}_\lambda^\times = \mathbb{Z}_\ell^\times$. For an inertia subgroup $I_\mathfrak{p}$ of $\mathrm{Gal}_K$ at the prime $\mathfrak{p}$, class field theory now implies that $\beta_{A,\lambda}(\sigma) = \chi_\ell(\sigma)^{-n_{\mathfrak{p},\lambda}}$ holds for all $\sigma \in I_\mathfrak{p}$, where $\chi_\ell\colon \mathrm{Gal}_K \to \mathbb{Z}_\ell^\times$ is the $\ell$-adic cyclotomic character. By Lemma 5.5 and using that $\mathbb{F}_\lambda^\times = \mathbb{F}_\ell^\times$ is cyclic, we deduce that $-n_{\mathfrak{p},\lambda}$ is congruent modulo $\ell - 1$ to an integer $0 \le b \le 2g$. □

We now prove Lemma 5.8 (in the case where $L$ is a field). Set $d := [K : \mathbb{Q}]$ and $e := [L : \mathbb{Q}]$.

Let $\sigma_1, \dots, \sigma_d \colon K \hookrightarrow \overline{\mathbb{Q}}$ be the $d$ distinct embeddings of $K$. Each $\sigma_i$ extends to a homomorphism $K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ of $\overline{\mathbb{Q}}$-algebras and defines a character $\alpha_i \in X(T_K) = \mathrm{Hom}((T_K)_{\overline{\mathbb{Q}}}, \mathbb{G}_{m,\overline{\mathbb{Q}}})$. Observe that $X(T_K)$ is a free abelian group of rank $d$ with basis $\alpha_1, \dots, \alpha_d$. The natural $\mathrm{Gal}_{\mathbb{Q}}$-action on $X(T_K)$ permutes the characters $\alpha_1, \dots, \alpha_d$.

Let $\tau_1, \dots, \tau_e \colon L \hookrightarrow \overline{\mathbb{Q}}$ be the $e$ distinct embeddings of $L$. As above, each $\tau_i$ determines a character $\gamma_i \in X(T_L)$. The group $X(T_L)$ is free abelian of rank $e$ with basis $\gamma_1, \dots, \gamma_e$. The natural $\mathrm{Gal}_{\mathbb{Q}}$-action on $X(T_L)$ permutes the characters $\gamma_1, \dots, \gamma_e$.

We have $\varphi(T_K) \subseteq T_L$. So for each $1 \le j \le e$, we have

$$\gamma_j \circ \varphi = \prod_{i=1}^{d} \alpha_i^{n_{i,j}} \tag{5.2}$$

for unique integers $n_{i,j}$.

A fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ induces isomorphisms $X(T_K) = X((T_K)_{\mathbb{Q}_\ell})$ and $X(T_L) = X((T_L)_{\mathbb{Q}_\ell})$. Observe that under these isomorphisms, we have $\{\alpha_{\mathfrak{p}} : \mathfrak{p} | \ell\} = \{\alpha_1, \dots, \alpha_d\}$ and $\{\gamma_\lambda : \lambda | \ell\} = \{\gamma_1, \dots, \gamma_e\}$. By comparing (5.1) and (5.2), we deduce that each $n_{i,j}$ is equal to some $n_{\mathfrak{p},\lambda}$. By Lemma 5.10, $n_{i,j}$ is congruent modulo $\ell - 1$ to an integer that has absolute value at most $2g$.

By the Chebotarev density theorem, there are infinitely many primes $\ell \ge 5$ that splits completely in the number fields $K$ and $L$ and are not divisible by any prime for which $A$ has bad reduction. Since $n_{i,j}$ is congruent modulo $\ell - 1$ to an integer with absolute value at most $2g$ for infinitely many $\ell$, we deduce that $|n_{i,j}| \le 2g$.

We now consider the general case where $L$ need not be a field. For each $1 \le i \le s$, let $\varphi_i \colon T_K \to T_{L_i}$ be the homomorphism $\varphi$ from §5.4 for the abelian variety $A_i$. Observe that $\varphi \colon T_K \to T_L = \prod_{i=1}^s T_{L_i}$ is given by $(\varphi_1, \dots, \varphi_s)$; one way to show this is to note the Proposition 5.7 characterizes $\varphi$ and that $\beta_{A,\ell} = \prod_{i=1}^s \beta_{A_i,\ell}$.

From the case of Lemma 5.8 we have already proved, we find that there is a basis $\alpha_1, \dots, \alpha_d$ of $X(T_K)$ such that for all $1 \le i \le s$, we have $\gamma_{i,j} \circ \varphi_i = \prod_{k=1}^d \alpha_k^{n_{i,j,k}}$, where $\gamma_{i,1}, \dots, \gamma_{i,[L_i:\mathbb{Q}]}$ is a basis of $X(T_{L_i})$ and $n_{i,j,k}$ is an integer with absolute value at most $2g$. Moreover, the bases $\alpha_1, \dots, \alpha_d$ and $\gamma_{i,1}, \dots, \gamma_{i,[L_i:\mathbb{Q}]}$ are stable under the natural $\mathrm{Gal}_{\mathbb{Q}}$-action. Lemma 5.8 now follows immediately with the basis $\alpha_1, \dots, \alpha_d$ for $X(T)$ and $\{\gamma_{i,j} : 1 \le i \le s, 1 \le j \le [L_i : \mathbb{Q}]\}$ for $X(T_L) = \oplus_{i=1}^s X(T_{L_i})$.

### 5.6. **Proof of Theorem 5.3.**

**Lemma 5.11.**

(i) *We have* $\varphi(T_K) = Y$.

(ii) *For any prime* $\ell$, *we have* $[Y(\mathbb{Q}_\ell)_c \colon \beta_{A,\ell}(\mathrm{Gal}_K)] \ll_g [Y(\mathbb{Q}_\ell)_c : \varphi(T_K(\mathbb{Q}_\ell)_c)]$.

*Proof.* Take the open subgroup $U \subseteq T_K(\mathbb{Q}_\ell)_c$ as in Proposition 5.7. We have

$$\beta_{A,\ell}(\pi_\ell(U)) = \varphi(U)^{-1} = \varphi(U).$$

The set $U$ is Zariski dense in $(T_K)_{\mathbb{Q}_\ell}$ and $\varphi(U) = \beta_{A,\ell}(\pi_\ell(U)) \subseteq Y(\mathbb{Q}_\ell)$, so $\varphi((T_K)_{\mathbb{Q}_\ell}) \subseteq Y_{\mathbb{Q}_\ell}$. Therefore, $\varphi(T_K) \subseteq Y$.

We now prove $\varphi(T_K) = Y$. Let $\psi \colon \mathrm{Gal}_K \to Y(\mathbb{Q}_\ell)/\varphi(T_K)(\mathbb{Q}_\ell)$ be the homomorphism obtained by composing $\beta_{A,\ell}$ with the obvious quotient map. By Lemma 5.1, there is a finite extension $F/K$ such that $\psi|_{\mathrm{Gal}_F}$ is unramified at all prime ideals $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_F$. Since $\varphi(U) \subseteq \varphi(T_K)(\mathbb{Q}_\ell)$ and $[T_K(\mathbb{Q}_\ell)_c : U] \ll_g 1$, we deduce, after possibly replacing $F$ by a finite extension, that $\psi|_{\mathrm{Gal}_F}$ is unramified at all prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$. Therefore, $\psi$ has finite image and hence $\psi|_{\mathrm{Gal}_F} = 1$ for some finite extension $F/K$. For such a finite extension $F/K$, we have $\beta_{A,\ell}(\mathrm{Gal}_F) \subseteq \varphi(T_K)(\mathbb{Q}_\ell)$. The group $\beta_{A,\ell}(\mathrm{Gal}_F)$ is Zariski dense in $Y_{\mathbb{Q}_\ell}$ by Proposition 5.2 and using that $Y$ is connected. So $\varphi(T_K)(\mathbb{Q}_\ell)$ is Zariski dense in $Y_{\mathbb{Q}_\ell}$. Therefore, $\varphi(T_K)_{\mathbb{Q}_\ell} = Y_{\mathbb{Q}_\ell}$ and hence $\varphi(T_K) = Y$ as desired.

Finally, we have

$$[Y(\mathbb{Q}_\ell)_c \colon \beta_{A,\ell}(\mathrm{Gal}_K)] \le [Y(\mathbb{Q}_\ell)_c \colon \beta_{A,\ell}(\pi_\ell(U))] = [Y(\mathbb{Q}_\ell)_c \colon \varphi(U)]. \ll_g [Y(\mathbb{Q}_\ell)_c \colon \varphi(T(\mathbb{Q}_\ell)_c)],$$

where the last inequality uses that $[T(\mathbb{Q}_\ell)_c : U] \ll_g 1$. □

Take any prime $\ell$. Let $\rho\colon \mathrm{Gal}_{\mathbb{Q}_\ell} \to \mathrm{Aut}_{\mathbb{Z}}(X((T_K)_{\mathbb{Q}_\ell}))$ be the Galois action on the character group of the torus $(T_K)_{\mathbb{Q}_\ell}$. Let $F'$ be the subfield of $\overline{\mathbb{Q}}_\ell$ fixed by $\ker\rho$. Let $F/\mathbb{Q}_\ell$ be any subfield of $F'$ for which the extension $F/\mathbb{Q}_\ell$ is Galois and the extension $F'/F$ is unramified. Define the integer

$$e := [F:\mathbb{Q}_\ell]\cdot[Y(F)_c\colon \varphi(T_K(F)_c)],$$

where $Y(F)_c$ and $T_K(F)_c$ are the maximal compact subgroups of $Y(F)$ and $T_K(F)$, respectively, with respect to the $\mathfrak{m}$-adic topology.

**Lemma 5.12.** *We have $y^e \in \varphi(T_K(\mathbb{Q}_\ell)_c)$ for each $y \in Y(\mathbb{Q}_\ell)_c$.*

*Proof.* Take any $y \in Y(\mathbb{Q}_\ell)_c$. We have $y^n = \varphi(t)$ for some $t \in T_K(F)_c$, where $n := [Y(F)_c : \varphi(T_K(F)_c)]$. Since $y$ and $\varphi$ are defined over $\mathbb{Q}_\ell$, we have $y^n = \varphi(\sigma(t))$ for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q}_\ell)$. Therefore, $y^e = y^{[F:\mathbb{Q}]n} = \varphi(t')$ for $t' := \prod_{\sigma\in\mathrm{Gal}(F/\mathbb{Q}_\ell)}\sigma(t)$. We have $t' \in T_K(\mathbb{Q}_\ell)$ since it stable under the $\mathrm{Gal}(F/\mathbb{Q}_\ell)$-action.

Each $\sigma \in \mathrm{Gal}(F/\mathbb{Q}_\ell)$ is a continuous automorphism of $F$ and hence $\sigma(t) \in T_K(F)_c$. Therefore, $t' \in T_K(F)_c \cap T_K(\mathbb{Q}_\ell) = T_K(\mathbb{Q}_\ell)_c$. □

**Lemma 5.13.** *We have $[Y(\mathbb{Q}_\ell)_c : \varphi(T(\mathbb{Q}_\ell)_c)] \le [Y(\mathbb{Q}_\ell) : \gamma(Y(\mathbb{Q}_\ell))]$, where $\gamma\colon Y \to Y$ is the $e$-th power map.*

*Proof.* Let $\gamma\colon Y \to Y$ be the $e$-th power map; it is an isogeny. We have a quotient homomorphism

$$Y(\mathbb{Q}_\ell)_c/\gamma(Y(\mathbb{Q}_\ell)_c) \to Y(\mathbb{Q}_\ell)/\gamma(Y(\mathbb{Q}_\ell)). \tag{5.3}$$

We claim that (5.3) is injective. Take any $y \in Y(\mathbb{Q}_\ell)_c$ for which $y = x^e$ for some $x \in Y(\mathbb{Q}_\ell)$. Let $G$ be the group generated by $x$ and $Y(\mathbb{Q}_\ell)_c$. Since $x^e \in Y(\mathbb{Q}_\ell)_c$, we find that $Y(\mathbb{Q}_\ell)_c$ is a finite index subgroup of $G$ and hence $G$ is compact. We have $G = Y(\mathbb{Q}_\ell)_c$ since $Y(\mathbb{Q}_\ell)_c$ is the maximal compact subgroup of $Y(\mathbb{Q}_\ell)$. Therefore, $x \in Y(\mathbb{Q}_\ell)_c$ which finishes the proof of the claim.

By the injectivity of (5.3), we have $[Y(\mathbb{Q}_\ell)_c : \gamma(Y(\mathbb{Q}_\ell)_c)] \le [Y(\mathbb{Q}_\ell) : \gamma(Y(\mathbb{Q}_\ell))]$. The lemma is now a consequence of Lemma 5.12 which says that $\varphi(T(\mathbb{Q}_\ell)_c) \supseteq \gamma(Y(\mathbb{Q}_\ell)_c)$. □

Let $\gamma\colon Y \to Y$ be the $e$-th power map. The map $\gamma$ is an isogeny and hence $Z := \ker\gamma$ is a finite group scheme. Starting with the short exact sequence $1 \to Z(\overline{\mathbb{Q}}_\ell) \to Y(\overline{\mathbb{Q}}_\ell) \xrightarrow{\gamma} Y(\overline{\mathbb{Q}}_\ell) \to 1$ and taking Galois cohomology gives an injective homomorphism $Y(\mathbb{Q}_\ell)/\gamma(Y(\mathbb{Q}_\ell)) \hookrightarrow H^1(\mathrm{Gal}_{\mathbb{Q}_\ell}, Z(\overline{\mathbb{Q}}_\ell))$. This injective homomorphism and Lemma 5.13 implies that

$$[Y(\mathbb{Q}_\ell)_c : \varphi(T(\mathbb{Q}_\ell)_c)] \le |H^1(\mathrm{Gal}_{\mathbb{Q}_\ell}, Z(\overline{\mathbb{Q}}_\ell))|. \tag{5.4}$$

**Lemma 5.14.** *Let $H$ be a finite abelian group with a $\mathrm{Gal}_{\mathbb{Q}_\ell}$-action. Then the cardinality of $H^1(\mathrm{Gal}_{\mathbb{Q}_\ell}, H)$ can be bounded in terms of $|H|$.*

*Proof.* Set $n = |H|$ and $G := \mathrm{Gal}_{\mathbb{Q}_\ell}$. There is an open normal subgroup $N \subseteq G$ of index at most $n!$ that acts trivially on $H$. We have an inflation-restriction exact sequence

$$0 \to H^1(G/N, H^N) \to H^1(G,H) \to H^1(N,H)$$

The cardinality of $H^1(G/N, H^N)$ can be bounded in terms of $|G/N| \le n!$ and $|H^N| \le n$. So it suffices to bound $H^1(N,H)$ which is the group of continuous homomorphisms $N \to H$ since $N$ acts trivially on $H$.

Let $K$ be the extension of $\mathbb{Q}_\ell$ corresponding to the subgroup $N$ of $G$. By local class field theory, we can idenitify $H^1(N,H)$ with $\mathrm{Hom}(K^\times/(K^\times)^n, H)$. The lemma follows by noting that the cardinality of $K^\times/(K^\times)^n$ can be bounded in terms of $n$ and $[K:\mathbb{Q}_\ell] \le n!$. □

The group scheme $Z$ is finite with cardinality $e^{\dim Y}$. Since $\dim Y \le 2g$, Lemma 5.14 and (5.4) imply that $[Y(\mathbb{Q}_\ell)_c : \varphi(T(\mathbb{Q}_\ell)_c)] \ll_{g,e} 1$.

**Lemma 5.15.** *We have $[Y(F)_c\colon \varphi(T_K(F)_c)] \ll_g 1$.*

*Proof.* Let $R$ be the ring of integers of $F$ and denote its maximal ideal by $\mathfrak{m}$. Define the residue field $\mathbb{F} = R/\mathfrak{m}$ and denote its cardinality by $q$. Let $F^{\mathrm{un}}$ be the maximal unramified extension of $F$ in $\overline{F}$.

We now consider algebraic group schemes of multiplicative type; for background, see [Con14, Appendix B]. The category of algebraic group schemes over $R$ of multiplicative type is equivalent to the category of algebraic group schemes over $F$ of multiplicative type for which the action of $\mathrm{Gal}_F$ on the character group is

unramified. This can be seen by noting that both are anti-equivalent to the category of discrete $\mathrm{Gal}(F^{\mathrm{un}}/F)$-modules that are finitely generated abelian groups, see [Con14, Corollary B.3.6]. Explicitly, the equivalence is given by base extension by $F$.

Let $\mathcal{H}$ be a torus over $R$. The group $\mathcal{H}(F)$ has a natural $\mathfrak{m}$-adic topology. Observe that $\mathcal{H}(R)$ agrees with the maximal compact subgroup $\mathcal{H}(F)_c$ of $\mathcal{H}(F)$ with respect to the $\mathfrak{m}$-adic topology (one can prove this by extending $R$ to reduce to the split case). One can use the smoothness of $\mathcal{H}$ and Hensel's lemma to show that $\mathcal{H}(R/\mathfrak{m}^{n+1}) \to \mathcal{H}(R/\mathfrak{m}^n)$ is surjective with kernel isomorphic to $\mathbb{F}^{\dim \mathcal{H}_F}$; in particular, the kernel has cardinality $q^{\dim \mathcal{H}_F}$. Therefore, $|\mathcal{H}(R/\mathfrak{m}^n)| = |\mathcal{H}(\mathbb{F})| \cdot q^{(n-1)\dim \mathcal{H}_F}$ for all $n \geq 1$.

Define $W := \ker(\varphi) \subseteq T_K$ and $B := W/W^\circ$. The group scheme $B$ is finite and denote it cardinality by $m$. By Lemma 5.9, we have $m \ll_g 1$.

By our choice of $F$, the action of $\mathrm{Gal}_F$ on $X((T_K)_F))$ is unramified, i.e., factors through $\mathrm{Gal}(F^{\mathrm{un}}/F)$. The actions of $\mathrm{Gal}_F$ on $X(W_F)$ and $X(Y_F)$ are also unramified since they can be viewed as a quotient and subgroup, respectively, of $X((T_K)_F)$ stable under the $\mathrm{Gal}_F$ action. So there are short exact sequences

$$1 \to \mathcal{W} \xrightarrow{\iota} \mathcal{T} \xrightarrow{\psi} \mathcal{Y} \to 1 \qquad \text{and} \qquad 1 \to \mathcal{W}_0 \to \mathcal{W} \to \mathcal{B} \to 1$$

of $R$-groups of multiplicative type such that base extension by $F$ gives rise to the short exact sequences

$$1 \to W_F \hookrightarrow (T_K)_F \xrightarrow{\varphi} Y_F \to 1 \qquad \text{and} \qquad 1 \to W_F^\circ \hookrightarrow W_F \to B_F \to 1.$$

We have $\mathcal{Y}(R) = Y(F)_c$ and $\mathcal{T}(R) = T_K(F)_c$, and hence $[\mathcal{Y}(R) : \psi(\mathcal{T}(R))] = [Y(F)_c : \varphi(T_K(F)_c)]$. So it suffices to prove that $[\mathcal{Y}(R) : \psi(\mathcal{T}(R))] \ll_g 1$. Since $\psi(\mathcal{T}(R))$ is a closed subgroup of $\mathcal{Y}(R)$ in the $\mathfrak{m}$-adic topology, it suffices to prove that $[\mathcal{Y}(R/\mathfrak{m}^n) : \psi(\mathcal{T}(R/\mathfrak{m}^n))] \ll_g 1$ holds for all $n \geq 1$.

First suppose that $n > 1$. We have $|\mathcal{Y}(R/\mathfrak{m}^n)| = |\mathcal{Y}(\mathbb{F})| \cdot q^{(n-1)\dim Y}$ and

$$\begin{aligned}
|\psi(\mathcal{T}(R/\mathfrak{m}^n))| &= \frac{|\mathcal{T}(R/m^n)|}{|\mathcal{W}(R/m^n)|} \\
&\geq \frac{1}{m} \frac{|\mathcal{T}(R/m^n)|}{|\mathcal{W}_0(R/m^n)|} \\
&\gg_g \frac{|\mathcal{T}(\mathbb{F})| \cdot q^{(n-1)\dim T_K}}{|\mathcal{W}_0(\mathbb{F})| \cdot q^{(n-1)\dim W_0}} \\
&\geq \frac{|\mathcal{T}(\mathbb{F})|}{|\mathcal{W}(\mathbb{F})|} \cdot q^{(n-1)(\dim T_K - \dim W)}.
\end{aligned}$$

Using that $\dim Y = \dim T_K - \dim W$, we have

$$[\mathcal{Y}(R/\mathfrak{m}^n) : \psi(\mathcal{T}(R/\mathfrak{m}^n))] \ll_g |\mathcal{Y}(\mathbb{F})|/(|\mathcal{T}(\mathbb{F})|/|\mathcal{W}(\mathbb{F})|) = [\mathcal{Y}(\mathbb{F}) : \psi(\mathcal{T}(\mathbb{F}))].$$

So it suffices to prove the $n = 1$ case, i.e., show that $[\mathcal{Y}(\mathbb{F}) : \psi(\mathcal{T}(\mathbb{F}))] \ll_g 1$.

From the short exact sequence $1 \to \mathcal{W}(\overline{\mathbb{F}}) \to \mathcal{T}(\overline{\mathbb{F}}) \xrightarrow{\psi} \mathcal{Y}(\overline{\mathbb{F}}) \to 1$, taking Galois cohomology gives an injective homomorphism $\mathcal{Y}(\mathbb{F})/\psi(\mathcal{T}(\mathbb{F})) \hookrightarrow H^1(\mathrm{Gal}_{\mathbb{F}}, \mathcal{W}(\overline{\mathbb{F}}))$. From the short exact sequence $1 \to \mathcal{W}_0(\overline{\mathbb{F}}) \to \mathcal{W}(\overline{\mathbb{F}}) \to \mathcal{B}(\overline{\mathbb{F}}) \to 1$, we have an exact sequence $H^1(\mathrm{Gal}_{\mathbb{F}}, \mathcal{W}_0(\overline{\mathbb{F}})) \to H^1(\mathrm{Gal}_{\mathbb{F}}, \mathcal{W}(\overline{\mathbb{F}})) \to H^1(\mathrm{Gal}_{\mathbb{F}}, \mathcal{B}(\overline{\mathbb{F}}))$. Since $(\mathcal{W}_0)_{\mathbb{F}}$ is connected, Lang's theorem implies that $H^1(\mathrm{Gal}_{\mathbb{F}}, \mathcal{W}_0(\overline{\mathbb{F}})) = 0$ and hence

$$[\mathcal{Y}(\mathbb{F}) : \psi(\mathcal{T}(\mathbb{F}))] \leq |H^1(\mathrm{Gal}_{\mathbb{F}}, \mathcal{W}(\overline{\mathbb{F}}))| \leq |H^1(\mathrm{Gal}_{\mathbb{F}}, \mathcal{B}(\overline{\mathbb{F}}))|.$$

Since $\mathcal{B}(\overline{\mathbb{F}})$ is a finite group of cardinality at most $m \ll_g 1$ and $\mathrm{Gal}_{\mathbb{F}}$ is pro-cyclic, we have $|H^1(\mathrm{Gal}_{\mathbb{F}}, \mathcal{B}(\overline{\mathbb{F}}))| \ll_g 1$ and hence $[\mathcal{Y}(\mathbb{F}) : \psi(\mathcal{T}(\mathbb{F}))] \ll_g 1$. □

Since $[Y(\mathbb{Q}_\ell)_c : \varphi(T(\mathbb{Q}_\ell)_c)] \ll_{g,e} 1$, Lemma 5.15 implies that $[Y(\mathbb{Q}_\ell)_c : \varphi(T(\mathbb{Q}_\ell)_c)] \ll_{g,[F:\mathbb{Q}_\ell]} 1$. If $\ell$ is unramified in $K$, then we can choose $F = \mathbb{Q}_\ell$ and hence $[Y(\mathbb{Q}_\ell) : \varphi(T(\mathbb{Q}_\ell)_c)] \ll_g 1$. This proves part (i).

To prove part (ii), it suffices to show that $[F : \mathbb{Q}_\ell] \ll_{[K:\mathbb{Q}]} 1$. By Lemma 5.8, there is a basis $\alpha_1, \ldots, \alpha_{[K:\mathbb{Q}]}$ of $X((T_K)_{\mathbb{Q}_\ell})$ that is permuted by the natural $\mathrm{Gal}_{\mathbb{Q}_\ell}$-action. Therefore, $[F : \mathbb{Q}_\ell] \leq [K : \mathbb{Q}]!$.

## 6. Proof of Theorem 1.2(a) and (b)

By Lemma 2.13, we may assume the groups $G_{A,\ell}$ are all connected.

Fix a prime $\ell \geq c\cdot\max(\{[K:\mathbb{Q}], h(A), N(\mathfrak{q})\})^\gamma$. We have already proved part (c) of Theorem 1.2 in §4, so by increasing the constants $c$ and $\gamma$ appropriately, we may assume that $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell}$ is reductive. Let $\mathcal{S}_{A,\ell}$ be the derived subgroup of $\mathcal{G}_{A,\ell}$; it is a semisimple group scheme over $\mathbb{Z}_\ell$. We have proved part (d) of Theorem 1.2 in §4, so by increasing the constants $c$ and $\gamma$ appropriately, we may also assume that $\rho_{A,\ell}(\mathrm{Gal}_K)$ contains the commutator subgroup $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)'$ of $\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell)$. In particular, $\rho_{A,\ell}(\mathrm{Gal}_K) \supseteq \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'$.

Define $S = (\mathcal{S}_{A,\ell})_{\mathbb{Q}_\ell}$; it is the derived subgroup of the connected reductive group $G_{A,\ell}$.

With notation as in §5.2 and Proposition 5.2, there is a homomorphism

$$\delta := \det_L \colon G_{A,\ell} \to Y_{\mathbb{Q}_\ell}$$

of algebraic groups over $\mathbb{Q}_\ell$, where $Y$ is a torus defined over $\mathbb{Q}$. Define $H := \ker(\delta)$.

**Lemma 6.1.** *We have $H^\circ = S$ and the cardinality of the group scheme $H/S$ can be bounded in terms of $g$.*

*Proof.* We have $H \supseteq S$ since $S$ is semisimple and $Y_{\mathbb{Q}_\ell}$ is a torus. It thus suffices to show that the kernel of $\delta|_C = \det_L|_C$ is finite with cardinality bounded in terms of $g$, where $C$ is the central torus of $G_{A,\ell}$. By Proposition 2.12, $C = (C_A)_{\mathbb{Q}_\ell}$ where $C_A$ is the central torus of $\mathrm{MT}_A$. As noted in §5.2, the homomorphism $\det_L|_{C_A} \colon C_A \to Y$ is an isogeny of degree $d_1\cdots d_s \ll_g 1$. □

Define the homomorphism $\beta_{A,\ell}\colon \mathrm{Gal}_K \to Y(\mathbb{Q}_\ell)$ by $\beta_{A,\ell} = \det_L \circ \rho_{A,\ell}$. We have $\beta_{A,\ell}(\mathrm{Gal}_K) \subseteq Y(\mathbb{Q}_\ell)_c$, where $Y(\mathbb{Q}_\ell)_c$ is the maximal compact subgroup of $Y(\mathbb{Q}_\ell)$ with respect to the $\ell$-adic topology.

We have inequalities

$$\begin{aligned}
[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] &= [\det_L(\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell))\colon \det_L(\rho_{A,\ell}(\mathrm{Gal}_K))] \cdot [H(\mathbb{Q}_\ell)\cap \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : H(\mathbb{Q}_\ell)\cap \rho_{A,\ell}(\mathrm{Gal}_K)] \\
&\leq [Y(\mathbb{Q}_\ell)_c\colon \beta_{A,\ell}(\mathrm{Gal}_K)] \cdot [H(\mathbb{Q}_\ell)\cap \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : H(\mathbb{Q}_\ell)\cap \rho_{A,\ell}(\mathrm{Gal}_K)] \\
&\ll_g [Y(\mathbb{Q}_\ell)_c\colon \beta_{A,\ell}(\mathrm{Gal}_K)] \cdot [S(\mathbb{Q}_\ell)\cap \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : S(\mathbb{Q}_\ell)\cap \rho_{A,\ell}(\mathrm{Gal}_K)],
\end{aligned}$$

where we have used Lemma 6.1 in the last inequality and we have also used that $\det_L(\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell))$ is a compact subgroup of $Y(\mathbb{Q}_\ell)$. We have

$$\begin{aligned}
[S(\mathbb{Q}_\ell)\cap \mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : S(\mathbb{Q}_\ell)\cap \rho_{A,\ell}(\mathrm{Gal}_K)] &= [\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell) : \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)\cap \rho_{A,\ell}(\mathrm{Gal}_K)] \\
&\leq [\mathcal{S}_{A,\ell}(\mathbb{Z}_\ell) : \mathcal{S}_{A,\ell}(\mathbb{Z}_\ell)'] \\
&\ll_g 1,
\end{aligned}$$

where the last inequality uses Proposition 4.25(iii). Combining our inequalities, we find that

$$[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] \ll_g [Y(\mathbb{Q}_\ell)_c\colon \beta_{A,\ell}(\mathrm{Gal}_K)].$$

Theorem 1.2(a) and (b) now follow from Theorem 5.3.

## 7. Proof of Theorem 1.4

We first give a slight generalization of Theorem 1.2.

**Theorem 7.1.** *The conclusion of Theorem 1.2 holds with (1.1) replaced by the assumption that $\ell \geq c\cdot \max(\{[K:\mathbb{Q}], h(A)\})^\gamma$ and $\ell \nmid n$, where $n$ is a positive integer satisfying $n < cN(\mathfrak{q})^\gamma$ that depends on $A$.*

*Proof.* There are only two times in the proof of Theorem 1.2 that we used the assumption

$$\ell \geq c\,N(\mathfrak{q})^\gamma. \tag{7.1}$$

In §4.1, we used (7.1) to prove that $\mathfrak{q}\nmid\ell$ and that $\ell$ does not divide a specific non-zero integer $D$ that satisfies $|D| < c\,N(\mathfrak{q})^\gamma$. In §4.5, we used (7.1) to prove that $\mathfrak{q}\nmid\ell$ and that $\ell$ does not divide non-zero integers $\beta_M$ satisfying $|\beta_M| < c\,N(\mathfrak{q})^\gamma$, where $M$ lie in a set $\mathcal{M}$ with $|\mathcal{M}| \ll_g 1$.

The theorem thus holds with $n := N(\mathfrak{q})\cdot|D|\cdot\prod_{M\in\mathcal{M}}|\beta_M|$ after possibly increasing the constants $c$ and $\gamma$ so that $n < cN(\mathfrak{q})^\gamma$. □

By the same arguments as in the proof of Lemma 2.13, we may assume that all the groups $G_{A,\ell}$ are connected; note that the integer $D$ is unchanged if we replace $A/K$ with $A_{K_A^{\mathrm{conn}}}/K_A^{\mathrm{conn}}$.

**Lemma 7.2.** *Let $\ell$ be a prime for which $\mathcal{G}_{A,\ell}$ is reductive. For each maximal torus $T$ of $G$, there is a subset $U_T \subseteq T(\mathbb{F}_\ell)$ such that the following conditions hold:*

(a) *Let $\mathfrak{p} \nmid \ell$ be a non-zero prime ideal of $\mathcal{O}_K$ for which $A$ has good reduction. If $\bar{\rho}_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ is conjugate in $G(\mathbb{F}_\ell)$ to an element of $T(\mathbb{F}_\ell) - U_T$, then $\Phi_{A,\mathfrak{p}} \cong \mathbb{Z}^r$.*

(b) *We have $|U_T| \ll_g \ell^{r-1}$.*

(c) *For any $h \in G(\mathbb{F}_\ell)$ and maximal torus $T$ of $G$, we have $U_{hTh^{-1}} = hU_Th^{-1}$.*

*Proof.* Fix a maximal torus $T$ of $G$. Let $\alpha_1, \dots, \alpha_{2g} \in X(T)$ be the weights of $T \subseteq \mathrm{GL}_{A[\ell]}$, with multiplicity, acting on $A[\ell]$. Let $M \subseteq \mathbb{Z}^{2g}$ be the group consisting of $e \in \mathbb{Z}^{2g}$ satisfying $\prod_{i=1}^{2g} \alpha_i^{e_i} = 1$. By Theorem 4.5 and Lemma 4.19, there are only finite many possibilities for $M$ in terms of $g$. Note that we have an isomorphism $X(T) \cong \mathbb{Z}^{2g}/M$; in particular, $\mathbb{Z}^{2g}/M$ is a free abelian group of rank $r$. Define the finite set

$$\mathscr{A} := \{m \in \mathbb{Z}^{2g} - M : \max_i |m_i| \leq C\},$$

where $C$ is a positive constant depending only on $g$ that we will later impose an additional condition on. For each $m \in \mathbb{Z}^{2g}$, define the character $\beta_m := \prod_{i=1}^{2g} \alpha_i^{m_i} \in X(T)$. We have $\beta_m \neq 1$ for each $m \in \mathscr{A}$ since $m \notin M$. Define $Y := \cup_{m \in \mathscr{A}} \ker \beta_m$. The set of characters $\{\beta_m : m \in \mathscr{A}\} \subseteq X(T)$ is stable under the action of $\mathrm{Gal}_{\mathbb{F}_\ell}$ since $\alpha_1, \dots, \alpha_{2g}$ is stable under this Galois action. We may thus view $Y$ as a subvariety of $T$ defined over $\mathbb{F}_\ell$. Define the subset $U_T := Y(\mathbb{F}_\ell)$ of $T(\mathbb{F}_\ell)$. Note that while $M$ and $\mathscr{A}$ depend on our choice of ordering $\alpha_1, \dots, \alpha_{2g}$ of weights, the set $U_T$ does not.

We now prove (a). Take any prime $\mathfrak{p} \nmid \ell$ for which $A$ has good reduction and $\bar{\rho}_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ is conjugate in $G(\mathbb{F}_\ell)$ to an element of $T(\mathbb{F}_\ell) - U_T$. We may assume that $t_\mathfrak{p} := \bar{\rho}_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ lies in $T(\mathbb{F}_\ell) - U$. The roots of $P_{A,\mathfrak{p}}(x)$ modulo $\ell$, with multiplicity, are $\alpha_1(t_\mathfrak{p}), \dots, \alpha_{2g}(t_\mathfrak{p}) \in \overline{\mathbb{F}}_\ell$. Let $R$ be the ring of integers of a splitting field $F/\mathbb{Q}_\ell$ of $P_{A,\mathfrak{p}}(x)$. Let $\pi_1, \dots, \pi_{2g} \in R$ be the roots of $P_{A,\mathfrak{p}}(x)$ with multiplicity; note that each $\pi_i$ lies in $R$ since it is an algebraic integer in $F$. Let $\mathbb{F}$ be the residue field of $R$. Let $\overline{\pi}_1, \dots, \overline{\pi}_{2g} \in \overline{\mathbb{F}}_\ell$ be the values obtained by reducing each $\pi_i$ and then applying a fixed embedding $\mathbb{F} \hookrightarrow \overline{\mathbb{F}}_\ell$. By rearranging the $\pi_i$, we may assume that $\overline{\pi}_i = \alpha_i(t_\mathfrak{p})$ holds for all $1 \leq i \leq 2g$. Let $M_\mathfrak{p}$ be the group of $e \in \mathbb{Z}^{2g}$ that satisfy $\prod_{i=1}^{2g} \pi_i^{e_i} = 1$. By Proposition 2.6, $M_\mathfrak{p}$ is one of a finite number of subgroups of $\mathbb{Z}^{2g}$ that depend on $g$.

We claim that $M_\mathfrak{p} \subseteq M$. Suppose to the contrary that there is an $m \in M_\mathfrak{p} - M$. We may assume that $\max_i |m_i| \leq C$, where $C$ is our constant depending only on $g$; we can take $m$ to be in a fixed finite set of generators for each of the groups $M_i$ from Proposition 2.6. We have $(\prod_{i=1}^{2g} \alpha^{m_i})(t_\mathfrak{p}) = 1$ since $m \in M_\mathfrak{p}$. In particular, by our choice of $C$, there is an $m \in \mathscr{A}$ such that $\beta_m(t_\mathfrak{p}) = 1$. Therefore, $t_\mathfrak{p} \in T(\mathbb{F}_\ell) \cap Y(\overline{\mathbb{F}}_\ell) = Y(\mathbb{F}_\ell) = U_T$. However, this is a contradiction since we assumed that $t_\mathfrak{p} \in T(\mathbb{F}_\ell) - U_T$. This proves the claim.

Since $M_\mathfrak{p} \subseteq M$, we have a surjective homomorphism $\Phi_{A,\mathfrak{p}} \cong \mathbb{Z}^{2g}/M_\mathfrak{p} \to \mathbb{Z}^{2g}/M \cong \mathbb{Z}^r$. Let $T_\mathfrak{p}$ be the Zariski closure in $G_{A,\ell}$ of the subgroup generated by the semisimple element $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$. As explained in the proof of Lemma 2.7, we have $X(T_\mathfrak{p}) \cong \Phi_{A,\mathfrak{p}}$. We thus have $X(T_\mathfrak{p}^\circ) = \Phi_{A,\mathfrak{p}}/(\Phi_{A,\mathfrak{p}})_{\mathrm{tors}}$, where the neutral component $T_\mathfrak{p}^\circ$ is a torus and $(\Phi_{A,\mathfrak{p}})_{\mathrm{tors}}$ is the torsion subgroup of $\Phi_{A,\mathfrak{p}}$. Since there is a surjective homomorphism $\Phi_{A,\mathfrak{p}} \twoheadrightarrow \mathbb{Z}^r$, the torus $T_\mathfrak{p}^\circ$ has dimension at least $r$. Since $T_\mathfrak{p}^\circ$ is contained in the reductive group $G_{A,\ell}$ of rank $r$, we find that $T_\mathfrak{p}^\circ$ is a maximal torus of $G_{A,\ell}$ and has dimension $r$. We have $T_\mathfrak{p} = T_\mathfrak{p}^\circ$ since a maximal torus of a connected reductive group is its own centralizer. So $\Phi_{A,\mathfrak{p}} \cong X(T_\mathfrak{p})$ is a free abelian group of rank $r$. This completes the proof of (a).

We now prove (b). Since $|\mathscr{A}| \ll_g 1$, to verify $|U_T| \ll_g \ell^{r-1}$ it suffices to prove that $|\{t \in T(\mathbb{F}_\ell) : \beta_m(t) = 1\}| \ll_g \ell^{r-1}$ for each $m \in \mathscr{A}$. Take any $m \in \mathscr{A}$. Let $\mathbb{F}_{\ell^d}/\mathbb{F}_\ell$ be the smallest extension over which $T$ splits; the character $\beta_m$ is defined over $\mathbb{F}_{\ell^d}$. We have $d \ll_g 1$. For $t \in T(\mathbb{F}_\ell)$ satisfying $\beta_m(t) = 1$, we have $\sigma(\beta_m)(t) = \sigma(\beta_m(t)) = \sigma(1) = 1$ for all $\sigma \in \mathrm{Gal}(\mathbb{F}_{\ell^d}/\mathbb{F}_\ell)$. Define $W := \bigcap_{\sigma \in \mathrm{Gal}(\mathbb{F}_{\ell^d}/\mathbb{F}_\ell)} \ker \sigma(\beta_m)$; it is a subvariety of $T$ defined over $\mathbb{F}_\ell$ that contains all $t \in T(\mathbb{F}_\ell)$ satisfying $\beta_m(t) = 1$. So to verify $|U_T| \ll_g \ell^{r-1}$ it suffices to prove that $|W(\mathbb{F}_\ell)| \ll_g \ell^{r-1}$. For any $\sigma \in \mathrm{Gal}(\mathbb{F}_{\ell^d}/\mathbb{F}_\ell)$, $\sigma$ permutes the characters $\alpha_1, \dots, \alpha_{2g}$ (with multiplicity) and hence there is an $m_\sigma \in \mathscr{A}$ satisfying $\sigma(\beta_m) = \beta_{m_\sigma}$. The algebraic group $W$ is diagonalizable (over $\mathbb{F}_{\ell^d}$) and

$$X(W) \cong \mathbb{Z}^{2g}/\Big(M + \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_{\ell^d}/\mathbb{F}_\ell)} \mathbb{Z}m_\sigma\Big)$$

There are only finitely many possibilities (in terms of $g$) for the group $X(W)$ since $d \ll_g 1$ and since there are only finitely many possibilities (in terms of $g$) for $M$ and each $m_\sigma$. In particular, the torsion subgroup

of $X(W)$ can be bounded in terms of $g$ and hence $|(W/W^\circ)(\overline{\mathbb{F}}_\ell)| \ll_g 1$. Therefore, $|W(\mathbb{F}_\ell)| \ll_g |W^\circ(\mathbb{F}_\ell)| \ll_g \ell^{r-1}$, where the last inequality uses that $W^\circ$ is a torus over $\mathbb{F}_\ell$ of rank at most $r-1$ and $r$ can be bounded in terms of $g$. We deduce that $|U_T| \ll_g \ell^{r-1}$.

It remains to prove (c). Take any $h \in G(\mathbb{F}_\ell)$ and define the maximal torus $T' := hTh^{-1}$ of $G$. We have an isomorphism $\iota\colon T' \to T$, $t \mapsto h^{-1}th$ of tori and an isomorphism $X(T) \to X(T')$, $\alpha \mapsto \alpha \circ \iota$ of groups that respects the $\mathrm{Gal}_{\mathbb{F}_\ell}$-actions. For $1 \le i \le 2g$, define $\alpha'_i := \alpha_i \circ \iota$. Observe that $\alpha'_1, \dots, \alpha'_{2g}$ are the weights, with multiplicity, of $T'$ acting on $A[\ell]$. The group $M$ is also the group consisting of $e \in \mathbb{Z}^{2g}$ satisfying $\prod_{i=1}^{2g}(\alpha'_i)^{e_i} = 1$. So we have the same set $\mathscr{A}$ when defining $U_{T'}$ (with our ordering of weights $\alpha'_1, \dots, \alpha'_{2g}$). For each $m \in \mathbb{Z}^{2g}$, define the character $\beta'_m := \prod_{i=1}^{2g}(\alpha'_i)^{m_i}$ of $T'$. Note that $\beta'_m = \beta_m \circ \iota$ for all $m \in \mathbb{Z}^{2g}$. For any $t \in T(\mathbb{F}_\ell)$, we have

$$t \in U_T \iff \beta_m(t) = 1 \text{ for some } m \in \mathscr{A} \iff \beta'_m(hth^{-1}) = 1 \text{ for some } m \in \mathscr{A} \iff hth^{-1} \in U_{T'}.$$

Since $\iota$ induces an isomorphism $T'(\mathbb{F}_\ell) \to T(\mathbb{F}_\ell)$, we have $U_{T'} = hU_Th^{-1}$. □

**Lemma 7.3.** *Let $\ell$ be a prime for which $\mathcal{G}_{A,\ell}$ is reductive. There is a subset $\mathcal{B}_\ell$ of $\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)$ stable under conjugation satisfying $|\mathcal{B}_\ell|/|\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)| = 1 + O_g(1/\ell)$ such that if $\mathfrak{p} \nmid \ell$ is a prime ideal of $\mathcal{O}_K$ for which $A$ has good reduction and $\bar\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \in \mathcal{B}_\ell$, then $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank $r$.*

*Proof.* The group $G := (\mathcal{G}_{A,\ell})_{\mathbb{F}_\ell}$ is connected and reductive. Let $\mathcal{B}_\ell$ be the set of elements in $G(\mathbb{F}_\ell) - \bigcup_T U_T$ that are semisimple and regular in $G$, where the union is over all maximal tori of $G$ and the sets $U_T$ are as in Lemma 7.2. Using property (c) of Lemma 7.2, we find that $\mathcal{B}_\ell$ is stable under conjugation by $G$.

Take any prime ideal $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_K$ for which $A$ has good reduction and $\bar\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \in \mathcal{B}_\ell$. In particular, $\bar\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})$ is conjugate in $G(\mathbb{F}_\ell)$ to an element of $T(\mathbb{F}_\ell) - U_T$ for some maximal torus $T$ of $G$. Property (a) of Lemma 7.2 implies that $\Phi_{A,\mathfrak{p}} \cong \mathbb{Z}^r$.

It remains to prove that $|\mathcal{B}_\ell|/|\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)| = 1 + O_g(1/\ell)$. Let $G(\mathbb{F}_\ell)_{\mathrm{rs}}$ be the set of elements in $G(\mathbb{F}_\ell)$ that are regular and semisimple in $G$. For each maximal torus $T$ of $G$, define $T(\mathbb{F}_\ell)_{\mathrm{rs}} = T(\mathbb{F}_\ell) \cap G(\mathbb{F}_\ell)_{\mathrm{rs}}$. We have $|G(\mathbb{F}_\ell)_{\mathrm{rs}}| = |G(\mathbb{F}_\ell)|(1 + O_g(1/\ell))$ and $|T(\mathbb{F}_\ell)_{\mathrm{rs}}| = \ell^r + O_g(\ell^{r-1})$ for any maximal torus $T$ of $G$ by the proof of Lemma 4.5 of [JKZ13]; note that the proof of this lemma only uses that $G/\mathbb{F}_\ell$ is reductive and there are only a finite number of possibilities, in terms of $g$, for the Lie type of $G$.

Every element of $G(\mathbb{F}_\ell)$ that is regular and semisimple element in $G$ lies in a unique maximal torus. We thus have a disjoint union $\mathcal{B}_\ell = \bigcup_T \big(T(\mathbb{F}_\ell)_{\mathrm{rs}} - U_T\big)$, with the union being over all maximal tori $T$ of $G$. Therefore,

$$|\mathcal{B}_\ell| \ge \sum_T \big(|T(\mathbb{F}_\ell)_{\mathrm{rs}}| - |U_T|\big) = \sum_T \ell^r \cdot (1 + O_g(1/\ell)),$$

where we have used property (b) of Lemma 7.2. We also have a disjoint union $G(\mathbb{F}_\ell)_{\mathrm{rs}} = \bigcup_T T(\mathbb{F}_\ell)_{\mathrm{rs}}$ and hence $|G(\mathbb{F}_\ell)_{\mathrm{rs}}| = \sum_T \ell^r \cdot (1 + O_g(1/\ell))$. Since $|G(\mathbb{F}_\ell)_{\mathrm{rs}}| = |G(\mathbb{F}_\ell)|(1 + O_g(1/\ell))$, we have inequalities $|G(\mathbb{F}_\ell)| \ge |\mathcal{B}_\ell| \ge |G(\mathbb{F}_\ell)|(1 + O_g(1/\ell))$. Therefore, $|\mathcal{B}_\ell|/|\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)| = 1 + O_g(1/\ell)$. □

Let $\mathfrak{q}$ be a non-zero prime ideal of $\mathcal{O}_K$ for which $A$ has good reduction and $\Phi_{A,\mathfrak{q}}$ is a free abelian group of rank $r$. We can assume that $\mathfrak{q}$ is chosen so that $N(\mathfrak{q})$ is minimal. We have $D = \prod_{p \in V} p$, where $V$ is the set of primes $p$ that ramify in $K$ or are divisible by a prime ideal for which $A$ has bad reduction.

By Theorem 7.1, there are positive constants $c$ and $\gamma$, depending only on $g$, and a positive integer $n < cN(\mathfrak{q})^\gamma$ such that for all primes $\ell \nmid nD$ satisfying $\ell \ge c \cdot \max(\{[K : \mathbb{Q}], h(A)\})^\gamma$, we have

$$[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] \ll_g 1$$

and the $\mathbb{Z}_\ell$-group scheme $\mathcal{G}_{A,\ell}$ is reductive.

**Lemma 7.4.** *Let $\ell \nmid nD$ be a prime satisfying $\ell \ge c \cdot \max(\{[K : \mathbb{Q}], h(A)\})^\gamma$. There is a subset $\mathcal{C}_\ell$ of $\bar\rho_{A,\ell}(\mathrm{Gal}_K)$ that is stable under conjugation such that the following hold:*

(a) *if $\mathfrak{p} \nmid \ell$ is a prime ideal of $\mathcal{O}_K$ for which $A$ has good reduction and $\bar\rho_{A,\ell}(\mathrm{Frob}_p) \in \mathcal{C}_\ell$, then $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank $r$.*

(b) $|\mathcal{C}_\ell|/|\bar\rho_{A,\ell}(\mathrm{Gal}_K)| = 1 + O_g(1/\ell)$.

*Proof.* Take any prime $\ell \nmid nD$ satisfying $\ell \geq c \cdot \max(\{[K:\mathbb{Q}], h(A)\})^\gamma$. From above, we know that $\mathcal{G}_{A,\ell}$ is reductive and $[\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] \ll_g 1$. Let $\mathcal{B}_\ell$ be the set of elements in $\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)$ as in Lemma 7.3. Define $\mathcal{C}_\ell := \bar{\rho}_{A,\ell}(\mathrm{Gal}_K) \cap \mathcal{B}_\ell$; it is stable under conjugation by $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$. Take any prime ideal $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_K$ for which $A$ has good reduction and $\bar{\rho}_{A,\ell}(\mathrm{Frob}_p) \in \mathcal{C}_\ell$. Since $\bar{\rho}_{A,\ell}(\mathrm{Frob}_p) \in \mathcal{B}_\ell$, the group $\Phi_{A,\mathfrak{p}}$ is free abelian of rank $r$. This proves part (a).

We have $\bar{\rho}_{A,\ell}(\mathrm{Gal}_K) - \mathcal{C}_\ell \subseteq \mathcal{G}_{A,\ell}(\mathbb{F}_\ell) - \mathcal{B}_\ell$ and hence

$$|\bar{\rho}_{A,\ell}(\mathrm{Gal}_K) - \mathcal{C}_\ell| \leq |\mathcal{G}_{A,\ell}(\mathbb{F}_\ell) - \mathcal{B}_\ell| = |\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)|(1 - |\mathcal{B}_\ell|/|\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)|) \ll_g |\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)|/\ell,$$

where the last inequality uses that $|\mathcal{B}_\ell|/|\mathcal{G}_{A,\ell}(\mathbb{F}_\ell)| = 1 + O_g(1/\ell)$. Using that $[\mathcal{G}_{A,\ell}(\mathbb{F}_\ell) : \bar{\rho}_{A,\ell}(\mathrm{Gal}_K)] \leq [\mathcal{G}_{A,\ell}(\mathbb{Z}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_K)] \ll_g 1$, we deduce that

$$|\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)| - |\mathcal{C}_\ell| = |\bar{\rho}_{A,\ell}(\mathrm{Gal}_K) - \mathcal{C}_\ell| \ll_g |\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)|/\ell.$$

Part (b) follows by dividing by $|\bar{\rho}_{A,\ell}(\mathrm{Gal}_K)|$. □

**Proposition 7.5.** *Take any prime $\ell \nmid nD$ satisfying $\ell \geq c \cdot \max(\{[K:\mathbb{Q}], h(A)\})^\gamma$. After possibly increasing the constant $c$, that depends only on $g$, we have $N(\mathfrak{q}) \ll_g (\max\{\ell, [K:\mathbb{Q}], \log D\})^e$, where $e \geq 1$ depends only on $g$.*

*Proof.* Take any prime $\ell \nmid nD$ satisfying $\ell \geq c \cdot \max(\{[K:\mathbb{Q}], h(A)\})^\gamma$. Define the group $G := \bar{\rho}_{A,\ell}(\mathrm{Gal}_K)$ and the field $L := K(A[\ell])$. Note that $L$ is the subfield of $\overline{K}$ fixed by $\ker \bar{\rho}_{A,\ell}$. Let $\mathcal{C}_\ell \subseteq G$ be the set from Lemma 7.4. By increasing the constant $c$, that only depends on $g$, we may assume that $|\mathcal{C}_\ell|/|G| \geq 1/2$.

Let $\pi_{\mathcal{C}_\ell}(x)$ be the set of non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ that are unramified in $L$ and satisfy $\bar{\rho}_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \in \mathcal{C}_\ell$. An effective version of the Chebotarev density theorem (Théorème 4 and Remark $(20_R)$ of [Ser81] along with the trivial bound $|\mathcal{C}_\ell| \leq [L:K]$) implies that

$$\Big|\pi_{\mathcal{C}_\ell}(x) - \frac{|\mathcal{C}_\ell|}{|G|}\operatorname{Li}(x)\Big| \ll [L:K]x^{1/2}\Big(\log x + \log[L:\mathbb{Q}] + [K:\mathbb{Q}]^{-1}\log d_K + \sum_{p \in P(L/K)} \log p\Big),$$

where $\operatorname{Li}(x) = \int_2^x (\log t)^{-1}\,dt$, $d_K$ is the absolute value of the discriminant of $K$, and $P(L/K)$ is the set of primes $p$ that are divisible by some prime ideal of $\mathcal{O}_K$ that ramifies in $L$. Note that this version of the Chebotarev density theorem uses our GRH assumption. By [Ser81, Proposition 6], we have

$$[K:\mathbb{Q}]^{-1}\log d_K \leq \sum_{p \in P(K)} \log p + |P(K)|\log[K:\mathbb{Q}] \ll (\log[K:\mathbb{Q}] + 1)\sum_{p \in P(K)} \log p,$$

where $P(K)$ is the set of primes $p$ that ramify in $K$. Since $P(K) \cup P(L/K) \subseteq V \cup \{\ell\}$, we have

$$\Big|\pi_{\mathcal{C}_\ell}(x) - \frac{|\mathcal{C}_\ell|}{|G|}\operatorname{Li}(x)\Big| \ll [L:\mathbb{Q}]x^{1/2}\Big(\log x + \log[L:\mathbb{Q}] + (\log[K:\mathbb{Q}]+1)(\textstyle\sum_{p\in V}\log p + \log \ell)\Big).$$

Since $[L:K] \leq |\operatorname{GL}_{2g}(\mathbb{F}_\ell)| \leq \ell^{4g^2}$, we find that

$$\Big|\pi_{\mathcal{C}_\ell}(x) - \frac{|\mathcal{C}_\ell|}{|G|}\operatorname{Li}(x)\Big| \ll_g \ell^{4g^2+1}[K:\mathbb{Q}]^2 x^{1/2}\Big(\log x + \textstyle\sum_{p\in V}\log p\Big)$$

and hence

$$\pi_{\mathcal{C}_\ell}(x) \geq \frac{1}{2}\operatorname{Li}(x) + O_g\Big(\ell^{4g^2+1}[K:\mathbb{Q}]^2 x^{1/2}(\log x + \log D)\Big).$$

So there is an $e \geq 2$, depending only on $g$, such that if $\max\{\ell, [K:\mathbb{Q}], \log D\} \ll x^{1/e}$, then $\pi_{\mathcal{C}_\ell}(x) \geq \frac{1}{2}\operatorname{Li}(x) + O_g(x^{9/10})$. Thus for $x \gg_g (\max\{\ell, [K:\mathbb{Q}], \log D\})^e$, we will have $\pi_{\mathcal{C}_\ell}(x) \geq \frac{1}{4}\operatorname{Li}(x)$ and also $\frac{1}{4}\operatorname{Li}(x) \geq 2[K:\mathbb{Q}](\log D + 1) + 1$ after possibly increasing $e$ (which depends only on $g$). Therefore, for $x \gg_g (\max\{\ell, [K:\mathbb{Q}], \log D\})^e$, we have $\pi_{\mathcal{C}_\ell}(x) \geq 2[K:\mathbb{Q}](\log D + 1) + 1$ and hence $\pi_{\mathcal{C}_\ell}(x)$ is strictly larger than the number of prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ dividing $D\ell$. So there is a non-zero prime ideal $\mathfrak{p} \nmid D\ell$ with $N(\mathfrak{p}) \ll_g (\max\{\ell, [K:\mathbb{Q}], \log D\})^e$ for which $\bar{\rho}_{A,\ell}(\mathrm{Frob}_\mathfrak{p}) \in \mathcal{C}_\ell$. The abelian variety $A$ has good reduction at $\mathfrak{p}$ since $\mathfrak{p} \nmid D$. By Lemma 7.4, $\Phi_{A,\mathfrak{p}}$ is a free abelian group of rank $r$. By the minimality of our choice of $\mathfrak{q}$, we have $N(\mathfrak{q}) \leq N(\mathfrak{p}) \ll_g (\max\{\ell, [K:\mathbb{Q}], \log D\})^e$. □

We have

$$\sum_{\ell \mid nD} \log \ell \leq \log n + \log D \leq \log(cN(\mathfrak{q})^{\gamma}) + \log D = \gamma \log N(\mathfrak{q}) + \log c + \log D$$

Define $C := c \cdot \max(\{[K:\mathbb{Q}], h(A)\})^{\gamma}$. By the prime number theorem, there is an absolute constant $m \geq 2$ such that for all $Q \geq mC$, we have

$$\sum_{C \leq \ell \leq Q} \log \ell \geq Q/2$$

So with $Q := 4 \max\{mC, \gamma \log N(\mathfrak{q}) + \log c + \log D\}$, we have

$$\sum_{C \leq \ell \leq Q} \log \ell \geq 2 \max\{mC, \gamma \log N(\mathfrak{q}) + \log c + \log D\} > \gamma \log N(\mathfrak{q}) + \log c + \log D \geq \sum_{\ell \mid nD} \log \ell.$$

From $\sum_{C \leq \ell \leq Q} \log \ell > \sum_{\ell \mid nD} \log \ell$, we deduce that there is a prime $C \leq \ell \leq Q$ with $\ell \nmid nD$. By Proposition 7.5, we have

$$\begin{aligned} N(\mathfrak{q}) &\ll_g (\max\{Q, [K:\mathbb{Q}], \log D\})^e \\ &\ll_g (\max\{C, \log N(\mathfrak{q}), [K:\mathbb{Q}], \log D\})^e \\ &\ll_g (\max\{\log N(\mathfrak{q}), [K:\mathbb{Q}], h(A), \log D\})^f, \end{aligned}$$

where $e \geq 1$ and $f \geq 1$ depend only on $g$. If $\log N(\mathfrak{q}) \leq \max\{[K:\mathbb{Q}], h(A), \log D\}$, then

$$N(\mathfrak{q}) \ll_g (\max\{[K:\mathbb{Q}], h(A), \log D\})^f. \tag{7.2}$$

Now suppose that $\log N(\mathfrak{q}) > \max\{[K:\mathbb{Q}], h(A), \log D\}$ and hence $N(\mathfrak{q}) \ll_g (\log N(\mathfrak{q}))^f$. Since $f$ depends only on $g$, we have $N(\mathfrak{q}) \ll_g 1$ and hence (7.2) holds as well.

Theorem 1.4 is now a direct consequence of Theorem 1.2 and the upper bound (7.2) for $N(\mathfrak{q})$.

## 8. Proof of Corollary 1.6

Take any prime $\ell \geq c \cdot \max(\{[K:\mathbb{Q}], h(A), N(\mathfrak{q})\})^{\gamma}$ that is unramified in $K$, where $c$ and $\gamma$ are constants as in Theorem 1.2. After possibly increasing the constants $c$ and $\gamma$, that depend only on $g$, Théorème 1.1 of [GR14] implies that $A$ has a polarization defined over $K$ whose degree is not divisible by $\ell$. This polarization gives rise to an isogeny $\varphi\colon A \to A^{\vee}$ whose degree is not divisible by $\ell$, where $A^{\vee}$ is the dual abelian variety of $A$. Combining the Weil pairing of $A$ with $\varphi$ gives rise to a non-degenerate skew-symmetric form of $\mathbb{Z}_\ell$-modules

$$e_\ell\colon T_\ell(A) \times T_\ell(A) \xrightarrow{\mathrm{id}\times\varphi} T_\ell(A) \times T_\ell(A^{\vee}) \to \mathbb{Z}_\ell(1) \cong \mathbb{Z}_\ell$$

such that $e_\ell(\sigma(P), \sigma(Q)) = \chi_\ell(\sigma) e_\ell(P,Q)$ for all $P, Q \in T_\ell(A)$ and $\sigma \in \mathrm{Gal}_K$, where $\chi_\ell\colon \mathrm{Gal}_K \to \mathbb{Z}_\ell^{\times}$ is the $\ell$-adic cyclotomic character. We thus have

$$\rho_{A,\ell}\colon \mathrm{Gal}_K \to \mathrm{GSp}(T_\ell(A), e_\ell) \cong \mathrm{GSp}_{2g}(\mathbb{Z}_\ell), \tag{8.1}$$

where the last isomorphism depends on a suitable choice of a $\mathbb{Z}_\ell$-basis of $T_\ell(A)$. We have $\chi_\ell(\mathrm{Gal}_K) = \mathbb{Z}_\ell^{\times}$ since $\ell$ is unramified in $K$. So to prove that $\rho_{A,\ell}(\mathrm{Gal}_K) = \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ it suffices to show that $\rho_{A,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$.

From (8.1), we may identify $G_{A,\ell}$ with a closed subgroup of $\mathrm{GSp}_{2g,\mathbb{Q}_\ell}$.

**Lemma 8.1.** *We have $G_{A,\ell} = \mathrm{GSp}_{2g,\mathbb{Q}_\ell}$.*

*Proof.* We have $G_{A,\ell} \subseteq \mathrm{GSp}_{2g,\mathbb{Q}_\ell}$ and hence the rank $r$ of $G_{A,\ell}^{\circ}$ is at most $g+1$, i.e., the rank of $\mathrm{GSp}_{2g,\mathbb{Q}_\ell}$. By assumption, we have a prime ideal $\mathfrak{q} \subseteq \mathcal{O}_K$ for which $A$ has good reduction and for which the group $\Phi_{A,\mathfrak{q}}$ is free abelian of rank $g+1$. By Lemma 2.7(i), we have $g+1 \leq r$. Therefore, $r = g+1$.

Our assumption $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$ and Proposition 2.3(iii) implies that the commutant of $G_{A,\ell}^{\circ}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ agrees with the scalar endomorphisms $\mathbb{Q}_\ell$. The commutant of $\mathrm{GSp}_{2g,\mathbb{Q}_\ell}$ in $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ is also $\mathbb{Q}_\ell$. By Lemma 4.6, we deduce that $G_{A,\ell}^{\circ} = \mathrm{GSp}_{2g,\mathbb{Q}_\ell}$ and hence $G_{A,\ell} = \mathrm{GSp}_{2g,\mathbb{Q}_\ell}$ □

By Lemma 8.1 and (8.1), we have $\mathcal{G}_{A,\ell} = \mathrm{GSp}_{2g,\mathbb{Z}_\ell}$. By Theorem 1.2(d), we have

$$\rho_{A,\ell}(\mathrm{Gal}_K) \supseteq \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)' \supseteq \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)'.$$

It remains to prove that $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)' = \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$.

With notation as in §4.6, we have $\mathcal{S}_{A,\ell} = \mathrm{Sp}_{2g,\mathbb{Z}_\ell}$. By Proposition 4.25(i) and Lemma 4.22, with appropriate $c$ and $\gamma$, it suffices to show that $\mathcal{S}_{A,\ell}(\mathbb{F}_\ell) = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ is generated by elements of order $\ell$. This is indeed true; moreover, $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ is generated by symplectic transvections.

## References


[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. MR574307 (81c:14025) ↑1

[Car08] Xavier Caruso, *Conjecture de l'inertie modérée de Serre*, Invent. Math. **171** (2008), no. 3, 629–699, DOI 10.1007/s00222-007-0091-9 (French, with French summary). MR2372809 ↑5.3

[Cha86] Ching-Li Chai, *Siegel moduli schemes and their compactifications over* **C**, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 231–251. MR861978 ↑2.3

[Con14] Brian Conrad, *Reductive group schemes*, Autour des schémas en groupes. Vol. I, Panor. Synthèses, vol. 42/43, Soc. Math. France, Paris, 2014, pp. 93–444 (English, with English and French summaries). MR3362641 ↑5.6

[CR81] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. I*, John Wiley & Sons, Inc., New York, 1981. With applications to finite groups and orders; Pure and Applied Mathematics; A Wiley-Interscience Publication. MR632548 ↑4.3, 4.6, 4.6

[DMOS82] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin-New York, 1982. MR654325 ↑2.6

[EHK12] Jordan S. Ellenberg, Chris Hall, and Emmanuel Kowalski, *Expander graphs, gonality, and variation of Galois representations*, Duke Math. J. **161** (2012), no. 7, 1233–1275. MR2922374 ↑3.1, 3.1

[Fal86] Gerd Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 9–27. Translated from the German original [Invent. Math. **7**3 (1983), no. 3, 349–366; ibid. **7**5 (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz. MR861971 ↑2.3

[FWG+92] Gerd Faltings, Gisbert Wüstholz, Fritz Grunewald, Norbert Schappacher, and Ulrich Stuhler, *Rational points*, 3rd ed., Aspects of Mathematics, E6, Friedr. Vieweg & Sohn, Braunschweig, 1992. Papers from the seminar held at the Max-Planck-Institut für Mathematik, Bonn/Wuppertal, 1983/1984; With an appendix by Wüstholz. MR1175627 ↑

[GR14] Éric Gaudron and Gaël Rémond, *Polarisations et isogénies*, Duke Math. J. **163** (2014), no. 11, 2057–2108 (French, with English and French summaries). ↑8

[Hen82] Guy Henniart, *Représentations l-adiques abéliennes*, Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981), 1982, pp. 107–126. MR693314 (85d:11070) ↑5.4

[JKZ13] F. Jouve, E. Kowalski, and D. Zywina, *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, Israel J. Math. **193** (2013), no. 1, 263–307, DOI 10.1007/s11856-012-0117-x. MR3038553 ↑7

[Lar10] Michael Larsen, *Exponential generation and largeness for compact p-adic Lie groups*, Algebra Number Theory **4** (2010), no. 8, 1029–1038. MR2832632 ↑3.1

[LP97] Michael Larsen and Richard Pink, *A connectedness criterion for l-adic Galois representations*, Israel J. Math. **97** (1997), 1–10. MR1441234 (98k:11066) ↑2.2, 2.5, 2.5

[LP11] ———, *Finite subgroups of algebraic groups*, J. Amer. Math. Soc. **24** (2011), 1105–1158. ↑3.2

[Lom15] Davide Lombardo, *Explicit open image theorems for abelian varieties with trivial endomorphism ring* (2015). arXiv:1508.01293. ↑1.2

[MW95] D. W. Masser and G. Wüstholz, *Refinements of the Tate conjecture for abelian varieties*, Abelian varieties (Egloffstein, 1993), 1995, pp. 211–223. MR1336608 (97a:11092) ↑2.3

[MR09] Alexander Miller and Victor Reiner, *Differential posets and Smith normal forms*, Order **26** (2009), no. 3, 197–228. MR2544610 ↑5.4

[Nor87] Madhav V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Invent. Math. **88** (1987), no. 2, 257–275. ↑3.1, 4.6

[Pet16] Sebastian Petersen, *Group-theoretical independence of ℓ-adic Galois representations*, Acta Arith. **176** (2016), no. 2, 161–176. MR3566639 ↑4.6

[Rib76] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. MR0457455 (56 #15660) ↑5.1, 5.3, 5.4, 5.4

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331, DOI 10.1007/BF01405086 (French). MR0387283 ↑5.3

[Ser77] ———, *Représentations l-adiques*, Algebraic number theory (Kyoto Internat. Sympos., Res. Inst. Math. Sci., Univ. Kyoto, Kyoto, 1976), 1977, pp. 177–193. MR0476753 (57 #16310) ↑2.6

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401 (French). MR644559 ↑7

[Ser98] ———, *Abelian l-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original. MR1484415 (98g:11066) ↑2.1, 5.4

[Ser00] ———, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000. 1985–1998. MR1730973 (2001e:01037) ↑2.2, 4.2

[SGA7 I] *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin-New York, 1972 (French). Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I); Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. MR0354656 ↑5.1

[UY13] Emmanuel Ullmo and Andrei Yafaev, *Mumford-Tate and generalised Shafarevich conjectures*, Ann. Math. Qué. **37** (2013), no. 2, 255–284, DOI 10.1007/s40316-013-0009-4 (English, with English and French summaries). MR3117743 ↑2.6

[Vas08] Adrian Vasiu, *Some cases of the Mumford-Tate conjecture and Shimura varieties*, Indiana Univ. Math. J. **57** (2008), no. 1, 1–75, DOI 10.1512/iumj.2008.57.3513. MR2400251 ↑2.6

[Win02] J.-P. Wintenberger, *Démonstration d'une conjecture de Lang dans des cas particuliers*, J. Reine Angew. Math. **553** (2002), 1–16. MR1944805 (2003i:11075) ↑1.3, 4.1, 4.6, 4.2, 4.26

[Zyw19] David Zywina, *Families of abelian varieties and large Galois images* (2019). arXiv:1910.14174. ↑1

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
*Email address*: zywina@math.cornell.edu
*URL*: http://www.math.cornell.edu/~zywina