# ABELIAN VARIETIES OVER LARGE ALGEBRAIC FIELDS WITH INFINITE TORSION

DAVID ZYWINA

Abstract. Let $A$ be a non-zero abelian variety defined over a number field $K$ and let $\overline{K}$ be a fixed algebraic closure of $K$. For each element $\sigma$ of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$, let $\overline{K}(\sigma)$ be the fixed field in $\overline{K}$ of $\sigma$. We show that the torsion subgroup of $A(\overline{K}(\sigma))$ is infinite for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ outside of some set of Haar measure zero. This proves the number field case of a conjecture of W.-D. Geyer and M. Jarden.

## 1. Introduction

Let $A$ be a non-zero abelian variety defined over a number field $K$. The Mordell-Weil group $A(K)$ is finitely generated while the group $A(\overline{K})$, with $\overline{K}$ a fixed algebraic closure of $K$, has infinite rank and infinitely many torsion points. It is interesting to bridge this gap and study the structure of the groups $A(L)$ for various infinite algebraic extensions $L$ of $K$. For example, the group $A(K_{\mathrm{ab}})$ has finite torsion if and only if $A$ has no abelian subvarieties with complex multiplication over $K$, where $K_{\mathrm{ab}}$ is the maximal abelian extension of $K$ [Zar87].

Let $\mathrm{Gal}_K$ be the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$. Fix an integer $e \geq 1$. The group $\mathrm{Gal}_K^e$ is profinite and is thus equipped with a unique Haar measure $\mu_K$ for which $\mu_K(\mathrm{Gal}_K^e) = 1$. For each $\sigma = (\sigma_1, \dots, \sigma_e) \in \mathrm{Gal}_K^e$, let $\overline{K}(\sigma)$ be the fixed field of $\sigma_1, \dots, \sigma_e$ in $\overline{K}$. In this paper, we will consider the fields $\overline{K}(\sigma)$ for almost all $\sigma$ in $\mathrm{Gal}_K^e$. By "almost all", we mean for all $\sigma \in \mathrm{Gal}_K^e$ outside of some set with Haar measure 0. For almost all $\sigma \in \mathrm{Gal}_K^e$, the field $\overline{K}(\sigma)$ is pseudo-algebraically closed [FJ05, Theorem 18.6.1] (i.e., every geometrically irreducible variety defined over $\overline{K}(\sigma)$ has a $\overline{K}(\sigma)$-rational point) and the absolute Galois group $\mathrm{Gal}_{\overline{K}(\sigma)}$ is isomorphic to the free profinite group on $e$ generators [FJ05, Theorem 18.5.6].

Frey and Jarden showed that the group $A(\overline{K}(\sigma))$ has infinite rank for almost all $\sigma \in \mathrm{Gal}_K^e$ [FJ74, Theorem 9.1]. We will thus focus on the torsion points of $A(\overline{K}(\sigma))$. Jacobson and Jarden showed that if $e \geq 2$, then $A(\overline{K}(\sigma))_{\mathrm{tors}}$ is finite for almost all $\sigma \in \mathrm{Gal}_K$ [JJ01]. Our main theorem deals with the remaining case $e = 1$.

**Theorem 1.1.** *Let $A$ be a non-zero abelian variety defined over a number field $K$. For all $\sigma \in \mathrm{Gal}_K$ outside a set of Haar measure zero, the group of torsion points in $A(\overline{K}(\sigma))$ is infinite.*

Since there are only countably many abelian varieties defined over $K$, the set of measure zero in Theorem 1.1 can actually be chosen independent of $A$.

For each positive integer $m$ and field extension $L/K$, let $A(L)[m]$ be the $m$-torsion subgroup of $A(L)$. Jacobson and Jarden have also shown that for almost all $\sigma \in \mathrm{Gal}_K$, the group $A(\overline{K}(\sigma))[\ell^\infty] := \bigcup_{n \geq 1} A(\overline{K}(\sigma))[\ell^n]$ is finite for all rational primes $\ell$ [JJ01]. So to prove Theorem 1.1, we will need to demonstrate that for almost all $\sigma \in \mathrm{Gal}_K$, the group $A(\overline{K}(\sigma))[\ell]$ is non-zero for infinitely many primes $\ell$.

A weaker version of Theorem 1.1 was proved by Geyer and Jarden in [GJ05] where they first needed to replace $K$ by some finite extension (which may depend on $A$). Our theorem, with the

2000 *Mathematics Subject Classification.* Primary 14K15; Secondary 11F80.
*Key words and phrases.* Torsion of abelian varieties, Galois representations.

earlier results cited above, completes the proof of the following conjecture of Geyer and Jarden in the case where $K$ is a number field, see [GJ78].

**Conjecture** (Geyer-Jarden)**.** *Let $A$ be a non-zero abelian variety defined over a finitely generated field $K$ and let $e$ be a positive integer. Then for almost all $\sigma \in \mathrm{Gal}_K^e$, we have:*

(a) *If $e = 1$, then $A(\overline{K}(\sigma))_{\mathrm{tors}}$ is infinite.*
(b) *If $e \geq 2$, then $A(\overline{K}(\sigma))_{\mathrm{tors}}$ is finite.*
(c) *The group $A(\overline{K}(\sigma))[\ell^\infty]$ is finite for each prime $\ell$.*

Geyer and Jarden made this conjecture after proving it for the special case of an elliptic curve. Following the approach of our main theorem, one should be able to prove this conjecture in the case where $K$ is a general finitely generated field of characteristic 0 (parts (b) and (c) are already known). The only thing stopping us from doing so is the lack of a convenient reference for the image of Galois representations over such fields.

1.1. **Galois representations.** Throughout this section, we will let $A$ be an abelian variety of dimension $g \geq 1$ defined over a number field $K$. For each prime $\ell$, the group $A(\overline{K})[\ell]$ is isomorphic to $\mathbb{F}_\ell^{2g}$ and has an action of $\mathrm{Gal}_K$ that respects the group structure. This action thus defines a Galois representation

$$\rho_{A,\ell} \colon \mathrm{Gal}_K \to \mathrm{Aut}(A(\overline{K})[\ell]) \cong \mathrm{GL}_{2g}(\mathbb{F}_\ell).$$

Observe that for $\sigma \in \mathrm{Gal}_K$, we have $A(\overline{K}(\sigma))[\ell] \neq 0$ if and only if the matrix $\rho_{A,\ell}(\sigma) \in \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ has 1 as an eigenvalue. Theorem 1.1 will be a straightforward application of the following proposition.

**Proposition 1.2.** *Let $A$ be a non-zero abelian variety defined over a number field $K$. Then there is a finite Galois extension $L/K$, a set $\mathcal{S}$ of rational primes with positive density, and a positive constant $c$ such that that the following hold:*

(a) *For each prime $\ell \in \mathcal{S}$ and $\beta \in \mathrm{Gal}_K$, we have*

$$\frac{|\{h \in \rho_{A,\ell}(\beta\,\mathrm{Gal}_L) : \det(I-h) = 0\}|}{|\rho_{A,\ell}(\beta\,\mathrm{Gal}_L)|} \geq \frac{c}{\ell}.$$

(b) *The homomorphism $\prod_{\ell\in\mathcal{S}} \rho_{A,\ell} \colon \mathrm{Gal}_L \to \prod_{\ell\in\mathcal{S}} \rho_{A,\ell}(\mathrm{Gal}_L)$ is surjective.*

Let us now explain how Theorem 1.1 follows from Proposition 1.2. We first define the measure $\mu = [L:K]\mu_K$ on $\mathrm{Gal}_K$, i.e., the Haar measure on $\mathrm{Gal}_K$ such that $\mu(\mathrm{Gal}_K) = [L:K]$. Now fix any element $\beta \in \mathrm{Gal}_K$. Since $\mu(\beta\,\mathrm{Gal}_L) = 1$, we may view $\beta\,\mathrm{Gal}_L$ with measure $\mu$ as a probability space. For each prime $\ell \in \mathcal{S}$, define the set $U_\ell := \{\sigma \in \beta\,\mathrm{Gal}_L : A(\overline{K}(\sigma))[\ell] \neq 0\}$. Since $A(\overline{K}(\sigma))[\ell] \neq 0$ is equivalent to $\det(I - \rho_{A,\ell}(\sigma)) = 0$, the set $U_\ell$ is thus $\mu$-measurable with

$$\mu(U_\ell) = |\{h \in \rho_{A,\ell}(\beta\,\mathrm{Gal}_L) : \det(I-h) = 0\}|/|\rho_{A,\ell}(\beta\,\mathrm{Gal}_L)|.$$

Using Proposition 1.2(b), we find that the map $\prod_{\ell\in\mathcal{S}} \rho_{A,\ell} \colon \beta\,\mathrm{Gal}_L \to \prod_{\ell\in\mathcal{S}} \rho_{A,\ell}(\beta\,\mathrm{Gal}_L)$ is surjective, and thus the $U_\ell$ are $\mu$-independent subsets of $\beta\,\mathrm{Gal}_L$ (i.e., $\mu(\cap_{\ell\in I} U_\ell) = \prod_{\ell\in I} \mu(U_\ell)$ for any finite subset $I$ of $\mathcal{S}$). By Proposition 1.2(a), we have

$$\sum_{\ell\in\mathcal{S}} \mu(U_\ell) \geq c \sum_{\ell\in\mathcal{S}} \frac{1}{\ell} = +\infty$$

where the divergence of the series uses that $\mathcal{S}$ has positive density. The second Borel-Cantelli lemma now implies that the set $\bigcap_{n=1}^\infty \bigcup_{\ell\geq n,\, \ell\in\mathcal{S}} U_\ell$ has $\mu$-measure 1. Equivalently, the set

$$\big\{\sigma \in \beta\,\mathrm{Gal}_L : A(\overline{K}(\sigma))[\ell] \neq 0 \text{ for infinitely many primes } \ell \in \mathcal{S}\big\}$$

has $\mu$-measure 1. By combining the $[L:K]$ cosets of $\mathrm{Gal}_L$ in $\mathrm{Gal}_K$, we find that the set

$$\big\{\sigma \in \mathrm{Gal}_K : A(\overline{K}(\sigma))[\ell] \neq 0 \text{ for infinitely many primes } \ell \in \mathcal{S}\big\}$$

has $\mu$-measure $[L:K]$. Theorem 1.1 follows by recalling that $\mu_K = [L:K]^{-1}\mu$.

**Acknowledgements.** Many thanks to Moshe Jarden for introducing his and Geyer's conjecture to me and suggesting that I should study it. Thanks to Moshe and Andrew Obus for their corrections. Thanks to the referee for his or her careful reading and suggestions.

## 2. Counting points

In this section, we give a quick application of the Weil conjectures. The essential feature of the bound in the following theorem is its uniformity; its proof requires a bound for the sum of Betti numbers due to Katz (which builds on estimates of Bombieri).

**Theorem 2.1.** *Let $V \subseteq \mathbb{A}^n_{\mathbb{F}_q}$ with $n > 1$ be a closed subvariety defined by the simultaneous vanishing of $r$ polynomials $f_1, \dots, f_r$ in $\mathbb{F}_q[x_1, \dots, x_n]$, each of degree at most $d$. Let $V_1, \dots, V_m$ be the irreducible components of $V_{\overline{\mathbb{F}}_q}$ which have the same dimension as $V$. Then*

$$|V(\mathbb{F}_q)| \leq mq^{\dim V} + 6(3+rd)^{n+1}2^r q^{\dim V - 1/2}.$$

*If the components $V_1, \dots, V_m$ are all defined over $\mathbb{F}_q$, then*

$$\Big| |V(\mathbb{F}_q)| - mq^{\dim V} \Big| \leq 6(3+rd)^{n+1}2^r q^{\dim V - 1/2}.$$

*Proof.* Set $N = \dim V$ and fix a prime $\ell$ that does not divide $q$. By the Grothendieck-Lefschetz theorem [Del77, II Théorème 3.2], we have

$$|V(\mathbb{F}_q)| = \sum_{i=0}^{2N} (-1)^i \operatorname{Tr}(F^* | H^i_c(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell))$$

where $F^*$ is the linear transformation arising from the Frobenius morphism which acts on the $\ell$-adic cohomology groups with compact support. From Deligne, we know that the eigenvalues of $F^*$ acting on $H^i_c(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ have absolute value at most $q^{i/2}$ under any embedding $\overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$ (see the comment following Théorème 1 of [Del80]). Therefore,

$$\begin{aligned} &\Big| |V(\mathbb{F}_q)| - \operatorname{Tr}(F^* | H^{2N}_c(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)) \Big| \\ &\leq \sum_{i=0}^{2N-1} q^{i/2} \dim H^i_c(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) \\ &\leq q^{N-1/2} \sum_{i=0}^{2N-1} \dim H^i_c(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)) \\ &\leq q^{N-1/2} \cdot 6(3+rd)^{n+1}2^r \end{aligned} \tag{2.1}$$

where the last inequality follows from the corollary of Theorem 1 in [Kat01].

First suppose that the components $V_1, \dots, V_m$ are all defined over $\mathbb{F}_q$. Choose a closed subvariety $Z$ with $\dim Z < \dim V = N$ such that $U := V - Z$ is the disjoint union of smooth, open and geometrically irreducible subvarieties $U_1, \dots, U_m$ of $V$. By Poincaré duality (for example, as in Corollary 11.2 of [Mil80]), we have an isomorphism between the $\mathbb{Q}_\ell$-vector space $H^{2N}_c(U_{i,\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ and the dual of $H^0(U_{i,\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell(1))$ which respects the Frobenius actions.

We have an exact sequence

$$H^{2N-1}_c(Z_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) \to H^{2N}_c(U_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) \to H^{2N}_c(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) \to H^{2N}_c(Z_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell),$$

cf. Remark 1.30 of [Mil80]. The inequality $\dim Z < N$ implies that $H^i_c(Z_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) = 0$ for all $i > 2(N-1)$, so we have an isomorphism $H^{2N}_c(U_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) \xrightarrow{\sim} H^{2N}_c(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ with compatible linear maps $F^*$. We have $H^{2N}_c(U_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) = \oplus_{i=1}^m H^{2N}_c(U_{i,\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$. Using that $U_i$ is smooth and absolutely irreducible, Poincaré duality gives an isomorphism $H^{2N}_c(U_{i,\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) = \mathbb{Q}_\ell(-N)$ for all $i$. Recall that $\mathbb{Q}_\ell(-N)$

is the space $\mathbb{Q}_\ell$ with $F^*$ acting on it by multiplication by $q^N$. Therefore, $H_c^{2N}(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ is an $m$-dimensional $\mathbb{Q}_\ell$-vector space and $F^*$ acts on it as multiplication by $q^N$. By (2.1), we deduce that

$$\Big| |V(\mathbb{F}_q)| - mq^N \Big| \leq 6(3+rd)^{n+1}2^r q^{N-1/2}.$$

Now suppose we are in the general case. We have just shown that $\dim_{\mathbb{Q}_\ell} H_c^{2N}(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell) = m$ (one can first base extend by a finite extension of $\mathbb{F}_q$ over which all of the $V_i$ are defined). The eigenvalues of $F^*$ acting on $H_c^{2N}(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ have absolute value at most $q^N$ by Deligne [Del80], so $|\operatorname{Tr}(F^*|H_c^{2N}(V_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell))| \leq mq^N$ and the theorem follows. □

*Remark* 2.2. For the main application in this paper, it would suffice to have a version of Theorem 2.1 where the term $6(3+rd)^{n+1}2^r$ is replaced by any constant depending only on $r$, $d$ and $n$. Such bounds can be readily deduced from the Weil-Lang bounds instead of the more sophisticated cohomological machinery. The above explicit version will be used in future work.

## 3. Proof of Proposition 1.2

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

$$\rho_{A,\ell} \colon \operatorname{Gal}_K \to \operatorname{Aut}(A(\overline{K})[\ell]) \cong \operatorname{GL}_{2g}(\mathbb{F}_\ell)$$

be the Galois representation coming from the Galois action on the $\ell$-torsion points of $A$. For each $\ell$, let $\rho_{A,\ell^\infty} \colon \operatorname{Gal}_K \to \operatorname{Aut}(A(\overline{K})[\ell^\infty]) \cong \operatorname{GL}_{2g}(\mathbb{Z}_\ell)$ be the $\ell$-adic representation which describes the Galois action on $A(\overline{K})[\ell^\infty]$.

For a finite extension $K'$ of $K$ and a maximal ideal $\mathfrak{p}$ of $\mathcal{O}_{K'}$ for which $A_{K'}$ has good reduction, let $P_{A,\mathfrak{p}}(x) \in \mathbb{Z}[x]$ be the characteristic polynomial of Frobenius for the reduction of $A$ modulo $\mathfrak{p}$; it is the unique polynomial in $\mathbb{Z}[x]$ such that $P_{A,\mathfrak{p}}(x) = \det(xI - \rho_{A,\ell^\infty}(\operatorname{Frob}_\mathfrak{p}))$ for all primes $\ell$ satisfying $\mathfrak{p} \nmid \ell$.

### 3.1. Image of Galois modulo $\ell$.

**Theorem 3.1** (Serre)**.** *There is a finite Galois extension $L$ of $K$ and positive integers $N$, $r$ and $\kappa$ such that the following hold:*

(a) *For all $\ell \geq \kappa$, there is a connected, reductive subgroup $H_\ell$ of $\operatorname{GL}_{2g,\mathbb{F}_\ell}$ of rank $r$ such that $\rho_{A,\ell}(\operatorname{Gal}_L)$ is contained in $H_\ell(\mathbb{F}_\ell)$ and the index $[H_\ell(\mathbb{F}_\ell) : \rho_{A,\ell}(\operatorname{Gal}_L)]$ divides $N$. Furthermore, $H_\ell$ contains the group $\mathbb{G}_m$ of homotheties.*

(b) *The homomorphism $\prod_\ell \rho_{A,\ell} \colon \operatorname{Gal}_L \to \prod_\ell \rho_{A,\ell}(\operatorname{Gal}_L)$ is surjective.*

The above theorem is a consequence of results of J.-P. Serre presented in his 1985-1986 course at the Collège de France, see [Ser86] for an overview of the course[1]. Detailed sketches were supplied in letters that have since been published in his collected papers; see the beginning of [Ser00], in particular the letters to M.-F. Vignéras [Ser00, #137] and K. Ribet [Ser00, #138] contain information on parts (a) and (b), respectively. The paper [Win02] contains a detailed construction of the reductive groups $H_\ell$ (where they are denoted by $G(\ell)^{\mathrm{alg}}$). A proof of part (b) can now be found in [Ser13]. For the rest of §3, we will use the notation of Theorem 3.1.

**Lemma 3.2.** *There is a finite Galois extension $M$ of $\mathbb{Q}$ such that if $\ell$ is a sufficiently large prime that splits completely in $M$, then the following hold:*

(a) *The reductive group $H_\ell$ is split.*

[1]The referee has pointed out that Eva Bayer-Fluckiger's notes for the course can be found at http://alg-geo.epfl.ch/~bayer/html/notes.html

(b) *Let $x_{i,j}$ $(1 \le i,j \le 2g)$ and $y$ be independent variables. We may identify $\mathrm{GL}_{2g,\mathbb{F}_\ell}$ with the closed subvariety of $\mathrm{Spec}(\mathbb{F}_\ell[x_{i,j},y]) = \mathbb{A}^n_{\mathbb{F}_\ell}$, with $n = 4g^2+1$, defined by the equation $\det(x_{i,j})\cdot y = 1$ (that is, identify a matrix $B$ with the $n$-tuple $((B_{i,j}), 1/\det(B))$).*

*Let $T$ be a split maximal torus of $H_\ell$. Then the torus $T$, viewed as a closed subvariety of $\mathbb{A}^n_{\mathbb{F}_\ell}$, is defined by at most $C_1$ polynomials of degree at most $C_2$, where $C_1$ and $C_2$ are constants that do not depend on $\ell$.*

*Proof.* Define the scheme $\mathbb{A}^{2g}_* = \mathbb{A}^{2g-1}\times\mathbb{G}_m$, and let $\mathrm{cl}\colon \mathrm{GL}_{2g}\to\mathbb{A}^{2g}_*$ be the morphism that associates to a matrix $B$ the $2g$-tuple $(a_1,\dots,a_{2g})$ where $\det(xI-B) = x^{2g}+a_1x^{2g-1}+\ldots+a_{2g-1}x+a_{2g}$. If $G$ is a connected reductive subgroup of $\mathrm{GL}_{2g,k}$ for a field $k$, then $\mathrm{cl}(G)$ is a closed irreducible subvariety of $\mathbb{A}^{2g}_{*,k}$ whose dimension is the same as the rank of $G$ (we have $\mathrm{cl}(G)=\mathrm{cl}(T)$, where $T$ is a maximal torus of $G$, so it suffices to consider a torus).

There is a finite extension $L'$ of $L$ such that the Zariski closure of $\rho_{A,\ell^\infty}(\mathrm{Gal}_{L'})$ in $\mathrm{GL}_{2g,\mathbb{Q}_\ell}$ is a *connected* algebraic group for each $\ell$, cf. [Ser00, p.18] and [LP97]. Let $\mathcal{P}$ be the Zariski closure in $\mathbb{A}^{2g}_{*,\mathbb{Q}}$ of the set of $2g$-tuples $P_\mathfrak{p} := (a_1,\dots,a_{2g})\in\mathbb{Z}^{2g}$ where $\mathfrak{p}$ varies over the maximal ideals of $\mathcal{O}_{L'}$ for which $A$ has good reduction and $P_{A,\mathfrak{p}}(x)$ equals $x^{2g}+a_1x^{2g-1}+\ldots+a_{2g-1}x+a_{2g}$.

Serre has shown that, after choosing an integral model of $\mathcal{P}$, we have $\mathrm{cl}(H_\ell) = \mathcal{P}_{\mathbb{F}_\ell}$ for all sufficiently large $\ell$, cf. [Ser00, #137 §6] where $\mathcal{P}$ is denoted $P_1$. In particular, the rank of $H_\ell$ agrees with $\dim(\mathcal{P})$ for $\ell$ large enough (this is how $r$ is determined in the proof of Thereom 3.1).

Let $d$ be the maximum number of distinct roots $P_{A,\mathfrak{p}}(x)$ has in $\overline{\mathbb{Q}}$ as $\mathfrak{p}$ varies over the maximal ideals of $\mathcal{O}_{L'}$ for which $A$ has good reduction. For $\ell$ large enough so that $H_\ell$ is defined, we define $d_\ell$ to be the maximum number of distinct roots $\det(xI-h)\in\overline{\mathbb{F}}_\ell[x]$ has as $h$ varies over the elements of $H_\ell(\overline{\mathbb{F}}_\ell)$. For $\ell$ large, the equality $\mathrm{cl}(H_\ell)=\mathcal{P}_{\mathbb{F}_\ell}$ implies that $d=d_\ell$ (the polynomials with less than $d$ roots are described by a codimension 1 subvariety of $\mathcal{P}$). By the Chebotarev density theorem, the set of maximal ideals $\mathfrak{p}\subseteq\mathcal{O}_{L'}$ for which $P_{A,\mathfrak{p}}(x)$ has $d$ distinct roots has density 1. Let $\mathfrak{q}$ be a maximal ideal of $\mathcal{O}_{L'}$ for which $A$ has good reduction and $P_{A,\mathfrak{q}}(x)$ has $d$ distinct roots. There is a constant $c_1$ such that $P_{A,\mathfrak{q}}(x)\equiv\det(xI-\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{q}))\in\mathbb{F}_\ell[x]$ has $d=d_\ell$ distinct roots for all $\ell\ge c_1$. Let $M$ be the splitting field of $P_{A,\mathfrak{q}}(x)$ over $\mathbb{Q}$. For the rest of the proof, suppose that $\ell$ is a prime greater than $c_1$ for which $\ell$ splits completely in $M$, and hence $\det(xI-\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{q}))\in\mathbb{F}_\ell[x]$ has $d$ distinct roots in $\mathbb{F}_\ell$.

Let $t_\mathfrak{q}\in H_\ell(\mathbb{F}_\ell)$ be the semisimple part of a representative of the conjugacy class $\rho_{A,\ell}(\mathrm{Frob}_\mathfrak{q})$. Let $T$ be a maximal torus of $H_\ell$ which contains $t_\mathfrak{q}$; we will show that $T$ is split (as a torus over $\mathbb{F}_\ell$). Let $X(T)$ be the group of characters $T_{\overline{\mathbb{F}}_\ell}\to\mathbb{G}_{m,\overline{\mathbb{F}}_\ell}$ and let $\iota\colon T\to\mathrm{GL}_{2g,\mathbb{F}_\ell}$ the inclusion morphism. For each character $\alpha\in X(T)$, define the vector space

$$V(\alpha) = \{v\in\overline{\mathbb{F}}_\ell^{2g} : \iota(t)\cdot v = \alpha(t)v \text{ for all } t\in T(\overline{\mathbb{F}}_\ell)\}.$$

We say that $\alpha$ is a *weight* of $\iota$ if $V(\alpha)\neq 0$, and we will denote the (finite) set of such weights by $\Omega$. We have $\overline{\mathbb{F}}_\ell^{2g} = \oplus_{\alpha\in\Omega}V(\alpha)$ since $\iota(T)$ is a diagonalizable subgroup of $\mathrm{GL}_{2g,\mathbb{F}_\ell}$. For each $t\in T(\overline{\mathbb{F}}_\ell)$, we thus have

$$\det(xI-\iota(t)) = \prod_{\alpha\in\Omega}(x-\alpha(t))^{\dim_{\overline{\mathbb{F}}_\ell}V(\alpha)}.$$

Since every semisimple element of $H_\ell$ is conjugate to an element in $T$, we find that $|\Omega|=d_\ell$ and hence $|\Omega|=d$. Since $P_{A,\mathfrak{q}}(x)\equiv\det(xI-t_\mathfrak{q})\in\mathbb{F}_\ell[x]$ has $d$ distinct roots in $\mathbb{F}_\ell$, we deduce that $\alpha(t_\mathfrak{q})$ belongs to $\mathbb{F}_\ell$ for each $\alpha\in\Omega$ and that $\alpha_1(t_\mathfrak{q})\neq\alpha_2(t_\mathfrak{q})$ for all distinct $\alpha_1,\alpha_2\in\Omega$.

For $\sigma\in\mathrm{Gal}_{\mathbb{F}_\ell}$ and $\alpha\in X(T)$, we define ${}^\sigma\alpha$ to be the character of $T$ for which $\sigma(\alpha(t)) = {}^\sigma\alpha(\sigma(t))$ for all $t\in T(\overline{\mathbb{F}}_\ell)$; this defines an action of the Galois group $\mathrm{Gal}_{\mathbb{F}_\ell}=\mathrm{Gal}(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$ on the character group $X(T)$. Since $\iota$ is defined over $\mathbb{F}_\ell$, $\mathrm{Gal}_{\mathbb{F}_\ell}$ also acts on the set $\Omega$. Take any $\alpha\in\Omega$ and $\sigma\in\mathrm{Gal}_{\mathbb{F}_\ell}$. Since $\alpha(t_\mathfrak{q})$ and $t_\mathfrak{q}$ are defined over $\mathbb{F}_\ell$, we have $\alpha(t_\mathfrak{q}) = \sigma(\alpha(t_\mathfrak{q})) = {}^\sigma\alpha(\sigma(t_\mathfrak{q})) = {}^\sigma\alpha(t_\mathfrak{q})$. Since $\beta(t_\mathfrak{q})$

takes distinct values for different $\beta \in \Omega$, we deduce that ${}^{\sigma}\alpha = \alpha$. Therefore, the action of $\mathrm{Gal}_{\mathbb{F}_\ell}$ on $\Omega$ is trivial. The group $X(T)$ is generated by $\Omega$ since $\iota$ is a faithful embedding (using the morphism $\prod_{\alpha\in\Omega}\alpha\colon T \to \mathbb{G}^n_{m,\mathbb{F}_\ell}$ with $n = |\Omega|$, one need only note that the character group of the full diagonal torus in $\mathrm{GL}_{m,\mathbb{F}_\ell}$ is generated by the $m$ obvious characters). Therefore, the $\mathrm{Gal}_{\mathbb{F}_\ell}$ action on $X(T)$ is also trivial. That $\mathrm{Gal}_{\mathbb{F}_\ell}$ acts trivially on $X(T)$ implies that $T$ is a split torus [Bor91, III §8.12]. This completes the proof of part (a).

We will now prove part (b). Since all split maximal tori of $H_\ell$ are conjugate by an element of $H_\ell(\mathbb{F}_\ell)$ [Spr09, §15.2.6], and conjugation does not change the number or degree of the equations needed to define the torus, we need only verify (b) for our specific split torus $T$. Similarly by conjugating $H_\ell$ by an element of $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$, we may assume that the split torus $T$ lies in the diagonal torus of $\mathrm{GL}_{2g,\mathbb{F}_\ell}$. Moreover, we may assume that the inclusion $T \to \mathrm{GL}_{2g,\mathbb{F}_\ell}$ maps $t \in T$ to the diagonal matrix

$$\begin{pmatrix} \alpha_1(t)I_{m_1} & & & \\ & \alpha_2(t)I_{m_2} & & \\ & & \ddots & \\ & & & \alpha_d(t)I_{m_d} \end{pmatrix}$$

where $\Omega = \{\alpha_1, \dots, \alpha_d\}$ and $m_i = \dim_{\overline{\mathbb{F}}_\ell} V(\alpha_i)$. For each $1 \le s \le d$, define $e_s = 1 + \sum_{1\le k<s} m_k$. The torus $T$ thus consists of the matrices $B \in \mathrm{GL}_{2g,\mathbb{F}_\ell}$ for which $B_{i,j} = 0$ for $i \ne j$, $B_{i,i} = B_{j,j}$ if $e_s \le i < j < e_{s+1}$ for $1 \le s < d$, and $\prod_{1\le i\le d} B_{e_i,e_i}^{n_i} = 1$ whenever $\prod_{1\le i\le d}\alpha_i^{n_i} = 1$ with $n_i \in \mathbb{Z}$. It thus suffices to prove that subgroup $\mathcal{N}$ of $\mathbb{Z}^d$ consisting of those $(n_1, \dots, n_d)$ for which $\prod_{1\le i\le d}\alpha_i^{n_i} = 1$ is generated by the finite set $\{(n_1, \dots, n_d) : |n_i| \le C\}$ where $C$ is some constant that does not depend on $\ell$.

One of the ingredients in Serre's proof of $\mathrm{cl}(H_\ell) = \mathcal{P}_{\mathbb{F}_\ell}$ for large $\ell$ is that we can lift $H_\ell$ to a reductive group $\mathcal{H}_\ell$ over a field $F$ of characteristic 0 [Ser00, #137 §6]. (Moreover for $\ell$ sufficiently large, the Zariski closure of $\rho_{A,\ell^\infty}(\mathrm{Gal}_{L'})$ in $\mathrm{GL}_{2g,\mathbb{Z}_\ell}$ is a reductive group scheme $\mathscr{H}_\ell$ whose special fiber is $H_\ell$; see [Win02, §2] and use [Win02, §3.4.1] to identify the special fiber with Serre's group. Then the generic fiber of $\mathscr{H}_\ell$ gives the desired lift $\mathcal{H}_\ell$.) By choosing the lift appropriately, one can assume that there is an embedding $F \hookrightarrow \mathbb{C}$ such that the reductive group $\mathcal{H}_{\ell,\mathbb{C}} \subseteq \mathrm{GL}_{2g,\mathbb{C}}$ is conjugate in $\mathrm{GL}_{2g,\mathbb{C}}$ to one of a *finite number* of reductive groups (which do not depend on $\ell$). This is a key step in [Ser00, #137 §6]; the idea is that there is a natural way to lift the central torus of $H_\ell$ that does not depend on $\ell$ (the central torus for $\ell$ sufficiently large enough is determined by the endomorphism ring of $A_{\overline{K}}$), then there are finitely many possibilities for the semisimple part of the lift. It is this finiteness of reductive groups that allows us to pick a constant $C$ that depends only on these finitely many reductive groups, and is hence independent of $\ell$. □

3.2. **Proof of Proposition 1.2.** With notation as in §3.1, we fix a conjugacy class $C$ of $\mathrm{Gal}(L/K)$. We define $d_C$ to be the maximum number of distinct roots $P_{A,\mathfrak{p}}(x^N)$ has in $\overline{\mathbb{Q}}$ as $\mathfrak{p}$ varies over the non-zero prime ideals of $\mathcal{O}_K$ such that $A$ has good reduction at $\mathfrak{p}$, $L$ is unramified at $\mathfrak{p}$, and $(\mathfrak{p}, L/K) = C$; fix such a prime $\mathfrak{p}_C$ for which this maximum occurs.

Let $\mathcal{S}$ be the set of primes $\ell$ that satisfy the following conditions:

- $\ell \ge \kappa$ and $\mathfrak{p}_C \nmid \ell$ for each conjugacy class $C$ of $\mathrm{Gal}(L/K)$,
- $\ell$ splits completely in $M$,
- For each conjugacy class $C$ of $\mathrm{Gal}(L/K)$, $P_{A,\mathfrak{p}_C}(x^N) \bmod \ell \in \mathbb{F}_\ell[x]$ has $d_C$ distinct roots in $\mathbb{F}_\ell$.

The set $\mathcal{S}$, after possibly removing a finite number of primes, will be the set of Proposition 1.2. The set $\mathcal{S}$ has positive density by the Chebotarev density theorem. After removing a finite number of primes from $\mathcal{S}$, by Lemma 3.2(a) we may assume that $H_\ell$ is split for all $\ell \in \mathcal{S}$.

For the rest of this section, fix a prime $\ell \in \mathcal{S}$ and an element $\beta \in \mathrm{Gal}_K$. Let $C$ be the conjugacy class of $\mathrm{Gal}(L/K) = \mathrm{Gal}_K / \mathrm{Gal}_L$ containing the coset $\beta \mathrm{Gal}_L$. Choose a matrix $B \in \rho_{A,\ell}(\beta \mathrm{Gal}_L)$ that lies in the conjugacy class $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}_C})$. Since the index of $\rho_{A,\ell}(\mathrm{Gal}_L)$ in $H_\ell(\mathbb{F}_\ell)$ divides $N$, we have $h^N \in \rho_{A,\ell}(\mathrm{Gal}_L)$ for all $h \in H_\ell(\mathbb{F}_\ell)$. In particular, $Bh^N \in \rho_{A,\ell}(\beta \mathrm{Gal}_L)$ for every $h \in H_\ell(\mathbb{F}_\ell)$. Therefore,

$$\bigcup_{\substack{T \text{ split maximal} \\ \text{torus of } H_\ell}} \left\{ Bt^N : \begin{array}{l} t \in T(\mathbb{F}_\ell) \text{ such that } \det(I - Bt^N) = 0 \\ \text{and } t^N \text{ is regular in } H_\ell \end{array} \right\} \tag{3.1}$$

is a subset of $\{h \in \rho_{A,\ell}(\beta \mathrm{Gal}_L) : \det(I - h) = 0\}$ (with *regular* defined as in [Bor91, IV §12]). Suppose that $t_1$ and $t_2$ are semisimple elements of $H_\ell(\mathbb{F}_\ell)$ with $t_1^N$ and $t_2^N$ regular in $H_\ell$. If $Bt_1^N = Bt_2^N$, then $t_1^N = t_2^N$, and since they are regular they must lie in a unique maximal torus of $H_\ell$; in particular, $t_1$ and $t_2$ lie in the same (unique) maximal torus of $H_\ell$. Therefore, (3.1) is actually a disjoint union.

If $h$ is an element of the rank $r$ torus $T$, then there are at most $N^r$ elements $t$ in $T$ for which $t^N = h$. We thus have

$$\begin{aligned} &|\{h \in \rho_{A,\ell}(\beta \mathrm{Gal}_L) : \det(I - h) = 0\}| \\ \geq &\frac{1}{N^r} \sum_T |\{t \in T(\mathbb{F}_\ell) : \det(I - Bt^N) = 0 \text{ and } t^N \text{ is regular in } H_\ell\}| \end{aligned} \tag{3.2}$$

where the sum is over all split maximal tori $T$ of $H_\ell$. The key technical lemma of this paper is the following:

**Lemma 3.3.** *There is a constant $c$ not depending on the choice of $B$ or $\ell$ such that*

$$|\{t \in T(\mathbb{F}_\ell) : \det(I - Bt^N) = 0 \text{ and } t^N \text{ is regular in } H_\ell\}|$$

*is greater than $\ell^{r-1} - c\ell^{r-3/2}$ for all split maximal tori $T$ of $H_\ell$.*

Assuming the validity of Lemma 3.3, let us finish the proof of Proposition 1.2. Combining (3.2) with Lemma 3.3, we find that $|\{h \in \rho_{A,\ell}(\beta \mathrm{Gal}_L) : \det(I - h) = 0\}|$ is greater or equal to $\frac{1}{N^r} \sum_T \left(\ell^{r-1} - c\ell^{r-3/2}\right)$ where the sum is over the split maximal tori of $H_\ell$.

Fix a split maximal torus $T$ of $H_\ell$ (such a torus exists by our choice of $\mathcal{S}$). All split maximal tori of $H_\ell$ are conjugate to $T$ by some element of $H_\ell(\mathbb{F}_\ell)$ [Spr09, §15.2.6]. Let $\mathcal{N}$ be the group of elements of $H_\ell(\mathbb{F}_\ell)$ that normalize the torus $T$. The group $\mathcal{N}$ clearly contains $T(\mathbb{F}_\ell)$ and the quotient $W := \mathcal{N}/T(\mathbb{F}_\ell)$ is isomorphic to a subgroup of the Weyl group $W(H_\ell)$. Therefore, there are exactly $|H_\ell(\mathbb{F}_\ell)|/|\mathcal{N}| = |H_\ell(\mathbb{F}_\ell)||W|^{-1}(\ell - 1)^{-r}$ split maximal tori of $H_\ell$. Combining this with our previous estimate, we have

$$\begin{aligned} &|\{h \in \rho_{A,\ell}(\beta \mathrm{Gal}_L) : \det(I - h) = 0\}| \\ &\geq N^{-r} |H_\ell(\mathbb{F}_\ell)||W|^{-1}(\ell - 1)^{-r} \cdot \left(\ell^{r-1} - c\ell^{r-3/2}\right) \\ &\geq N^{-r} |H_\ell(\mathbb{F}_\ell)||W(H_\ell)|^{-1}(1 - c\ell^{-1/2}) \cdot \ell^{-1}. \end{aligned}$$

Using that $|H_\ell(\mathbb{F}_\ell)| \geq |\rho_{A,\ell}(\mathrm{Gal}_L)| = |\rho_{A,\ell}(\beta \mathrm{Gal}_L)|$, we find that

$$\frac{|\{h \in \rho_{A,\ell}(\beta \mathrm{Gal}_L) : \det(I - h) = 0\}|}{|\rho_{A,\ell}(\beta \mathrm{Gal}_L)|} \geq \frac{1}{N^r \cdot |W(H_\ell)|} \frac{(1 - c\ell^{-1/2})}{\ell}.$$

Since $H_\ell$ is a reductive group of rank $r$, there is a lower bound for $|W(H_\ell)|^{-1}$ that depends only on $r$ (more precisely, $W(H_\ell)$ depends only on the Lie type of $H_\ell$ and there are only finite many for a given $r$). Proposition 1.2(a) is now immediate after removing a finite number of primes from $\mathcal{S}$. Proposition 1.2(b) is a consequence of Theorem 3.1(b) and our choice of $L$.

3.3. **Proof of Lemma 3.3.** Fix a split maximal torus $T$ of $H_\ell$. Let $W$ be the closed subvariety of $T$ defined by the equation $\det(I - Bt^N) = 0$ where $t \in T$. By Theorem 3.1(a), $T$ contains the group $\mathbb{G}_m$ of homotheties. Let $\varphi\colon W \to T/\mathbb{G}_m$ be the morphism obtained by composing the inclusion $W \hookrightarrow T$ with the quotient homomorphism. Take any $t \in T(\overline{\mathbb{F}}_\ell)$, and let $\bar{t}$ be the corresponding coset in $T/\mathbb{G}_m$. Then $\varphi^{-1}(\bar{t}) = \{\lambda t : \lambda \in \overline{\mathbb{F}}_\ell,\ \det(I - \lambda^N Bt^N) = 0\}$, and hence $|\varphi^{-1}(\bar{t})|$ equals the number of distinct roots of $\det(x^N - Bt^N)$ in $\overline{\mathbb{F}}_\ell$. Let $d$ be the integer such that for a generic $t'$ in $T/\mathbb{G}_m$, $\varphi^{-1}(t')$ has $d$ distinct points (counted without multiplicity).

**Lemma 3.4.** *Assuming $\ell \in \mathcal{S}$ is sufficiently large, there exists an element $t \in T(\mathbb{F}_\ell)$ such that $\varphi^{-1}(\bar{t})$ consists of $d$ distinct points each belonging to $W(\mathbb{F}_\ell)$.*

*Proof.* By our choice of $\mathfrak{p}_C$, the polynomial $P_{A,\mathfrak{p}_C}(x^N)$ has degree $d_C$. Our set $\mathcal{S}$ was chosen so that the polynomial

$$P_{A,\mathfrak{p}_C}(x^N) \equiv \det(x^N I - \rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}_C})) = \det(x^N I - B) \in \mathbb{F}_\ell[x]$$

has $d_C$ distinct roots all of which belong to $\mathbb{F}_\ell$, see §3.2. In terms of our morphism $\varphi$, this shows that $\varphi^{-1}(\bar{I})$ consists of $d_C$ points each belonging to $W(\mathbb{F}_\ell)$. So $d_C \le d$ and it thus suffices to prove equality.

Let $V$ be the subvariety of $T$ consisting of those $t \in T$ for which $\det(x^N I - Bt^N)$ has strictly less than $d$ distinct roots in an algebraically closed field. Since $V$ is a proper subvariety of $T$; it has dimension at most $\dim T - 1 = r - 1$. Using Lemma 3.2(b) and Theorem 2.1, we find that $|V(\mathbb{F}_\ell)| = O(\ell^{r-1})$ where the implicit constant does not depend on $B$ or $\ell$. Since $T$ is split, we have $|T(\mathbb{F}_\ell)| = (\ell - 1)^r$. Thus for all sufficiently large $\ell \in \mathcal{S}$, the set $T(\mathbb{F}_\ell) - V(\mathbb{F}_\ell)$ is non-empty, and hence there is a $t_1 \in T(\mathbb{F}_\ell)$ such that $\det(x^N I - Bt_1^N) \in \mathbb{F}_\ell[x]$ has exactly $d$ distinct roots in $\overline{\mathbb{F}}_\ell$. Since the index $[H_\ell(\mathbb{F}_\ell) : \rho_{A,\ell}(\mathrm{Gal}_L)]$ divides $N$, we find that $t_1^N$ lies in $\rho_{A,\ell}(\mathrm{Gal}_L)$, and hence $Bt_1^N$ belongs to $\rho_{A,\ell}(\beta\,\mathrm{Gal}_L)$. By the Chebotarev density theorem, there is a prime $\mathfrak{p} \nmid \ell$ of $\mathcal{O}_K$ for which $A$ has good reduction at $\mathfrak{p}$, $(\mathfrak{p}, L/K) = C$, and $Bt_1^N$ is in the conjugacy class $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})$. Since $P_{A,\mathfrak{p}}(x^N) \equiv \det(x^N I - Bt_1^N) \bmod \ell$ has $d$ distinct roots in $\overline{\mathbb{F}}_\ell$, the polynomial $P_{A,\mathfrak{p}}(x^N)$ will have at least $d$ distinct roots in $\overline{\mathbb{Q}}$. From our definition of $d_C$ (see the beginning of §3.2), we deduce that $d \le d_C$. Therefore, $d = d_C$ as claimed. □

**Lemma 3.5.** *For $\ell \in \mathcal{S}$ sufficiently large, each irreducible components of $W_{\overline{\mathbb{F}}_\ell}$ has dimension $r - 1$ and is defined over $\mathbb{F}_\ell$.*

*Proof.* The variety $W$ has dimension $r - 1$. Let $W_1, \ldots, W_m$ be the irreducible components of $W_{\overline{\mathbb{F}}_\ell}$. Each component $W_i$ has dimension $r - 1$, cf. [Lan72, II Theorem 11]. So it remains to show that all of the $W_i$ are defined over $\mathbb{F}_\ell$, at least for $\ell$ sufficiently large.

Set $V := (T/\mathbb{G}_m)_{\overline{\mathbb{F}}_\ell}$. For each $1 \le i \le m$, let $\varphi_i$ be the morphism $\varphi|_{W_i}\colon W_i \to V$. The morphism $\varphi_i$ is a cover; by cover, we mean that it is étale of some degree $d_i$ after replacing $W_i$ and $V$ by non-empty Zariski open subsets. Let $Z$ be the Zariski closure of $\varphi(\bigcup_{i \ne j} W_i \cap W_j)$ in $V$. Using that the $\varphi_i$ are covers, one can show that $Z \ne V$. So for a general $v \in V(\overline{\mathbb{F}}_\ell)$ outside $Z$, we have a disjoint union $\varphi^{-1}(v) = \bigcup_i \varphi_i^{-1}(v)$ with $d = |\varphi^{-1}(v)|$ and $d_i = |\varphi_i^{-1}(v)|$. Therefore, $d = \sum_i d_i$.

Assuming $\ell \in \mathcal{S}$ is sufficiently large, we can fix an element $t \in T(\mathbb{F}_\ell)$ satisfying the conditions of Lemma 3.4. By our choice of $t$, the fiber $\varphi^{-1}(\bar{t}) = \bigcup_i \varphi_i^{-1}(\bar{t})$ has $d$ distinct elements. Since $|\varphi_i^{-1}(\bar{t})| \le d_i$ for each $1 \le i \le m$ and $d = \sum_i d_i$, we deduce that $\varphi^{-1}(\bar{t})$ is the disjoint union of the sets $\varphi_i(\bar{t})$ and each $\varphi_i^{-1}(\bar{t})$ consists of $d_i$ distinct elements. The disjointness implies that each point in $\varphi^{-1}(\bar{t})$ lies in a unique irreducible component of $W_{\overline{\mathbb{F}}_\ell}$.

Fix $1 \le i \le m$. Choose a point $w_i \in \varphi_i^{-1}(\bar{t})$ (such a point exists since $\varphi_i^{-1}(\bar{t})$ consists of $d_i \ge 1$ elements). We have $w_i \in W(\mathbb{F}_\ell)$ by our choice of $t$, so $w_i = \sigma(w_i) \in \sigma(W_i)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{F}_\ell}$. Since $W_i$ is the unique irreducible component of $W_{\overline{\mathbb{F}}_\ell}$ that contains $w_i$, we deduce that $\sigma(W_i) = W_i$ for all $\sigma \in \mathrm{Gal}_{\mathbb{F}_\ell}$ and hence $W_i$ is defined over $\mathbb{F}_\ell$ as claimed. □

By taking $\ell \in \mathcal{S}$ sufficiently large, we may assume by Lemma 3.5 that all of the irreducible components of $W_{\overline{\mathbb{F}}_\ell}$ are defined over $\mathbb{F}_\ell$ (by adjusting $c$ appropriately, it is easy to verify Lemma 3.3 for the finitely many excluded primes). From Lemma 3.2(b) and our choice of $\mathcal{S}$, the split torus $T$ (viewed as a closed subvariety of $\mathbb{A}^n_{\mathbb{F}_\ell}$) is defined by a bounded number of equations of bounded degree (that is, bounded independently of the choice of $B$ and $\ell \in \mathcal{S}$). Theorem 2.1 thus implies that

$$|\{t \in T(\mathbb{F}_\ell) : \det(I - Bt^N) = 0\}| = |W(\mathbb{F}_\ell)| \geq \ell^{r-1} + O(\ell^{r-3/2}) \tag{3.3}$$

where the implicit constant does not depend on the choice of $B$ or $\ell$.

**Lemma 3.6.** *For $\ell \in \mathcal{S}$, we have*

$$|\{t \in T(\mathbb{F}_\ell) : t \text{ is not regular in } H_\ell\}| = O(\ell^{r-1})$$

*where the implicit constant depends only on $r$.*

*Proof.* For each diagonalizable group $D$ defined over $\mathbb{F}_\ell$, let $X(D)$ be the group of characters $D_{\overline{\mathbb{F}}_\ell} \to \mathbb{G}_{m,\overline{\mathbb{F}}_\ell}$. Let $R = R(H_\ell, T)$ be the set of *roots of $H_\ell$ relative to $T$*, see [Bor91, 8.17] (more precisely, the roots of $H_{\ell,\overline{\mathbb{F}}_\ell}$ relative to $T_{\overline{\mathbb{F}}_\ell}$); it is a finite subset of $X(T)$. Since $T$ is split, we can also identify $X(T)$ with the group of characters $T \to \mathbb{G}_{m,\mathbb{F}_\ell}$. We will follow the usual convention and view $X(T)$ as an additive group.

An element $t \in T(\mathbb{F}_\ell)$ is regular if and only if $\alpha(t) \neq 1$ for all $\alpha \in R$ [Bor91, 12.2]. We thus have

$$\{t \in T(\mathbb{F}_\ell) : t \text{ is not regular in } H_\ell\} = \bigcup_{\alpha \in R} D_\alpha(\mathbb{F}_\ell), \tag{3.4}$$

where $D_\alpha := \ker \alpha$ is an algebraic group defined over $\mathbb{F}_\ell$.

Take any root $\alpha \in R$. The group $D_\alpha$ is split and diagonalizable since $D_\alpha$ is a subgroup of the split torus $T$. Therefore, $D_\alpha = D_\alpha^\circ \times F_\alpha$ where $D_\alpha^\circ$ is a split torus and $F_\alpha$ is a finite abelian group (whose order is relatively prime to $\ell$) [Bor91, 8.7]. Since $\alpha$ is non-trivial, $D_\alpha^\circ$ is a split torus of rank $r-1$. Therefore,

$$|D_\alpha(\mathbb{F}_\ell)| \leq m_\alpha |D_\alpha^\circ(\mathbb{F}_\ell)| = m_\alpha(\ell - 1)^r \leq m_\alpha \ell^{r-1},$$

where $m_\alpha$ is the cardinality of $F_\alpha$. From (3.4), we deduce that

$$|\{t \in T(\mathbb{F}_\ell) : t \text{ is not regular in } H_\ell\}| \leq |R| \cdot \max_{\alpha \in R} m_\alpha \cdot \ell^{r-1}.$$

It thus remains to prove that $|R|$ and $m_\alpha$ can be bounded in terms of $r$ only. These are geometric quantities, so for the rest of the proof we may assume (after base extending) that $H_\ell$, $T$ and $D_\alpha$ are all defined over $\overline{\mathbb{F}}_\ell$. Associated to the connected reductive group $H_\ell/\overline{\mathbb{F}}_\ell$ and maximal torus $T$ is its *root datum* $\Psi = (X, R, X^\vee, R^\vee)$, where $X := X(T)$; see [Spr09, §7.4] for details. For us, an important part of the root datum is a perfect pairing of free abelian groups $\langle\ ,\ \rangle \colon X \times X^\vee \to \mathbb{Z}$ and a bijection $R \to R^\vee, \alpha \mapsto \alpha^\vee$ such that $\langle \alpha, \alpha^\vee \rangle = 2$.

We claim that $m_\alpha \in \{1, 2\}$ for each $\alpha \in R$. From the exact sequence

$$1 \to D_\alpha \to T \xrightarrow{\alpha} \mathbb{G}_{m,\overline{\mathbb{F}}_\ell} \to 1,$$

we have a dual exact sequence

$$1 \to \mathbb{Z} \to X(T) \to X(D_\alpha) \to 1 \tag{3.5}$$

of finitely generated abelian groups [Bor91, III 8.12]. In (3.5), the homomorphism $\mathbb{Z} \to X(T)$ is determined by $1 \mapsto \alpha$ and the homomorphism $X(T) \to X(D_\alpha)$ is restriction. Therefore, $X(T)/\langle\alpha\rangle$ is isomorphic to $X(D_\alpha) = X(D_\alpha^\circ) \times X(F_\alpha) \cong \mathbb{Z}^{r-1} \times F_\alpha$. So there is a character $\beta \in X(T)$ whose image in $X(T)/\langle\alpha\rangle$ generates a group of order $m_\alpha$. The group generated by $\alpha$ and $\beta$ is cyclic of infinite order ($\alpha$ and $\beta$ lie in the free abelian group $X(T)$ and satisfy some relation since $m_\alpha \beta \in \langle\alpha\rangle$.

So by making an appropriate choice of $\beta$, we find that $\alpha = n\beta$ for some integer divisible by $m_\alpha$. This implies that $2 = \langle \alpha, \alpha^\vee \rangle = n\langle \beta, \alpha^\vee \rangle \equiv 0 \pmod{m_\alpha}$ and hence $m_\alpha$ is 1 or 2.

From the root datum we can view $R$ as a root system in a Euclidean space of dimension at most $r$, cf. [Spr09, §7.4.1]. Finally, note that there are only finitely many such root systems up to isomorphism (just reduce to the irreducible case where we have the familiar classification in terms of Dynkin diagrams). □

Let $D$ be the set of $t \in T(\mathbb{F}_\ell)$ for which $t^N$ is not regular in $H_\ell$. For each $t' \in T(\mathbb{F}_\ell)$, there are at most $N^r$ elements $t \in T(\mathbb{F}_\ell)$ for which $t^N = t'$. Thus by Lemma 3.6, we have

$$|D| \leq N^r |\{t' \in T(\mathbb{F}_\ell) : t' \text{ is not regular in } H_\ell\}| = O(\ell^{r-1}) \tag{3.6}$$

where the implicit constant depends only on $r$ and $N$. The group $\mathbb{G}_m(\mathbb{F}_\ell) = \mathbb{F}_\ell^\times$ acts on $D$ by multiplication since $\mathbb{G}_m \subseteq T$. For each $t \in D$, there are at most $d$ values of $\lambda \in \mathbb{F}_\ell^\times$ such that $\lambda t \in W(\mathbb{F}_\ell)$. Therefore,

$$|\{t \in W(\mathbb{F}_\ell) : t^N \text{ not regular in } H_\ell\}| \leq d|D|/(\ell - 1) = O(\ell^{r-2}) \tag{3.7}$$

where the last equality follows from (3.6) and the implicit constant depends only on $r$, $N$ and $d$. Lemma 3.3 follows by combining (3.3) and (3.7).

## References


[Bor91] A. Borel, *Linear algebraic groups*, second edition, Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991. ↑3.1, 3.2, 3.3, 3.3, 3.3

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

[Del80] P. Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252. ↑2, 2

[Del77] ———, *Cohomologie étale*, Lecture Notes in Mathematics, Vol. 569, Springer-Verlag, Berlin, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 1/2, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier. ↑2

[FJ74] G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields*, Proc. London Math. Soc. (3) **28** (1974), 112–128. ↑1

[FJ05] M. D. Fried and M. Jarden, *Field arithmetic*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 11, Springer-Verlag, Berlin, 2005. ↑1

[GJ05] W.-D. Geyer and M. Jarden, *Torsion of abelian varieties over large algebraic fields*, Finite Fields Appl. **11** (2005), no. 1, 123–150. ↑1

[GJ78] ———, *Torsion points of elliptic curves over large algebraic extensions of finitely generated fields*, Israel J. Math. **31** (1978), no. 3-4, 257–297. ↑1

[JJ01] M. Jacobson and M. Jarden, *Finiteness theorems for torsion of abelian varieties over large algebraic fields*, Acta Arith. **98** (2001), no. 1, 15–31. ↑1, 1

[Kat01] N. M. Katz, *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. **7** (2001), no. 1, 29–44. ↑2

[Lan72] S. Lang, *Introduction to algebraic geometry*, Addison-Wesley Publishing Co., Inc., Reading, Mass., 1972. Third printing, with corrections. ↑3.3

[LP97] M. Larsen and R. Pink, *A connectedness criterion for l-adic Galois representations*, Israel J. Math. **97** (1997), 1–10. ↑3.1

[Mil80] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. ↑2

[Ser13] J-P. Serre, *Un critère d'indépendance pour une famille de représentations $\ell$-adiques*, Comment. Math. Helv. **88** (2013), no. 3, 541–554. ↑3.1

[Ser00] ———, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000. 1985–1998. ↑3.1, 3.1

[Ser86] ———, *Résumé des cours de 1985-1986*, Annuaire du Collège France (1986), 95–100. (=Œuvres. Collected papers. IV, 33–37). ↑3.1

[Spr09] T. A. Springer, *Linear algebraic groups*, 2nd ed., Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2009. ↑3.1, 3.2, 3.3, 3.3

[Win02] J.-P. Wintenberger, *Démonstration d'une conjecture de Lang dans des cas particuliers*, J. Reine Angew. Math. **553** (2002), 1–16. ↑3.1, 3.1

[Zar87] Yu. G. Zarhin, *Endomorphisms and torsion of abelian varieties*, Duke Math. J. **54** (1987), no. 1, 131–145. ↑1

Department of Mathematics, Cornell University, Ithaca, NY 14853
*E-mail address*: zywina@math.cornell.edu