# TORSION OF ABELIAN VARIETIES OVER LARGE ALGEBRAIC FIELDS*

by

Wulf-Dieter Geyer, Erlangen University

and

Moshe Jarden, Tel Aviv University

Dedicated to the memory of Marcel Jacobson

ABSTRACT. We prove: Let $A$ be an abelian variety over a number field $K$. Then $K$ has a finite Galois extension $L$ such that for almost all $\sigma \in \mathrm{Gal}(L)$ there are infinitely many prime numbers $l$ with $A_l(\tilde{K}(\sigma)) \neq 0$.

Here $\tilde{K}$ denotes the algebraic closure of $K$ and $\tilde{K}(\sigma)$ the fixed field in $\tilde{K}$ of $\sigma$. The expression "almost all $\sigma$" means "all but a set of $\sigma$ of Haar measure 0".

MR Classification: 12E30

Directory: \Jarden\Diary\torsion

23 April, 2004

* Research supported by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation

## Introduction

Let $K$ be an infinite finitely generated field over its prime field. Denote the separable closure of $K$ by $K_s$, the algebraic closure of $K$ by $\tilde{K}$, and the absolute Galois group of $K$ by $\mathrm{Gal}(K)$. The latter group is profinite and is therefore equipped with a unique Haar measure $\mu_K$ satisfying $\mu_K(\mathrm{Gal}(K)) = 1$. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$ let $K_s(\boldsymbol{\sigma})$ be the fixed field of $\sigma_1, \ldots, \sigma_e$ in $K_s$ and $\tilde{K}(\boldsymbol{\sigma})$ the maximal purely inseparable extension of $K_s(\boldsymbol{\sigma})$. Properties of $K_s(\boldsymbol{\sigma})$ and $\tilde{K}(\boldsymbol{\sigma})$ that hold for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ (i.e. for all but a set of $\boldsymbol{\sigma}$ of measure zero) reflect fundamental theorems of arithmetic geometry like Hilbert Irreducibility Theorem and Mordell-Weil Theorem which hold over finite extensions of $K$. The following statements summarize some of these properties:

THEOREM A: *The following statements hold for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$:*

(a) $\mathrm{Gal}(K_s(\boldsymbol{\sigma}))$ *is isomorphic to the free profinite group on $e$ generators [FrJ, Thm. 16.13].*

(b) *The field $K_s(\boldsymbol{\sigma})$ is PAC; that is every absolutely irreducible variety defined over $K_s(\boldsymbol{\sigma})$ has a $K_s(\boldsymbol{\sigma})$-rational point [FrJ, Thm. 16.18].*

(c) $\mathrm{rank}(A(K_s(\boldsymbol{\sigma}))) = \infty$ *for every abelian variety $A$ defined over $K_s(\boldsymbol{\sigma})$ [FyJ, Thm. 9.1].*

Each of the properties (a), (b), and (c) of Theorem A indicates that the fields $K_s(\boldsymbol{\sigma})$ and $\tilde{K}(\boldsymbol{\sigma})$ are, in general, large algebraic extensions of $K$.

As a complement to Theorem A(c), it was only natural to ask about the torsion part of $A$ over the fields $K_s(\boldsymbol{\sigma})$. First we proved the following result for elliptic curves:

THEOREM B ([GeJ, Thm. 1.1]): *Let $E$ be an elliptic curve over $K$. Then the following holds for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$:*

(a) *If $e = 1$, then there are infinitely many prime numbers $l$ with $E_l(\tilde{K}(\boldsymbol{\sigma})) \neq 0$.*

(b) *If $e \geq 2$, then there are only finitely many $l$ with $E_l(\tilde{K}(\boldsymbol{\sigma})) \neq 0$.*

(c) *If $e \geq 1$, then for each $l$ the set $\bigcup_{i=1}^{\infty} E_{l^i}(\tilde{K}(\sigma))$ is finite.*

In contrast to the large rank over these fields, torsion is bounded when $e \geq 2$, and the only unboundedness statement is that for $e = 1$. This case says, for a measure 1 set of $\sigma$ in the absolute Galois group, the set of primes $l$ with $E_l$ nontrivial is infinite. This is a statement about disjointness of fields generated by various taking $l$-division points for infinitely many $l$. So, one sees it is a result that comes (at least in the case where $E$ has no complex multiplication) from Serre's famous open image theorem on the action of $\mathrm{Gal}(\mathbb{Q})$ on the product of all $E_l$'s. That theorem has not yet been extended to general abelian varieties. Yet we have been able to make progress on the following conjecture for arbitrary abelian varieties:

CONJECTURE C ([GeJ, p. 260]): *Let $A$ be an abelian variety over $K$. Then the following holds for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$:*

(a) *If $e = 1$, then there are infinitely many prime numbers $l$ with $A_l(\tilde{K}(\boldsymbol{\sigma})) \neq 0$.*

(b) *If $e \geq 2$, then there are only finitely many $l$ with $A_l(\tilde{K}(\boldsymbol{\sigma})) \neq 0$.*

(c) *If $e \geq 1$, then for each $l$ the set $\bigcup_{i=1}^{\infty} A_{l^i}(\tilde{K}(\sigma))$ is finite.*

Conjecture C was fully verified when $K$ is a finite field [JaJ1, Prop. 4.2]. Part (c) of the Conjecture is proved in [JaJ2, Main Thm.] for an arbitrary finitely generated field $K$. The same theorem proves Part (b) if $\mathrm{char}(K) = 0$. Parts (a) and (b) are still open if $\mathrm{char}(K) > 0$.

The goal of this work is to prove a weak version of Part (a) of Conjecture C for number fields $K$:

MAIN THEOREM: *Let $A$ be an Abelian variety over a number field $K$. Then $K$ has a finite Galois extension $L$ such that for almost all $\sigma \in \mathrm{Gal}(L)$ there are infinitely many prime numbers $l$ with $A_l(\tilde{L}(\sigma)) \neq 0$.*

We can take $L = K$ in the Main Theorem and thus prove Part (a) of Conjecture $C$ in a few special cases:

(a) $E = \mathbb{Q} \otimes \mathrm{End}_{\mathbb{C}} A$ is a totally real number field with $[E : \mathbb{Q}] = n$ and there is a prime of $K$ at which $A$ has no potential good reduction.

(b) $\mathrm{End}_{\mathbb{C}} A = \mathbb{Z}$ and $\dim(A)$ is 2, 6, or an odd positive integer.

Whether $L$ can be taken as $K$ in the general case remains open.

The proof of the result for elliptic curves depends on a good knowledge of the image of $\mathrm{Gal}(K)$ under the $l$-ic (also known as the "mod $l$") representations associated with $A$. In the general case we have relevant information only over a finite Galois extension $L$ of $K$.

Let $A$ be an abelian variety of dimension $d$ over a number field $K$. We know that for each prime number $l$ we have $A_l(\tilde{K}) \cong \mathbb{F}_l^{2d}$. The action of $\mathrm{Gal}(K)$ on $A_l(\tilde{K})$ gives, after choosing an appropriate basis for $A_l$, a representation $\rho_l$: $\mathrm{Gal}(K) \to \mathrm{GL}_{2d}(\mathbb{F}_l)$. Put $G_K(l) = \rho_l(\mathrm{Gal}(K))$. For each number field $N$ denote the set of all prime numbers which split completely in $N$ by $\mathrm{Splt}(N)$. Using results of Serre, we are able to find a finite Galois extension $L$ of $K$, a number field $N$, a connected reductive subgroup $H$ of $\mathrm{GL}_{2d}$ over $N$ with a positive dimension $r$, a connected algebraic group $\hat{H}$, an isogeny $\theta$: $\hat{H} \to H$ over $N$, and a set $\Lambda$ of prime numbers satisfying the following conditions:

(1a) $\Lambda \subseteq \mathrm{Splt}(N)$.

(1b) $\sum_{l\in\Lambda\cap\mathrm{Splt}(N')} \frac{1}{l} = \infty$ for each number field $N'$.

(1c) $\theta(\hat{H}(\mathbb{F}_l)) \le G_L(l) \le H(\mathbb{F}_l)$ and $(H(\mathbb{F}_l) : \theta(\hat{H}(\mathbb{F}_l)) \le |\mathrm{Ker}(\theta)|$ for each $l \in \Lambda$.

(1d) The fields $L(A_l)$, with $l$ ranging over $\Lambda$, are linearly disjoint over $L$.

We indicate how the main theorem follows from the properties (1a)-(1d): For each $l \in \Lambda$ let $\tilde{S}_l = \{\sigma \in \mathrm{Gal}(L) \mid A_l(\tilde{L}(\sigma)) \ne 0\}$. By (1d), the sets $\tilde{S}_l$ are $\mu$-independent. If we prove that $\sum_{l\in\Lambda} \mu(\tilde{S}_l) = \infty$, then almost all $\sigma \in \mathrm{Gal}(L)$ will belong to infinitely many $\tilde{S}_l$ (a lemma of Borel-Cantelli). This will prove the Main Theorem.

For each $l \in \Lambda$ let $S_l$ be the set of all $\sigma \in \mathrm{Gal}(L(A_l)/L)$ for which there is a nonzero $\mathbf{a} \in A_l(\tilde{L})$ with $\sigma\mathbf{a} = \mathbf{a}$. Then $\mathrm{res}_{L(A_l)}^{-1}(S_l) = \tilde{S}_l$. Hence, $\mu(\tilde{S}_l) = \frac{|S_l|}{[L(A_l):L]}$. By (1c) and Weil-Lang, $[L(A_l) : L] = |G_L(l)| \le |H(\mathbb{F}_l)| \le c_1 l^r$ for some constant $c_1 > 0$. Next use (1c) to estimate $|S_l|$ from below:

$$(2)\qquad \begin{aligned} |S_l| &= \#\{\mathbf{h} \in G_L(l) \mid \det(1-\mathbf{h}) = 0\} \\ &\ge \frac{1}{|\mathrm{Ker}(\theta)|}\#\{\hat{\mathbf{h}} \in \hat{H}(\mathbb{F}_l) \mid \det(1-\theta(\hat{\mathbf{h}})) = 0\}. \end{aligned}$$

Now let $V$ be the intersection of $\hat{H}$ with the hypersurface defined by $\det(1-\theta(\hat{\mathbf{h}})) = 0$. Let $W$ be an absolutely irreducible component of $V$. Then $\dim(W) = r-1$ and $W$ is defined over a finite extension $N'$ of $N$. Let $\Lambda' = \Lambda \cap \mathrm{Splt}(N')$. For each $l \in \Lambda'$ Weil-Lang gives a constant $c_2 > 0$ with $|W(\mathbb{F}_l)| \ge c_2 l^{r-1}$. Combined with (2), this gives $|\mu(\tilde{S}_l)| \ge \frac{c}{l}$ with $c = \frac{c_2}{|\mathrm{Ker}(\theta)|c_1}$. It follows from (1b), that $\sum_{l\in\Lambda'} \mu(\tilde{S}_l) = \infty$, as claimed.

The main body of this work consists of constructing $N$, $\Lambda$, $H$, and $\hat{H}$ as above out of results of Serre lectured by him during 1985-86 in Collège de France. We acknowledge use of lecture notes taken by Eva Bayer as well as a letter of Serre sent to us. We thank Michael Larsen for useful conversation and correspondence and Michael Fried for helpful comments. Finally we thank Gopal Prasad and Andrei Rapinchuk for help on algebraic groups.

## 1. Reductive Groups over Pseudofinite Fields

An **isogeny** $\theta\colon \hat{H} \to H$ of algebraic groups is an epimorphism with a finite kernel. If $\theta$ is defined over a field $F$ and $F$ is algebraically closed, then $\theta(\hat{H}(F)) = H(F)$. In the general case, $\theta(\hat{H}(F))$ is a subgroup of $H(F)$ which may be proper.

We denote the absolute Galois group of a field $F$ by $\mathrm{Gal}(F)$. The field $F$ is **PAC** if every absolutely irreducible variety over $F$ has an $F$-rational point. The field $F$ is **pseudofinite** if $F$ is perfect, PAC, and $\mathrm{Gal}(F) \cong \hat{\mathbb{Z}}$.

Hrushovski-Pillay use heavy model theory to prove the following result. We suggest an alternative proof which uses cohomological arguments:

LEMMA 1.1 ([HrP, Lemma 5.5]): *Let $F$ be a pseudo-finite field and $\theta\colon H \to G$ an isogeny of connected algebraic groups over $F$. Then $|\mathrm{Ker}(\theta)(F)| = (G(F) : \theta(H(F)))$.*

*Proof* (Prasad): Put $K = \mathrm{Ker}(\theta)$. Then the short exact sequence

$$1 \longrightarrow K(\tilde{F}) \longrightarrow H(\tilde{F}) \xrightarrow{\theta} G(\tilde{F}) \longrightarrow 1$$

gives rise to a long exact sequence of nonabelian cohomology groups:

$$(1)\quad 1 \longrightarrow K(F) \longrightarrow H(F) \xrightarrow{\theta} G(F) \longrightarrow H^1(\mathrm{Gal}(F), K(\tilde{F})) \longrightarrow H^1(\mathrm{Gal}(F), H(\tilde{F})),$$

[Ser4, p. 50, Prop. 36]. Each element of $H^1(\mathrm{Gal}(F), H(\tilde{F}))$ may be represented by an absolutely irreducible variety $V$ which is defined over $F$ such that $V \times_F \tilde{F} \cong H$ [LaT, Prop. 4]. Since $F$ is PAC, $V$ has an $F$-rational point. Hence, $V$ represents the trivial element of $H^1(\mathrm{Gal}(F), H(\tilde{F}))$ [LaT, Prop. 4], so $H^1(\mathrm{Gal}(F), H(\tilde{F})) = 1$. Therefore, by (1),

$$(2)\qquad G(F)/\theta(H(F)) \cong H^1(\mathrm{Gal}(F), K(\tilde{F})).$$

Since $K(\tilde{F})$ is finite and normal in $H(\tilde{F})$ and $H$ is connected, $K(\tilde{F})$ is abelian [Spr2, Exer. 2.2.2(4)]. Since $F$ is pseudo-finite, $\mathrm{Gal}(F) \cong \hat{\mathbb{Z}}$. For each positive integer $n$,

$$(3)\qquad |H^0(\mathbb{Z}/n\mathbb{Z}, K(\tilde{F}))| = |H^1(\mathbb{Z}/n\mathbb{Z}, K(\tilde{F}))|$$

[CaF, p. 109, Prop. 11]. Since $\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}$, taking direct limit of (3) gives

$$|H^1(\mathrm{Gal}(F), K(\tilde{F}))| = |H^0(\mathrm{Gal}(F), K(\tilde{F}))| = |K(F)|.$$

We conclude from (2) that $(G(F) : \theta(H(F))) = |K(F)|$. ∎

Let $G$ be a connected linear algebraic group over a field $F$. A **Borel subgroup** of $G$ is a maximal connected solvable subgroup $B$ of $G(\tilde{F})$. We say that $G$ **quasi-splits** over $F$ if $G$ contains a Borel subgroup which is defined over $F$. Suppose $G$ is an algebraic subgroup of $\mathrm{GL}_n$. Then $G$ is said to **split** over $F$ if $G$ has a maximal torus $T$ which is defined and split over $F$. Thus, there is $\mathbf{g} \in \mathrm{GL}_n(F)$ such that $T(\tilde{F})^{\mathbf{g}} \le \mathbb{D}_n(\tilde{F})$. It is known (yet we don't use it) that if $G$ splits over $F$, then $G$ quasi-splits over $F$.

In this section we use the property of being quasi-split to investigate subgroups of finite index of $G(F)$ when $F$ is a perfect PAC field. Section 4 will give sufficient conditions for a reductive group to split over a given perfect field.

LEMMA 1.2: *Let $G$ be a connected linear group over a perfect PAC field $F$. Then $G$* **quasi-splits** *over $F$.*

*Proof:* Denote the class of all field extensions of $F$ by $\mathcal{F}$. For each $F' \in \mathcal{F}$ let $\mathcal{B}(F')$ be the set of all Borel subgroups of $G \times_F F'$. By [Dem, p. 230, Cor. 5.8.3(i)] or [BoS, Cor. 8.5], the functor $\mathcal{B}$ from $\mathcal{F}$ to the class of sets is representable by an absolutely irreducible variety $V$ over $F$ (which is projective and smooth). In particular, $\mathcal{B}(F) = V(F)$. Since $F$ is PAC, $V(F)$ is nonempty. Hence, there is $B \in \mathcal{B}(F)$. Thus, $B$ is a Borel subgroup of $G$ which is defined over $F$. ∎

Let $G$ be a linear algebraic group. $G$ is **semisimple** if it has no infinite solvable normal subgroup. $G$ is **simply connected** if there is no isogeny $\theta$: $H \to G$ with $\mathrm{Ker}(\theta) \neq 1$. An element $g$ of $G$ is **unipotent** if $G$ can be embedded in some $\mathrm{GL}_m$ such that 1 is the only eigenvalue of $g$ (Then this holds for each embedding of $G$ in $\mathrm{GL}_n$.) A subgroup $U$ of $G$ is **unipotent** if each element of $G$ is unipotent. In this case, $U$ is nilpotent, hence solvable. Finally, $G$ is **reductive** if it has no infinite unipotent normal subgroup.

LEMMA 1.3 (Prasad): *Let $F$ be an infinite perfect field and $G$ a simply connected quasi-split semisimple linear algebraic group over $F$. Then each subgroup of $G(F)$ of finite index coincides with $G(F)$.*

*Proof:* Assume $J$ be a proper subgroup of $G(F)$ of finite index. Replace $J$ by the intersection of its conjugates, if necessary, to assume $J \triangleleft G(F)$.

Suppose first $G$ is **almost $F$-simple** (or, in the terminology of [Tit2, p.314] **quasi-simple over** $F$). This means, $G$ has no connected proper normal subgroup over $F$ except 1. Denote the subgroup of $G(F)$ which all unipotent elements generate by $G(F)^+$. By [Tit2, Main Theorem], $G(F)^+$ is **almost simple**; that is, every proper normal subgroup of $G(F)^+$ is contained in the center $Z(G)$ of $G$. Since $G$ is semisimple, simply connected, and quasi-split over $F$ and $F$ is perfect, a theorem of Steinberg asserts that $G(F) = G(F)^+$ [Ste, p. 65, Cor. 3]. Hence, $G(F)$ is almost simple. Since $G$ is semisimple, $Z(G)$ is finite. Hence, every proper normal subgroup of $G(F)$ is finite.

Since $G$ is reductive, $G(F)$ is Zariski dense in $G(\tilde{F})$ [Bor2, p. 220, Cor. 18.3]. In particular, $G(F)$ is infinite. Hence, $J$ is also infinite. Thus, by the preceding paragraph, $J = G(F)$.

In the general case let $G_i$, $i = 1, \ldots, m$, be the minimal groups among the closed connected normal $F$-subgroups of $G$ of positive dimension. Then each $G_i$ is almost $F$-simple and there is an $F$-isogeny $\theta$: $\prod_{i=1}^m G_i \to G$ whose restriction to each $G_i$ is the inclusion [Bor2, Thm. 22.10(i)]. Since $G$ is simply connected, $\theta$ is an isomorphism. Hence, $G \cong \prod_{i=1}^m G_i$ and each $G_i$ is simply connected. Thus, $G(F) \cong \prod_{i=1}^m G_i(F)$. For each $i$, $J \cap G_i(F)$ has finite index in $G_i(F)$. Since $G$ is semisimple and quasi-split over $F$, so is each $G_i$ [Bor2, Prop. 11.14(1)]. By the special case, $J \cap G_i(F) = G_i(F)$. Therefore, $J = G(F)$, as required. ∎

Let $N$ be a field and $S$ a connected semisimple linear algebraic group over $N$. Then there exists a connected semisimple linear algebraic group $\hat{S}$ and an isogeny $\theta$: $\hat{S} \to S$ over $N$ with the following property: For each isogeny $\theta_1$: $S_1 \to S$ over $N$ there exists an isogeny $\kappa$: $\hat{S} \to S_1$ with $\theta_1 \circ \kappa = \theta$ [Tit1, p. 38]. The isogeny $\theta$: $\hat{S} \to S$ is the **simply connected covering of** $S$.

Lemma 1.4 (Prasad): *Let $F$ be a perfect PAC field. Consider a connected semisimple algebraic group $S$ over $F$. Let $\theta\colon \hat{S} \to S$ be the simply connected covering of $S$ over $F$. Then, every subgroup of $S(F)$ of finite index contains $\theta(\hat{S}(F))$.*

*Proof:* Let $J$ be a subgroup of $S(F)$ of a finite index. Then $J' = \theta^{-1}(J \cap \theta(\hat{S}(F)))$ is a subgroup of $\hat{S}$ of a finite index. By Lemma 1.2, $\hat{S}$ is quasi-split. By Lemma 1.3, $J' = \hat{S}(F)$. Therefore, $\theta(\hat{S}(F)) \le J$. ∎

We denote the connected component of 1 of an algebraic group $G$ by $G^0$.

*Remark 1.5: Decomposition of reductive groups.* Let $H$ be a connected reductive group over an algebraically closed field $C$. By [Bor2, §14.2], $H = TH'$, where

(4a) $T$ is a torus and $H'$ is the commutator subgroup of $H$;

(4b) $H'$ is semisimple; and

(4c) $T = Z(H)^0$, where $Z(H)$ is the center of $H$.

In particular, $T$ commutes elementwise with $H'$. Also, $T \cap H'$ is a closed normal abelian subgroup of $H'$. Hence, by (4b), $T \cap H'$ is finite. We call $T$ the **central torus** of $H$ and $H'$ the **semisimple part** of $H$. If $H$ is defined over a perfect subfield $F$ of $C$, then so are $H'$, $Z(H)$, and $T$.

Conversely, if $H = TS$ where $S$ is semisimple and $T$ is a torus which commutes elementwise with $S$, then $H$ is reductive [Bor1, Thm. 5.2]. ∎

We supply an algebraic proof to a special case of [HrP, Prop. 3.3] proved by model theoretic methods.

Lemma 1.6: *Let $F$ be a pseudofinite field of characteristic $0$, $N$ a subfield of $F$, $H$ a connected reductive algebraic group over $N$, and $k$ a positive integer. Then there exist a connected reductive algebraic group $\hat{H}$ and an isogeny $\theta\colon \hat{H} \to H$ over $N$ satisfying this:*

(a) *$\theta(\hat{H}(F))$ is contained in each subgroup of $H(F)$ of index that divides $k$.*

(b) $|\mathrm{Ker}(\theta)(F)| = (H(F) : \theta(\hat{H}(F)))$.

*Proof:* Statement (b) is a special case of Lemma 1.1. We prove (a).

Let $T$ be the central torus and $S$ the semisimple part of $H$. The map $(t,s) \mapsto ts$ is an isogeny $\pi\colon T \times S \to H$, because $\mathrm{Ker}(\pi)$ is a normal closed abelian subgroup of $S$. Let $\kappa\colon T \to T$ be the isogeny defined by $\kappa(\mathbf{t}) = \mathbf{t}^{k!}$. Let $\sigma\colon \hat{S} \to S$ be the simply connected covering over $N$. Then $\theta = \pi \circ (\kappa \times \sigma)\colon T \times \hat{S} \to H$ is an isogeny over $N$. By [Bor1, Thm. 5.1], $\hat{H} = T \times \hat{S}$ is reductive and defined over $N$ (comments preceding Lemma 1.4). Since both $T$ and $\hat{S}$ are connected and linear, so is $\hat{H}$.

Now consider a subgroup $B$ of $H(F)$ of index that divides $k$. The intersection of all conjugates of $B$ is a normal subgroup $B_0$ of $H(F)$ of index dividing $k!$. Then $D = \pi^{-1}(B_0)$ is a normal subgroup of $T(F) \times S(F)$ of index dividing $k!$. Hence, $D_1 = D \cap T(F)$ is a normal subgroup of $T(F)$ of index dividing $k!$. Since $T(F)$ is abelian, $\kappa(T(F)) = T(F)^{k!} \le D_1$. Similarly, $D_2 = D \cap S(F)$ is a normal subgroup of $S(F)$ of index dividing $k!$. By Lemma 1.4, $\sigma(\hat{S}(F)) \le D_2$. The $N$-isogeny $\theta\colon \hat{H} \to H$ satisfies

$$\theta(\hat{H}(F)) = \pi\big(\kappa(T(F)) \times \sigma(\hat{S}(F))\big) \le \pi(D_1 \times D_2) \le \pi(D) \le B_0 \le B. \qquad \blacksquare$$

## 2. Axiomatic Approach

Consider a field $K$ and an Abelian variety $A$ of dimension $d$ over $K$. Let $\mu = \mu_K$ be the normalized Haar measure of $\mathrm{Gal}(K)$. Our goal in this section is to give a proof of the Main Theorem based on certain assumptions which we make on $A$ and $K$:

Let $\mathbb{P}$ be the set of all prime numbers. Recall that the **Dirichlet density** of a subset $B$ of $\mathbb{P}$ is defined as the limit (if it exists)

$$\delta(B) = \lim_{s\to 1^+} \frac{\sum_{l\in B} l^{-s}}{\sum_{l\in\mathbb{P}} l^{-s}}.$$

It has the following properties:

(1a) $\delta(\mathbb{P}) = 1$.

(1b) If $\sum_{l\in B}\frac{1}{l} < \infty$, then $\delta(B) = 0$ (because $\sum_{l\in\mathbb{P}}\frac{1}{l} = \infty$).

(1c) If $\delta(B) = 0$ and $C \subseteq B$, then $\delta(C) = 0$.

(1d) If $B$ and $C$ are disjoint sets with Dirichlet density, then $\delta(B\cup C) = \delta(B) + \delta(C)$.

(1e) $\delta(\mathbb{P}\smallsetminus B) = 1 - \delta(B)$, if $\delta(B)$ exists.

(1f) If $\delta(B) = 0$ and $\delta(C)$ exists, then $\delta(B\cup C) = \delta(C)$. This follows from the following inequality:

$$\sum_{l\in C}\frac{1}{l^s} \le \sum_{l\in B\cup C}\frac{1}{l^s} \le \sum_{l\in B}\frac{1}{l^s} + \sum_{l\in C}\frac{1}{l^s}.$$

(1g) If $\delta(B) = 1$ and $\delta(C)$ exists, then $\delta(B\cap C) = \delta(C)$ (use (1e) and (1f)).

(1h) For each number field $N$ let $\mathrm{Splt}(N)$ be the set of all prime numbers $l$ that split completely in $N$. Thus, if $l \in \mathrm{Splt}(N)$ and $\mathfrak{l}$ is a prime of $N$ over $l$, then the residue field of $N$ at $\mathfrak{l}$ is $\mathbb{F}_l$. Note that $l \in \mathrm{Splt}(N)$ if and only if $l \in \mathrm{Splt}(\hat{N})$, where $\hat{N}$ is the Galois closure of $N/\mathbb{Q}$. By the Chebotarev density theorem [FrJ, Thm. 5.6], $\delta(\mathrm{Splt}(N)) = \frac{1}{[\hat{N}:\mathbb{Q}]}$. ∎

*Construction 2.1: Ultrafilter of prime numbers.* Denote the collection of all subsets of $\mathbb{P}$ of the form $\mathrm{Splt}(N)$ where $N$ is a number field and the sets of Dirichlet Density 1 by $\mathcal{L}_0$. If $N \subseteq N'$ are number fields, then $\mathrm{Splt}(N') \subseteq \mathrm{Splt}(N)$. If $\delta(B) = 1$, then, by (1g) and (1h), $\delta(B\cap\mathrm{Splt}(N)) = \delta(\mathrm{Splt}(N)) > 0$. Thus, the intersection of finitely many sets in $\mathcal{L}_0$ is never empty. Hence, there exists an ultrafilter $\mathcal{L}$ of $\mathbb{P}$ which contains $\mathcal{L}_0$ [FrJ, Cor. 6.7]. In particular, $\mathcal{L}$ contains no subsets of $\mathbb{P}$ of Dirichlet density 0. Hence, by (1b), if $\Lambda \in \mathcal{L}$, then $\sum_{l\in\Lambda} \frac{1}{l} = \infty$. Denote the ultraproduct $\prod \mathbb{F}_l/\mathcal{L}$ by $F$. ∎

Lemma 2.2: *$F$ is a pseudofinite field which contains $\tilde{\mathbb{Q}}$.*

*Proof:* For the first statement see [FrJ, §18.9]. To embed $\tilde{\mathbb{Q}}$ in $F$ consider an irreducible polynomial $f \in \mathbb{Z}[X]$. Denote the decomposition field of $f$ by $N$. For all but finitely many $l \in \mathrm{Splt}(N)$, $f$ decomposes modulo $l$ into distinct linear factors. So, $f$ decomposes into distinct linear factors in $F$. This gives a (noncanonical) embedding of $\tilde{\mathbb{Q}}$ into $F$ which we fix for the whole work. ∎

*Construction 2.3: Choice of an extension of $l$.* Let $N$ be a finite Galois extension of $\mathbb{Q}$. Choose a primitive element $x$ for $N$ which is integral over $\mathbb{Z}$. Put $f = \mathrm{irr}(x,\mathbb{Q})$. By Lemma 2.2, $x \in F$. Choose a system of representatives $(\bar{x}_l)_l$ for $x$ modulo $\mathcal{L}$. For each $l \in \mathrm{Splt}(N)$ denote the local ring of $\mathbb{Z}$ at $l$ by $\mathbb{Z}_{(l)}$. Then $A = \{l \in \mathrm{Splt}(N) \mid \bar{x}_l$ is a root of $f$ modulo $l\}$ belongs to $\mathcal{L}$. For all but finitely many $l \in A$, $\mathbb{Z}_{(l)}[x]$ is the integral closure of $\mathbb{Z}_{(l)}$ in $N$ [FrJ, Lemma 5.3]. Hence, the map $x \mapsto \bar{x}_l$ defines a prime divisor $\mathfrak{l}$ of $N$ which extends $l$ with residue field $\mathbb{F}_l$. For all other $l \in \mathbb{P}$ choose an extension $\mathfrak{l}$ of $l$ to $N$ arbitrarily. It follows that for each $y \in N$ with a system of representatives $(\bar{y}_l)_l$ modulo $\mathcal{L}$ there is $B \in \mathcal{L}$ such that $\bar{y}_l$ is the reduction of $y$ modulo $\mathfrak{l}$ for each $l \in B$.

In particular, suppose $H$ is an algebraic subgroup of $\mathrm{GL}_n$ defined over $N$. Then, for all but finitely many $l \in \mathrm{Splt}(N)$ the group $H(\mathbb{F}_l)$ of all $\mathbb{F}_l$-rational points of $H$ is well defined. If $\mathbf{a}$ is a point of $H(F)$ with a system of representative $(\bar{\mathbf{a}}_l)$ modulo $\mathcal{L}$, then $\{l \in \mathrm{Splt}(N) \mid \bar{\mathbf{a}}_l \in H(\mathbb{F}_l)\} \in \mathcal{L}$. Moreover, if $\mathbf{a} \in H(N)$, then for a set of $l$'s in $\mathcal{L}$, $\bar{\mathbf{a}}_l$ is the reduction of $\mathbf{a}$ modulo $\mathfrak{l}$. ∎

Denote the ring of integers of a number field $N$ by $O_N$.

For each prime number $l$ choose a basis $\mathbf{a}_1,\ldots,\mathbf{a}_{2d}$ of $A_l(\tilde{\mathbb{Q}})$ over $\mathbb{F}_l$ and let $\rho_l\colon \mathrm{Gal}(K) \to \mathrm{GL}_{2d}(\mathbb{F}_l)$ be the $l$-ic representation of $\mathrm{Gal}(K)$ corresponding to this basis. Put $G_K(l) = \rho_l(\mathrm{Gal}(K))$. Then $\rho_l$ induces an isomorphism $\bar{\rho}_l\colon \mathrm{Gal}(K(A_l)/K) \to G_K(l)$.

Assumption 2.4: *There exist*

(2a) *a finite Galois extension $N$ of $\mathbb{Q}$;*

(2b) *a set $\Lambda$ of prime numbers;*

(2c) *a finite Galois extension $L$ of $K$;*

(2d) *a linear algebraic group $H \leq \mathrm{GL}_{2d}$ defined over $N$;*

(2e) *and a positive integer $c$;*

*with the following properties:*

(3a) *$H$ is a connected reductive group of dimension $r$.*

(3b) *$H$ contains the group $\mathbb{G}_m$ of homotheties.*

(3c) *$\Lambda \subseteq \mathrm{Splt}(N)$ and $\Lambda \in \mathcal{L}$.*

(3d) *For each $l \in \Lambda$ we choose a prime $\mathfrak{l}$ of $N$ which lies over $l$ as in Construction 2.3. Then $H(\mathbb{F}_l)$ is a well defined subgroup of $\mathrm{GL}_{2d}(\mathbb{F}_l)$.*

(3e) *$G_L(l)$ is a subgroup of $H(\mathbb{F}_l)$ of index $\leq c$.*

(3f) *The fields $L(A_l)$, $l \in \Lambda$, are linearly disjoint over $L$.*

Lemma 2.5: *In the notation of Construction 2.1, there exist a connected group $\hat{H}$, an isogeny $\theta$: $\hat{H} \to H$ over $N$, and a subset $\Lambda' \in \mathcal{L}$ of $\Lambda$ such that for each $l \in \Lambda'$*

(4a) *$\theta(\hat{H}(\mathbb{F}_l)) \leq G_L(l)$ and*

(4b) *$|\mathrm{Ker}(\theta)(\mathbb{F}_l)| = (H(\mathbb{F}_l) : \theta(\hat{H}(\mathbb{F}_l))$.*

*Proof:* By (3e), $H^* = \prod G_L(l)/\mathcal{L}$ is a subgroup of $H(F) = \prod H(\mathbb{F}_l)/\mathcal{L}$ of index at most $c$. Lemma 1.6 gives a connected algebraic group $\hat{H}$ and an isogeny $\theta$: $\hat{H} \to H$ over $N$ with $\theta(\hat{H}(F)) \leq H^*$ and $(H(F) : \theta(\hat{H}(F)) = |\mathrm{Ker}(\theta)(F)| < \infty$. Therefore, there exists a subset $\Lambda' \in \mathcal{L}$ of $\Lambda$ such that $\theta$: $\hat{H}(\mathbb{F}_l) \to H(\mathbb{F}_l)$ is a homomorphism and (4) holds for each $l \in \Lambda'$. ∎

*Construction 2.6: A change of $N$ and $\Lambda$.*

Part A: *Intersection with a hypersurface.* Let $\mathbf{z}$ be a set of variables for the coordinates of the ambient affine space of $\hat{H}$. Let $V$ be the intersection of $\hat{H}$ with the hypersurface $Z(\det(1-\theta(\mathbf{z})))$ of that ambient space defined by the equation $\det(1-\theta(\mathbf{z})) = 0$. By (3b), $r \geq 1$.

CLAIM: *$V$ is a union of absolutely irreducible varieties of dimension $r-1$.* Indeed, $\hat{H}$ is absolutely irreducible and $\theta$: $\hat{H} \to H$ is an isogeny. Hence, $\dim(\hat{H}) = \dim(H) = r$. By the dimension theorem [Lan1, p. 36, Thm. 11], it suffices to prove $Z(\det(1-\theta(\mathbf{z}))) \cap \hat{H}$ is nonempty and properly contained in $\hat{H}$.

To this end consider $\lambda \in \tilde{\mathbb{Q}}$ with $\lambda \neq 0$. Since $\theta$: $\hat{H}(\tilde{\mathbb{Q}}) \to H(\tilde{\mathbb{Q}})$ is an epimorphism and $\mathbb{G}_m \leq H$ (Assumption (3b)), there is $\hat{\mathbf{h}} \in \hat{H}(\tilde{\mathbb{Q}})$ with $\theta(\hat{\mathbf{h}}) = \lambda$. Hence,

$$\det(1-\theta(\hat{\mathbf{h}})) = \det(1-\lambda) = (1-\lambda)^{2d}.$$

Thus, $\hat{h} \in V(\tilde{\mathbb{Q}})$ if and only if $\lambda = 1$.

Denote the absolutely irreducible components of $V$ by $V_1, \ldots, V_m$. By the claim, each of them is of dimension $r-1$.

PART B: *Change of $N$ and $\Lambda$.* Let $N'$ be a finite Galois extension of $\mathbb{Q}$ which contains $N$ and $V_i$ is defined over $N$ for $i = 1, \ldots, m$. Let $\Lambda'$ be the subset of $\mathcal{L}$ which Lemma 2.5 gives. Set $\Lambda'' = \Lambda' \cap \mathrm{Splt}(N')$. Omitting finitely many elements from $\Lambda'$, Assumption 2.4 and Condition (4) remain valid if we replace $N$ and $\Lambda$, respectively, by $N'$ and $\Lambda''$.

PART C: *Additional conditions.* Replace $N$ by $N'$ and $\Lambda$ by $\Lambda''$, if necessary, to assume that in addition to (3) and (4) the following conditions hold:

(5a) The intersection $V = \hat{H} \cap Z(\det(1-\theta(\mathbf{z})))$ is nonempty. Let $V_1, \ldots, V_m$ be the absolutely irreducible components of $V$. Each of them has dimension $r-1$.

(5b) $V_i$ is defined over $N$ for $i = 1, \ldots, m$ and $V_i(\mathbb{F}_l)$ is well defined for each $l \in \Lambda$. ∎

Denote the normalized Haar measure of $\mathrm{Gal}(L)$ by $\mu_L$. For each $l \in \Lambda$ let

$$\begin{aligned}\tilde{S}_l &= \{\sigma \in \mathrm{Gal}(L) \mid \ A_l(K_s(\sigma)) \neq 0\} \\ &= \{\sigma \in \mathrm{Gal}(L) \mid \exists \mathbf{p} \in A_l(K_s)\colon \mathbf{p} \neq 0 \text{ and } \sigma\mathbf{p} = \mathbf{p}\}\end{aligned}$$

and

$$S_l = \{\sigma \in \mathrm{Gal}(L(A_l)/L) \mid \exists \mathbf{p} \in A_l(K_s)\colon \mathbf{p} \neq 0 \text{ and } \sigma\mathbf{p} = \mathbf{p}\}.$$

Then $\mathrm{res}^{-1}_{L(A_l)}(S_l) = \tilde{S}_l$, so $\mu_L(\tilde{S}_l) = \frac{|S_l|}{[L(A_l):L]}$. By (3f), the fields $L(A_l)$, $l \in \Lambda$, are linearly disjoint over $L$. Hence, by [FrJ, Lemma 16.11],

(6) the sets $\tilde{S}_l$, $l \in \Lambda$, are $\mu_L$-independent.

Lemma 2.7: *There exists a constant $b > 0$ with $\mu_L(S_l) > \frac{b}{l}$ for all $l \in \Lambda$.*

*Proof:* Consider $l \in \Lambda$. Since $\bar{\rho}_l$ is the isomorphism induced by the action of $\mathrm{Gal}(L(A_l)/L)$ on $A_l$, $\bar{\rho}_l$ maps $S_l$ bijectively onto the set

$$\begin{aligned}\bar{S}_l &= \{\mathbf{h} \in G_K(l) \mid \exists \mathbf{v} \in \mathbb{F}_l^{2d} \colon \mathbf{v} \neq 0 \text{ and } \mathbf{hv} = \mathbf{v}\}.\\ &= \{\mathbf{h} \in G_L(l) \mid 1 \text{ is an eigenvalue of } \mathbf{h}\}\\ &= \{\mathbf{h} \in G_L(l) \mid \det(1 - \mathbf{h}) = 0\}.\end{aligned}$$

By (4a), $\theta(\hat{H}(\mathbb{F}_l)) \leq G_L(l)$. Hence,

$$\bar{S}_l \supseteq \{\theta(\hat{\mathbf{h}}) \in G_L(l) \mid \det(1 - \theta(\hat{\mathbf{h}})) = 0\}.$$

Thus, in the notation of (5a),

$$|\bar{S}_l| \geq \#\{\theta(\hat{\mathbf{h}}) \in H(\mathbb{F}_l) \mid \hat{\mathbf{h}} \in \hat{H}(\mathbb{F}_l) \text{ and } \det(1 - \theta(\hat{\mathbf{h}})) = 0\} = |\theta(V(\mathbb{F}_l))|.$$

Put $m = |\mathrm{Ker}(\theta)|$. By Lemma 2.5 each fiber of the homomorphism $\theta \colon \hat{H}(\mathbb{F}_l) \to H(\mathbb{F}_l)$ consists of at most $m$ elements. Hence,

$$|V(\mathbb{F}_l)| \leq m \cdot |\theta(V(\mathbb{F}_l))|.$$

Therefore,

$$\mu_L(\tilde{S}_l) = \frac{|S_l|}{|G_L(l)|} \geq \frac{|\theta_l(V(\mathbb{F}_l))|}{|G_L(l)|} \geq \frac{|V(\mathbb{F}_l)|}{m \cdot |G_L(l)|} \geq \frac{|V(\mathbb{F}_l)|}{m|H(\mathbb{F}_l)|} .$$

By (5), $V_1$ is an absolutely irreducible variety of dimension $r-1$ defined over $N$. By (3a), $\dim(H) = r$. Hence, by Lang-Weil [LaW, Thm. 1], $|H(\mathbb{F}_l)| = l^r + O(l^{r-\frac{1}{2}})$ and $|V_1(\mathbb{F}_l)| = l^{r-1} + O(l^{r-\frac{3}{2}})$. This gives $b > 0$ independent of $l$ with $\mu_L(S_l) \geq \frac{|V_1(\mathbb{F}_l)|}{m|H(\mathbb{F}_l)|} \geq \frac{b}{l}$ for all $l \in \Lambda$. ∎

By Construction 2.1, $\sum_{l\in\Lambda} \frac{1}{l} = \infty$. Hence, by Lemma 2.7, $\sum_{l\in\Lambda} \mu_L(\tilde{S}_l) = \infty$. By (6), the sets $\tilde{S}_l$, $l \in \Lambda$, are $\mu_L$-independent. It follows from Borel-Cantelli [FrJ, Lemma 16.7(b)] that almost all $\sigma \in \mathrm{Gal}(L)$ belong to infinitely many sets $\tilde{S}_l$. Thus, $A_l(K_s(\boldsymbol{\sigma})) \neq 0$ for infinitely many $l \in \Lambda$. This proves the following result:

Proposition 2.8: *Let $A$ be an Abelian variety over a field $K$ satisfying Assumption 2.4. Then $K$ has a finite Galois extension $L$ such that for almost all $\sigma \in \mathrm{Gal}(L)$ there are infinitely many prime numbers $l$ with $A_l(L_s(\sigma)) \neq 0$.*

## 3. Finiteness Theorems for Linear Representations

Let $F$ be a field extension of $\tilde{\mathbb{Q}}$. The classification theorems for connected semisimple algebraic groups over $\tilde{\mathbb{Q}}$ lead to a finiteness theorem of split connected reductive subgroups of $\mathrm{GL}_n$ over $F$ having a fixed central torus which is defined over $\tilde{\mathbb{Q}}$ (Proposition 3.10).

Let $H$ be a connected algebraic group. Then all maximal tori of $H$ are conjugate [Bor2, Cor. 11.3]. Denote the common dimension of all maximal tori of $H$ by $\mathrm{rank}(H)$ *.

Let $G$ be an algebraic group over a field $N$ and $C$ an algebraically closed extension of $N$. We follow the tradition of the theory of algebraic group that identifies the group $G(C)$ of $C$-rational points of $G$ with the group $G \times_N C$ obtained by a base change from $N$ to $C$.

Algebraic groups $G_1$ and $G_2$ over $C$ are said to be **strictly isogeneous** of there exists an algebraic group $G$ over $C$ and separable isogenies $\theta_i\colon G \to G_i$, $i = 1, 2$.

LEMMA 3.1: *Let $C$ be an algebraically closed field and $r$ a positive integer. Then:*

(a) *There are only finitely many $C$-isomorphism classes of connected semisimple groups of rank $r$ over $C$. Let $H_1, \ldots, H_k$ be representatives of the $\tilde{\mathbb{Q}}$-isomorphism classes of connected semisimple groups of rank $r$ over $\tilde{\mathbb{Q}}$.*

(b) *Suppose $\tilde{\mathbb{Q}} \subseteq C$. Then, $H_1(C), \ldots, H_k(C)$ represent the $C$-isomorphism classes of connected semisimple algebraic groups over $C$ of rank $r$.*

*Proof of (a):* By [Tit1, Thm. 1], each connected semisimple algebraic group $H$ over $C$ is characterized up to strict isogeny by its Dynkin Diagram $\mathcal{D}_H$. The cardinality of $\mathcal{D}_H$ is $\mathrm{rank}(H)$ and there are at most three edges between two given vertices. Hence, there are only finitely many possibilities for $\mathcal{D}_H$ with $\mathrm{rank}(H)$ fixed. Thus, there are only finitely many strict isogeny classes of connected semisimple algebraic groups of rank $r$ over $C$.

* This definition agrees with those of [Spr2, §7.2.1] and [Hum, p. 135] but differs from that of [Bor2, §12.2]. The latter defines $\mathrm{rank}(H)$ as the dimension of a Cartan subgroup of $H$. However, in most of our applications, $H$ is a reductive group. In that case a Cartan subgroup is just a maximal torus [Bor2, §13.17, Cor. 2(c)], so Borel's definition agrees with the one we have made.

Let now $H$ be a connected semisimple algebraic group over $C$. Denote the affine Dynkin diagram of $H$ by $\mathcal{D}'_H$. It is obtained from $\mathcal{D}_H$ by adding one more vertex [Tit1, 1.1.3]. Let $\mathcal{G}$ be the strict isogeny class of $H$. Section 1.5.2 of [Tit1] associates a finite group $\Gamma(\mathcal{G})$ with $\mathcal{G}$ which is naturally embedded in $\mathrm{Aut}(\mathcal{D}'_H)$. Then [Tit1, 1.5.4] associates a subgroup $\Gamma'(H)$ of $\Gamma(\mathcal{G})$ with $H$. Both associations are natural, i.e. remain unchanged if we replace $C$ by an algebraically closed extension $C'$. Moreover, if $H_1, H_2 \in \mathcal{G}$ and $\Gamma'(H_1) = \Gamma'(H_2)$, then $H_1 \cong H_2$. Since $\mathrm{Aut}(\mathcal{D}'_H)$ has only finitely many subgroups, there are only finitely many isomorphism classes in $\mathcal{G}$. Together with the preceding paragraph, this proves there are only finitely isomorphism classes of connected semisimple algebraic groups of rank $r$.

*Proof of (b):* Let $C$ be an algebraically closed field containing $\tilde{\mathbb{Q}}$ and $J$ a connected semisimple group over $C$. Then $J$ is strictly isogeneous to a direct product $J_1 \times \cdots \times J_s$ of connected simple groups $J_1, \ldots, J_s$ over $C$ [Bor2, p. 191]. For each $i$ [Tit1, Thm. 1] gives a connected simple algebraic group $G_i$ over $\tilde{\mathbb{Q}}$ with $\mathcal{D}_{G_i} = \mathcal{D}_{J_i}$. Put $G = G_1 \times \cdots \times G_s$. Then $\mathcal{D}_G = \dot{\bigcup}_{i=1}^s \mathcal{D}_{G_i} = \dot{\bigcup}_{i=1}^s \mathcal{D}_{J_i} = \mathcal{D}_J$. Hence, by [Tit1, Thm. 1], $G(C)$ and $J(C)$ are strictly isogeneous over $C$.

Denote the common strict isogeny class of $G(C)$ and $J(C)$ by $\mathcal{G}$. Denote the strict isogeny class of $G$ over $\tilde{\mathbb{Q}}$ by $\mathcal{G}_0$. By [Tit1, §1.5.4, Prop. 1], there is an algebraic group $G'$ over $\tilde{\mathbb{Q}}$ in $\mathcal{G}$ with $\Gamma'(G') = \Gamma'(J)$. By (a), we may take $G$ to be $H_i$ for some $1 \le i \le k$. Hence, by [Tit1, §1.5.4, Prop. 1], $H_i(C) \cong J(C)$, as needed. ∎

The following result is a consequence of Weyl's dimension formula. It follows also from [Ric, Prop. 12.1 and Prop. 9.2].

LEMMA 3.2: *Let $\mathfrak{h}$ a finite dimensional semisimple Lie algebra over $\mathbb{C}$. Then, for each positive integer $n$, $\mathfrak{h}$ has only finitely many $n$-dimensional irreducible representations.*

LEMMA 3.3: *Let $H$ be a semisimple connected algebraic group over $\mathbb{C}$. Then, for each positive integer $n$, $H$ has, up to equivalence, only finitely many $n$-dimensional linear representations.*

*Proof:* We may consider $H(\mathbb{C})$ as a complex Lie group. Each $n$-dimensional linear representation of $H$ uniquely corresponds (up to equivalence) to a linear representation

$\rho: H(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C})$. The latter is uniquely determined by the associated representation of the Lie-algebra $d\rho: \mathfrak{h} \to \mathfrak{gl}_n(\mathbb{C})$ [Var, 2.7.5].

By [Hum, 13.5], $\mathfrak{h}$ is a semisimple complex Lie-algebra. By [Var, 3.13.1], $d\rho$ is the direct sum of irreducible linear representations of $\mathfrak{h}$. By Lemma 3.2, $\mathfrak{h}$ has only finitely many $n$-dimensional irreducible representations. Therefore, $H$ has only finitely many $n$-dimensional linear representations. ∎

Let $G$ be an algebraic group over an algebraically closed field $C$ and $n$ a positive number. Denote the set of equivalence classes of $n$-dimensional linear representations of $G(C)$ by $\mathcal{R}_n(G(C))$. Let $r_n(G(C))$ be the cardinality of $\mathcal{R}_n(G(C))$ if it is finite and $\infty$ otherwise.

Lemma 3.4: *Let $C \subseteq C'$ be algebraically closed fields and $G$ an algebraic group over $C$. Then $r_n(G(C)) = r_n(G(C'))$. If $k = r_n(G(C)) < \infty$, and $\rho_1, \ldots, \rho_k$ are linear representatives of $\mathcal{R}_n(G(C))$, then the canonical extensions of $\rho_1, \ldots, \rho_k$ to $G(C')$ represent $\mathcal{R}_n(G(C'))$.*

*Proof:* Suppose first $\rho_1, \ldots, \rho_k$ are inequivalent $n$-dimensional linear representations of $G(C)$. Assume $\rho_i$ is equivalent to $\rho_j$ over $C'$ for some $1 \le i, j \le k$. Then there is $\mathbf{g}' \in \mathrm{GL}_n(C')$ with $\rho_i(\mathbf{a}) = \rho_j(\mathbf{a})^{\mathbf{g}'}$ for all $\mathbf{a} \in G(C')$. An appropriate specialization $\mathbf{g} \in \mathrm{GL}_n(C)$ of $\mathbf{g}'$ satisfies $\rho_i(\mathbf{a}) = \rho_j(\mathbf{a})^{\mathbf{g}'}$ for all $\mathbf{a} \in \mathrm{GL}_n(C)$. Thus, $\rho_i$ and $\rho_j$ are equivalent over $C$. So, by assumption, $i = j$. It follows that $r_n(G(C)) \le r_n(G(C'))$.

Thus, $\rho_i: G(C) \to \mathrm{GL}_n(C)$ is an algebraic homomorphism and for all $i \ne j$ there exists no $\mathbf{g} \in \mathrm{GL}_n(C)$ with $\rho_i(\mathbf{a}) = \rho_j(\mathbf{a})^{\mathbf{g}}$ for all $\mathbf{a} \in G(C)$. This is an elementary statement with parameters in $C$ which holds in $C$. Therefore, it holds in $C'$ [FrJ, Cor. 8.5]. It follows, $\rho_1, \ldots, \rho_k$, viewed as linear representations of $G(C')$ are inequivalent. This implies, $r_n(G(C)) \le r_n(G(C'))$.

Conversely, suppose $\psi_1, \ldots, \psi_{k'}$ are inequivalent $n$-dimensional linear representations of $G(C')$. They are defined by polynomials with finitely many coefficients $u_1, \ldots, u_m \in C'$. Then, "$\psi_1, \ldots, \psi_{k'}$ are inequivalent $n$-dimensional linear representations of $G(C')$" is an elementary statement on $u_1, \ldots, u_m$ which holds in $C'$. By [FrJ, Thm. 8.3], there is a $C$-specialization of $(u_1, \ldots, u_m)$ to an $m$-tuple $(\bar{u}_1, \ldots, \bar{u}_m)$

of elements of $C$ such that the specialized rational functions $\bar{\psi}_1, \ldots, \bar{\psi}_m$ are inequivalent $n$-dimensional linear representations of $G(C)$. Hence, $r_n(G(C')) \le r_n(G(C))$.

The combination of the first two paragraphs proves the lemma. ∎

The combination of Lemmas 3.3 and 3.4 yields the following result.

LEMMA 3.5: *Let $H$ be a connected semisimple group over $\tilde{\mathbb{Q}}$ and $n$ a positive integer. Then $r_n(H(\tilde{\mathbb{Q}})) < \infty$. Let $\rho_1, \ldots, \rho_k$ be representatives of $\mathcal{R}_n(H(\tilde{\mathbb{Q}}))$. Then for every algebraically closed extension $C$ of $\tilde{\mathbb{Q}}$ the canonical extensions of $\rho_1, \ldots, \rho_k$ to $H(C)$ form a system of representatives of $\mathcal{R}_n(H(C))$.*

LEMMA 3.6: *Let $F$ be a field of characteristic $0$, $H$ a connected semisimple algebraic group over $F$, and $n$ a positive integer. Consider $n$-dimensional linear representations $\rho, \rho'$ of $H$ over $F$. Suppose $\rho$ and $\rho'$ become equivalent over a field extension $F'$ of $F$. Then $\rho$ and $\rho'$ are equivalent over $F$.*

*Proof:* Our assumptions gives $\mathbf{g} \in \mathrm{GL}_n(F')$ with $\rho(\mathbf{h})^{\mathbf{g}} = \rho'(\mathbf{h})$ for all $\mathbf{h} \in H(F')$. Hence, $\mathrm{trace}(\rho(\mathbf{h})) = \mathrm{trace}(\rho'(\mathbf{h}))$ for all $\mathbf{h} \in H(F)$. By [Spr1, Prop. 3.9(a)], $\rho$ and $\rho'$ are semisimple representations of $H(F)$. Hence, by [Lan2, p. 650, Cor. 3.8], $\rho$ and $\rho'$ are equivalent representations of $H(F)$. That is, there is $\mathbf{b} \in \mathrm{GL}_n(F)$ such that $\rho(\mathbf{h})^{\mathbf{b}} = \rho'(\mathbf{b})$ for all $\mathbf{h} \in H(F)$. Since $H(F)$ is Zariski-dense in $H(\tilde{F})$ [Bor2, Cor. 18.3], $\rho(\mathbf{h})^{\mathbf{b}} = \rho'(\mathbf{h})$ for all $\mathbf{h} \in H(\tilde{F})$. In other words, $\rho$ and $\rho'$ are $F$-equivalent. ∎

For the rest of this section fix a direct product $G = \prod_{i=1}^{p} \mathrm{GL}_{n_i}$. A **$G$-representation** of an algebraic group $H$ is just a homomorphism $\rho$: $H \to G$. Suppose $\rho$ and $\rho'$ are $G$-representations of $H$ over a field $F$. We say $\rho$ and $\rho'$ are **equivalent** over $F$ if there is $\mathbf{b} \in G(F)$ such that $\rho'(\mathbf{h}) = \rho(\mathbf{h})^{\mathbf{b}}$ for all $\mathbf{h} \in H(\tilde{F})$.

LEMMA 3.7: *Let $F$ be a field of characteristic $0$ and $H$ a connected semisimple algebraic group over $F$. Consider $G$-representations $\rho, \rho'$ of $H$ over $F$. Suppose $\rho$ and $\rho'$ become equivalent over a field extension $F'$ of $F$. Then $\rho$ and $\rho'$ are equivalent over $F$.*

*Proof:* Let $\pi_i$: $G \to \mathrm{GL}_{n_i}$ be the projection on the $i$th factor. By assumption, there is $\mathbf{b} \in G(F')$ with $\rho'(\mathbf{h}) = \rho(\mathbf{h})^{\mathbf{b}}$ for all $\mathbf{h} \in H(\widetilde{F'})$. Hence, for each $i$, $\pi_i(\rho'(\mathbf{h})) = \pi_i(\rho(\mathbf{h}))^{\pi_i(\mathbf{b})}$ for all $\mathbf{h} \in H(\widetilde{F'})$. By Lemma 3.6, there is $\mathbf{a}_i \in \mathrm{GL}_{n_i}(F)$ with $\pi_i(\rho'(\mathbf{h})) =$

$\pi_i(\rho(\mathbf{h}))^{\mathbf{a}_i}$ for all $\mathbf{h} \in H(\tilde{F})$. Then $\mathbf{a} = (\mathbf{a}_1, \ldots, \mathbf{a}_p) \in G(F)$ and $\rho'(\mathbf{h}) = \rho(\mathbf{h})^{\mathbf{a}}$ for all $\mathbf{h} \in H(\tilde{F})$. Thus, $\rho$ and $\rho'$ are equivalent over $F$. ∎

LEMMA 3.8: *There are connected semisimple subgroups $S_1, \ldots, S_m$ of $G(\tilde{\mathbb{Q}})$ with this property: For every field $F$ which contains $\tilde{\mathbb{Q}}$, every connected semisimple algebraic subgroup of $G$ which is defined and split over $F$ is conjugate over $F$ to $S_i \times_{\tilde{\mathbb{Q}}} F$ for some $i$ between 1 and $m$.*

*Proof:* The dimension of each subtorus of $G$ is at most $n = \sum_{j=1}^p n_j$. Let $H_1, \ldots, H_k$ be representatives of the isomorphism classes of connected semisimple algebraic groups of rank at most $n$ over $\tilde{\mathbb{Q}}$ (Lemma 3.1(a)). By Lemma 3.5, each $H_i$ has only finitely many equivalence classes of $n_j$-dimensional linear representations over $\tilde{\mathbb{Q}}$. Hence, each $H_i$ has only finitely many equivalence classes of $G$-representations over $\tilde{\mathbb{Q}}$. Let $\rho_{ij}$, $j = 1, \ldots, q_i$ be representatives of the classes of faithful $G$-representations of $H_i$ over $\tilde{\mathbb{Q}}$. Then list the distinct groups among the $\rho_{ij}(H)$ as $S_1, \ldots, S_m$. Each $S_k$ is a connected semisimple subgroup of $G(\tilde{\mathbb{Q}})$.

Consider now a field $F$ which contains $\tilde{\mathbb{Q}}$. Let $H$ be a connected semisimple algebraic subgroup of $G$ which is defined and split over $F$. Lemma 3.1(b) gives $i$ with $H(\tilde{F}) \cong H_i(\tilde{F})$. By [Tit1, Thm. 2] or [Sat, p. 233, last paragraph], there is an isomorphism $\theta$: $H_i \times_{\tilde{\mathbb{Q}}} F \to H$ over $F$. View $\theta$ as a faithful $G$-representation of $H_i \times_{\tilde{\mathbb{Q}}} F$. By the preceding paragraph, there is $j$ such that $\theta$ is equivalent to $\rho_{ij}$ over $\tilde{F}$. Hence, by Lemma 3.7, $\theta$ is equivalent over $F$ to $\rho_{ij}$. In particular, $H = \theta(H_i \times_{\tilde{\mathbb{Q}}} F)$ is conjugate over $F$ to $\rho_{ij}(H)$ by an element of $G(F)$, that is to one of the groups $S_1 \times_{\tilde{\mathbb{Q}}} F, \ldots, S_m \times_{\tilde{\mathbb{Q}}} F$. ∎

LEMMA 3.9: *Let $C$ be an algebraically closed field and $T$ a subtorus of $\mathrm{GL}_n(C)$. Then the centralizer of $T$ in $\mathrm{GL}_n$ is conjugate to $\prod_{j=1}^p \mathrm{GL}_{n_j}$ with $n_1, \ldots, n_p$ positive numbers and $\sum_{j=1}^p n_j = n$.*

*Proof:* Denote the centralizer of $T$ in $\mathrm{GL}_n(C)$ by $G$. Let $\chi_1, \ldots, \chi_p$ be the **weights** of $T$. Thus, $\chi_j$: $T \to \mathbb{G}_m$ is a homomorphism and the vector space $V_j = \{\mathbf{v} \in C^n \mid \mathbf{tv} = \chi_j(\mathbf{t})\mathbf{v}$ for all $\mathbf{t} \in T(C)\}$ is not zero. Put $n_j = \dim(V_j)$. Then $C^n = \bigoplus_{j=1}^p V_j$ [Bor2, §8.17]. For each $j$ choose a basis $B_j$ of $V_j$. Then $B = B_1 \cup \cdots \cup B_p$ is a basis of $C^n$.

Using conjugation in $\mathrm{GL}_n(C)$, we may assume $B$ to be the standard base of $C^n$.

Consider now an element $\mathbf{g} \in G(C)$ which commutes with $T$. Then, $\mathbf{g}V_j = V_j$. Hence, $\mathbf{g} \in \prod_{j=1}^p \mathrm{GL}(V_j) = \prod_{j=1}^p \mathrm{GL}_{n_j}(C)$. Conversely, every matrix in the latter group belongs to $G$. Therefore, $G = \prod_{j=1}^p \mathrm{GL}_{n_j}(C)$. ∎

PROPOSITION 3.10: *Let $n$ be a positive integer and $T$ a subtorus of $\mathrm{GL}_n(\tilde{\mathbb{Q}})$. Then there exist connected reductive subgroups $H_1, \ldots, H_m$ of $\mathrm{GL}_n(\tilde{\mathbb{Q}})$ with this property: Let $F$ be a field which contains $\tilde{\mathbb{Q}}$ and $H$ a connected reductive subgroup of $\mathrm{GL}_n$ over $F$. Suppose $T \times_{\tilde{\mathbb{Q}}} F$ is the central torus of $H$ and the semisimple part $H'$ of $H$ splits over $F$. Then $H$ is conjugate over $F$ to $H_i$ for some $i$ between 1 and $m$.*

*Proof:* Let $G$ be the centralizer of $T$ in $\mathrm{GL}_n$. By Lemma 3.9, $G$ is conjugate over $\tilde{\mathbb{Q}}$ to $\prod_{j=1}^p \mathrm{GL}_{n_j}$ for some positive integers $n_1, \ldots, n_p$ with $n_1 + \cdots + n_p = n$. Let $S_1, \ldots, S_m$ be as in Lemma 3.8. For each $i$, $S_i$ commutes with $T$. Hence, $H_i = TS_i$ is a connected reductive group over $\tilde{\mathbb{Q}}$ (Remark 1.5).

Consider now $F$ and $H$ as in the Proposition. Then $H = TH'$ and $H'$ commutes with $T$. Hence, $H' \le G$. Also, $H'$ is connected, semisimple and splits over $F$. Hence, by Lemma 3.8, there are $i$ between 1 and $m$ and $\mathbf{a} \in G(F)$ with $H'(\tilde{F}) = S_i(\tilde{F})^{\mathbf{a}}$. Therefore, $H_i(\tilde{F})^{\mathbf{a}} = T(\tilde{F})S_i(\tilde{F})^{\mathbf{a}} = T(\tilde{F})H'(\tilde{F}) = H(\tilde{F})$, as required. ∎

## 4. Splitting of Reductive Groups

We prove in this section a criterion for a connected reductive group to split over a field $K$: There exists a $K$-rational point with the maximal possible number of different eigenvalues, each of them is in $K$.

Let $C$ a **universal extension** of $K$. That is, $C$ is an algebraically closed extension of $K$ with $\mathrm{trans.deg}(C/K) = \infty$. Consider a point $\mathbf{x} \in \mathrm{GL}_n(C)$. Let

$$f_{\mathbf{x}}(X) = \det(X \cdot 1 - \mathbf{x}) \tag{1}$$

be the characteristic polynomial of $\mathbf{x}$ and $\xi_1, \ldots, \xi_m$ the distinct roots of $f_{\mathbf{x}}(X)$ in $C$. Thus,

$$f_{\mathbf{x}}(X) = \prod_{i=1}^{m} (X - \xi_i)^{e_i}, \tag{2}$$

with $e_1, \ldots, e_m \geq 1$ and $\sum_{i=1}^m e_i = n$. Put $\nu(\mathbf{x}) = m$.

Suppose $\mathbf{x} \to \mathbf{x}'$ is a $K$-specialization. That is, $\mathbf{x}' \in \mathrm{GL}_n(C)$ and the map $\mathbf{x} \to \mathbf{x}'$ extends to a $K$-homomorphism $K[\mathbf{x}] \to K[\mathbf{x}']$. By (1), $f_{\mathbf{x}} \in K[\mathbf{x}, X]$ and $\varphi$ uniquely extends to a homomorphism $\varphi$: $K[\mathbf{x}, X] \to K[\mathbf{x}', X]$ with $\varphi(X) = X$ and $\varphi(f_{\mathbf{x}}) = f_{\mathbf{x}'}$. Moreover, $\xi_1, \ldots, \xi_m$ are integral over $K[\mathbf{x}]$. Hence, $\varphi$ further extends to a homomorphism $\varphi$: $K[\mathbf{x}, X, \xi_1, \ldots, \xi_m] \to K[\mathbf{x}', X, \xi_1', \ldots, \xi_m']$ with $f_{\mathbf{x}'}(X) = \prod_{i=1}^m (X - \xi_i')^{e_i}$. It follows, $\nu(\mathbf{x}) \geq \nu(\mathbf{x}')$. If $\nu(\mathbf{x}') = \nu(\mathbf{x})$, then $\varphi$ maps $\{\xi_1, \ldots, \xi_m\}$ bijectively onto $\{\xi_1', \ldots, \xi_m'\}$.

Consider a connected subgroup $H$ of $\mathrm{GL}_n(C)$ which is defined over $K$. Let $\mathbf{x}$ be a generic point of $H$ over $K$. Thus, $\mathbf{x} \in H(C)$ and $\mathbf{x} \to \mathbf{x}'$ is a $K$-specialization for every $\mathbf{x}' \in H(C)$. By the preceding paragraph, $\nu(\mathbf{x}) = \max\{\nu(\mathbf{x}') \mid \mathbf{x}' \in H(C)\}$. Denote the latter number by $\nu(H)$. Each point $\mathbf{a} \in H(C)$ with $\nu(\mathbf{a}) = \nu(H)$ is said to be **strongly regular**.

Define a morphism cl: $\mathrm{GL}_n \to \mathbb{A}^n$ over $\mathbb{Z}$ in the following way: Let $R$ be a commutative ring with 1 and $\mathbf{a} \in \mathrm{GL}_n(R)$. Then let $f_{\mathbf{a}}(X) = X^n + b_1 X^{n-1} + \cdots + b_n$ with $b_1, \ldots, b_{n-1} \in R$ and $b_n \in R^\times$ and set $\mathrm{cl}(\mathbf{a}) = \mathbf{b}$. When $R$ is an integral domain with quotient field $F$ we write $\nu(\mathbf{b}) = \nu(\mathbf{a})$ for the number of distinct roots of $f_{\mathbf{a}}$ in $\tilde{F}$.

Now suppose $H$ and $\mathbf{x}$ are as above. Let $f_{\mathbf{x}}(X) = X^n + y_1 X^{n-1} + \cdots + y_n$. Denote the Zariski closure of $\mathrm{cl}(H)$ by $P$. Then $P$ is an absolutely irreducible subvariety of $\mathbb{A}^n$ defined over $K$ with generic point $\mathbf{y}$. As above $\nu(\mathbf{y}) = \max\{\nu(\mathbf{y}') \mid \mathbf{y}' \in P(C)\}$. and $\nu(P) = \nu(\mathbf{y}) = \nu(\mathbf{x}) = \nu(H)$.

LEMMA 4.1: *Let $K$ be a field, $C$ a universal extension of $K$, $H$ a connected subgroup of $\mathrm{GL}_n$ over $K$, and $T$ a maximal subtorus of $H$ over $K$. Set $P = \mathrm{cl}(H)$. Then:*

(a) $\nu(\mathbf{a}^{\mathbf{h}}) = \nu(\mathbf{a})$ *for all $\mathbf{a} \in H(C)$ and $\mathbf{h} \in \mathrm{GL}_n(C)$.*

(b) *Let $\mathbf{a} = \mathbf{a}_s \mathbf{a}_u$ be the Jordan decomposition of a point $\mathbf{a}$ of $H(C)$ with $\mathbf{a}_s$ semisimple and $\mathbf{a}_u$ unipotent. Then $\nu(\mathbf{a}) = \nu(\mathbf{a}_s)$.*

(c) $\nu(H) = \nu(T)$.

(d) $\nu(T)$ *is the number of weights of $T$.*

(e) *Suppose $K$ is infinite and $T$ splits over $K$. Then $H$ has a strongly regular $K$-rational point whose eigenvalues belong to $K$.*

(f) *The set $\{\mathbf{y}' \in P(C) \mid \nu(\mathbf{y}') = \nu(P)\}$ is nonempty and Zariski open in $P$.*

(g) *The set of strongly regular points of $H(C)$ is a nonempty Zariski open subset which is closed under conjugation.*

*Proof of (a):* Conjugate points have the same characteristic polynomials.

*Proof of (b):* Conjugate $\mathbf{a}$ by an element of $\mathrm{GL}_n(C)$, if necessary, to assume $\mathbf{a}$ is in a Jordan normal form. Then $\mathbf{a}_s$ is the diagonal part of $\mathbf{a}$. This implies, $f_{\mathbf{a}_s} = f_{\mathbf{a}}$. Hence, $\nu(\mathbf{a}) = \nu(\mathbf{a}_s)$.

*Proof of (c):* By definition, $\nu(T) \le \nu(H)$. To prove the inverse equality, consider $\mathbf{a} \in H(C)$. Then $\mathbf{a}_s$ is contained in a maximal torus $T'$ of $H$. By [Bor2, Cor. 11.3(1)], $T'(C)$ is conjugate to $T(C)$ in $H(C)$. Hence, by (a) and (b), $\nu(\mathbf{a}) = \nu(\mathbf{a}_s) \le \nu(T)$. This implies $\nu(H) \le \nu(T)$. We conclude that $\nu(H) = \nu(T)$.

*Proof of (d):* Let $\chi_i$, $i = 1, \ldots, m$ be the distinct weights of $T$. Thus, the $\chi_i$ are those characters of $T$ with a nonzero eigenspace $V_i$. Then $C^n = \bigoplus_{i=1}^m V_i$ [Bor2, §8.17]. Choose a basis for each $V_i$ and take the union of these bases. A computation of the characteristic polynomial with respect to the latter basis of $C^n$ gives $f_{\mathbf{a}}(X) = \prod_{i=1}^m (X - \chi_i(\mathbf{a}))^{e_i}$, where $e_i = \dim(V_i)$. It follows $\nu(T) \le m$.

Since $\chi_1, \ldots, \chi_m$ are distinct, there is $\mathbf{a} \in T(C)$ such that $\chi_1(\mathbf{a}), \ldots, \chi_m(\mathbf{a})$ are distinct. Then, $\nu(\mathbf{a}) = m$, so $\nu(T) = m$, as claimed.

*Proof of (e):* Since $K$ is infinite and $\chi_1, \ldots, \chi_m$ are distinct, there is $\mathbf{a} \in T(K)$ with $\chi_1(\mathbf{a}), \ldots, \chi_m(\mathbf{a})$ distinct. Then $\mathbf{a}$ is a $K$-rational strongly regular point of $H$ whose eigenvalues, $\chi_1(\mathbf{a}), \ldots, \chi_m(\mathbf{a})$, are in $K$.

*Proof of (f) and (g):* Let $m = \nu(H) = \nu(P)$. Denote the set of all $\mathbf{x}' \in H(C)$ with $\nu(\mathbf{x}') = m$ by $H_0$. Then $H_0$ is closed under conjugation. Denote the set of all $\mathbf{y}' \in P(C)$ with $\nu(\mathbf{y}') = m$ by $P_0$. Let $\mathbf{x}$ be a generic point of $H$ over $C$, write

$$f_{\mathbf{x}}(X) = X^n + y_1 X^{n-1} + \cdots + y_n = \prod_{i=1}^{n} (X - z_i)$$

where the roots $z_1, \ldots, z_n$ of $f_{\mathbf{x}}$ are ordered such that $z_1, \ldots, z_m$ are distinct. Then $\mathbf{y} = \mathrm{cl}(\mathbf{x})$ is a generic point of $P$ over $C$. Let $Z = \mathrm{Spec}(K[\mathbf{z}])$ be the variety generated by $\mathbf{z}$ over $K$.

The $y_i$'s are, up to a sign, the values of the fundamental symmetric polynomials in $n$ variables at $(z_1, \ldots, z_n)$. Since $f_{\mathbf{x}}$ is monic, the map $(z_1, \ldots, z_n) \mapsto (y_1, \ldots, y_n)$ defines a finite morphism $\pi \colon Z \to P$. In particular, $\pi$ is surjective and closed. Also, $Z_1 = \bigcup_{1 \le i < j \le m} \{\mathbf{z}' \in Z(C) \mid z_i' = z_j'\}$ is a Zariski closed subset of $Z(C)$. Hence, $P_1 = \pi(Z_1)$ is Zariski closed in $P(C)$. By definition, $P(C) = P_0 \cup P_1$, so $P_0$ is Zariski open in $P$, which proves (f). Finally, $H_0 = \mathrm{cl}^{-1}(P_0)$, so $H_0$ is Zariski open in $H$, as contended by (g).

A point $\mathbf{a}$ of $H(C)$ is said to be **regular** in $H$, if $\mathbf{a}_s$ is contained in a unique maximal torus of $H$ .

LEMMA 4.2: *Let $H$ be a connected reductive subgroup of $\mathrm{GL}_n$ over a field $K$ and $\mathbf{a} \in H(\tilde{K})$. Suppose $\mathbf{a}$ is strongly regular. Then $\mathbf{a}$ is a regular point of $H$.*

*Proof:* Let $m = \nu(H)$. Since $\mathbf{a}_s \in H(\tilde{K})$ and $\nu(\mathbf{a}) = \nu(\mathbf{a}_s)$, we may assume $\mathbf{a}$ is semisimple. Conjugating $H$ by an element of $\mathrm{GL}_n(\tilde{K})$, we may assume

$$\mathbf{a} = \mathrm{Diag}(\alpha_1 I_{e_1}, \ldots, \alpha_m I_{e_m})$$

with $\alpha_1, \ldots, \alpha_m \in \tilde{K}$ distinct, where $I_{e_i}$ is the unit matrix of order $e_i \times e_i$.

Let $T$ be a maximal torus of $H$ over $\tilde{K}$ with $\mathbf{a} \in T(\tilde{K})$. Choose a generic point $\mathbf{t}$ of $T$ over $\tilde{K}$. Then $\mathbf{ta} = \mathbf{at}$. The block structure of $\mathbf{a}$ corresponds to a decomposition $C^n = \bigoplus_{i=1}^m V_i$ where $V_i = \{\mathbf{v} \in C^n \mid \mathbf{av} = \alpha_i \mathbf{v}\}$. Thus, $\mathbf{t}V_i = V_i$, $i = 1, \ldots, m$. This implies $\mathbf{t} = \mathrm{Diag}(\mathbf{t}_1, \ldots, \mathbf{t}_m)$ is a diagonal block matrix with $\mathbf{t}_i \in \mathrm{GL}_{e_i}(C)$, $i = 1, \ldots, m$.

The specialization

$$(\mathbf{t}_1, \ldots, \mathbf{t}_m) \to (\alpha_1 I_{e_1}, \ldots, \alpha_m I_{e_m})$$

extends to a specialization of the eigenvalues of $\mathbf{t}_i$ onto $\alpha_i$. It follows, the sets of eigenvalues of $\mathbf{t}_i$ and $\mathbf{t}_j$ are disjoint, if $i \neq j$. If for some $i$, $\mathbf{t}_i$ had more than one eigenvalue, then $\nu(\mathbf{t}) > m$. This contradiction proves that each $\mathbf{t}_i$ has exactly one eigenvalue $\tau_i$.

Since $\mathbf{t}$ is semisimple, so is each $\mathbf{t}_i$. Thus, $\mathbf{t}_i$ is conjugate in $\mathrm{GL}_{e_i}(C)$ to a diagonal matrix. By the preceding paragraph, that matrix is $\tau_i I_{e_i}$. Therefore, $\mathbf{t}_i = \tau_i I_{e_i}$, so $\mathbf{t} = \mathrm{Diag}(\tau_1 I_{e_1}, \ldots, \tau_m I_{e_m})$ is a diagonal matrix.

Now suppose $T'$ is another maximal torus of $H$ over $\tilde{K}$ with $\mathbf{a} \in T'(\tilde{K})$. Let $\mathbf{t}'$ be a generic point of $T'$ over $\tilde{K}$. Then, as before, $\mathbf{t}' = \mathrm{Diag}(\tau_1' I_{e_1}, \ldots, \tau_m' I_{e_m})$. Hence, $\mathbf{tt}' = \mathbf{t}'\mathbf{t}$. Thus, $\mathbf{t}'$ belongs to the centralizer of $T(C)$ in $H(C)$ which is $T(C)$ itself, because $H$ is reductive [Bor2, p. 175, Cor. 2]. Therefore, $T'(C) \leq T(C)$. The maximality of $T'$ implies $T' = T$. It follows that $\mathbf{a}$ is a regular point of $H$. ∎

The converse of Lemma 4.2 is not true. Every point of a torus $T$ of dimension at least 2 is regular in $T$ but the unit is not strongly regular.

LEMMA 4.3 ([Ser7]): *Let $K$ be a perfect field, $H$ a connected reductive subgroup of $\mathrm{GL}_n$ over $K$. Suppose $H$ has a $K$-rational strongly regular point $\mathbf{a}$ whose eigenvalues belong to $K$. Then $H$ splits over $K$.*

*Proof:* Since $K$ is perfect, $\mathbf{a}_s \in H(K)$ [Bor2, p. 81, Cor. 1(3)]. Let $T$ be a maximal torus of $H$ over $\tilde{K}$ with $\mathbf{a}_s \in T(\tilde{K})$. Conjugating $H$ with an element of $\mathrm{GL}_n(\tilde{K})$, if necessary, we may assume $T(\tilde{K}) \leq \mathbb{D}_n(\tilde{K})$.

For each $\sigma \in \mathrm{Gal}(K)$ we have $\mathbf{a}_s \in T^\sigma(K)$. By Lemma 4.2, $T^\sigma = T$. Since $K$ is perfect, $T$ is defined over $K$. Therefore, since $T \leq \mathbb{D}_n$, $T$ splits over $K$, as claimed. ∎

## 5. Special Semisimple Groups

Ultraproducts of algebraic subgroups of $\mathrm{GL}_n(\tilde{\mathbb{F}}_l)$ need not be Zariski closed because the degrees of the polynomials that define the subgroups need not be bounded. Fortunately, the semisimple groups associated with the $l$-ic representations of abelian varieties are "special" and yield the needed bound. We discuss these "special semisimple groups" in this section.

It is well known that the concept of absolute irreducibility of algebraic sets is elementary. Unfortunately, we have not been able to find a reference to this fact with a solid proof. We therefore give here a short proof based on classical elimination theory.

Denote the first order language of rings by $\mathcal{L}(\mathrm{ring})$ [FrJ, Example 6.1]. Let $I$ be the set of all $n$-tuples $(i_1, \ldots, i_n)$ of nonnegative integers with $i_1 + \cdots + i_n \le d$. Put $r = |I|$. Choose a bijective map $j\colon I \to \{1, \ldots, r\}$. Then the general polynomial in $X_1, \ldots, X_n$ of degree $d$ can be written as $f(\mathbf{T}, X_1, \ldots, X_n) = \sum_{\mathbf{i}\in I} T_{j(\mathbf{i})} X_1^{i_1} \cdots X_n^{i_n}$, with $\mathbf{T} = (T_1, \ldots, T_r)$. Given a ring $R$, every polynomial in $R[X_1, \ldots, X_n]$ of degree at most $d$ can then be written as $f(\mathbf{a}, X_1, \ldots, X_n)$ with $\mathbf{a} \in R^r$.

LEMMA 5.1: *For all positive integers $d, m, n$ there is a formula $\theta(\mathbf{T}_1, \ldots, \mathbf{T}_m)$ in $\mathcal{L}(\mathrm{ring})$ satisfying this: Let $F$ be a field and $f_1, \ldots, f_m$ be polynomials in $F[X_1, \ldots, X_n]$ of degree at most $d$ with vectors of coefficients $\mathbf{a}_1, \ldots, \mathbf{a}_m$, respectively. Then the Zariski $F$-closed subset of $\mathbb{A}^n$ defined by the system of equations $f(\mathbf{a}_i, X_1, \ldots, X_n) = 0$, $i = 1, \ldots, m$, is absolutely irreducible if and only if $\theta(\mathbf{a}_1, \ldots, \mathbf{a}_m)$ holds in $F$.*

*Proof:* Let $F$ be a field and $V$ a Zariski closed subset of $\mathbb{A}^n$ defined by polynomials in $F[X_1, \ldots, X_n]$ of degrees at most $d$. Classical elimination theory gives an effective procedure to decompose $V$ into irreducible $F$-components, if the basic field operations of $F$ are explicitly given and if one can effectively decompose polynomials in $F[X]$ into a product of irreducible factors. The proof of this procedure, as presented in [FrJ, Lemma 17.18 and Proposition 17.20] gives, for general $F$, a bound on the degrees of the polynomials defining the irreducible $F$-components of $V$ in terms of the degrees of the polynomials defining $F$. Thus, there exist positive integers $e$, $s$, and $k$ depending only on $n$ and $d$ such that "$V$ is irreducible over $\tilde{F}$" is equivalent to the following statement:

(1) There exist no polynomials $g_{ij} \in \tilde{F}[X_1, \ldots, X_n]$, $i = 1, \ldots, k$, $j = 1, \ldots, s$, of degree at most $e$ and with $k \geq 2$ such that

$$V = \bigcup_{i=1}^{k} V(g_{i1}, \ldots, g_{is})$$

and no $V(g_{i1}, \ldots, g_{is})$ is contained in the other.

For all distinct $i, i'$ the statement "$V(g_{i1}, \ldots, g_{is}) \not\subseteq V(g_{i'1}, \ldots, g_{i's})$" is equivalent over $\tilde{F}$ to "There exists $\mathbf{x}$ with $g_{i1}(\mathbf{x}) = \cdots = g_{ir}(\mathbf{x}) = 0$ and $g_{i'j}(\mathbf{x}) \neq 0$ for at least one $j$." Statement (1) is therefore equivalent to a formula $\tilde{\theta}(\mathbf{T}_1, \ldots, \mathbf{T}_m)$ of $\mathcal{L}(\mathrm{ring})$ with the following property:

(2) Let $\tilde{F}$ be an algebraically closed field and $\mathbf{a}_1, \ldots, \mathbf{a}_m \in \tilde{F}^r$. Then $V(f(\mathbf{a}_1, \mathbf{X}), \ldots, f(\mathbf{a}_m, \mathbf{X}))$ is irreducible over $\tilde{F}$ if and only if $\tilde{\theta}(\mathbf{a}_1, \ldots, \mathbf{a}_m)$ is true in $\tilde{F}$.

Elimination of quantifiers [FrJ, Thm. 8.3] gives a quantifier free formula $\theta(\mathbf{T}_1, \ldots, \mathbf{T}_m)$ which is equivalent to $\tilde{\theta}(\mathbf{T}_1, \ldots, \mathbf{T}_m)$ over every algebraically closed field. Observe that a quantifier free formula with parameters in $F$ is true in $F$ if and only if it is true in $\tilde{F}$. Consequently, for every field $F$ and all $\mathbf{a}_1, \ldots, \mathbf{a}_m \in F^r$ the following chain of equivalencies holds:

$$\begin{aligned}
&\theta(\mathbf{a}_1, \ldots, \mathbf{a}_m) \text{ is true in } F \\
\iff &\theta(\mathbf{a}_1, \ldots, \mathbf{a}_m) \text{ is true in } \tilde{F} \\
\iff &\tilde{\theta}(\mathbf{a}_1, \ldots, \mathbf{a}_m) \text{ is true in } \tilde{F} \\
\iff &V(f_1, \ldots, f_m) \text{ is irreducible over } \tilde{F} \\
\iff &V(f_1, \ldots, f_m) \text{ is absolutely irreducible.}
\end{aligned}$$

This completes the proof of the proposition. ∎

LEMMA 5.2: *Let $\mathcal{D}$ be an ultrafilter of a set $I$ and $n$ a positive integer. For each $i \in I$ let $F_i$ be a perfect field and $G_i$ a connected reductive subgroup of $\mathrm{GL}_n$ over $F_i$. Denote the ideal of all polynomials in $F_i[X_{jk}]_{1 \leq j,k \leq n}$ which vanish on $G_i$ by $J_i$. Suppose $J_i$ is generated by polynomials of bounded degree. Let $F = \prod_{i \in I} F_i/\mathcal{D}$ and $J = \prod_{i \in I} J_i/\mathcal{D}$.*

*Then the Zariski closed subset $G$ of $\mathrm{GL}_n$ which the ideal $J$ of $F[X_{jk}]_{1\le j,k\le n}$ defines over $F$ is a connected reductive subgroup of $\mathrm{GL}_n$ and $G(F) = \prod_{i\in I} G_i(F_i)/\mathcal{D}$.*

*Proof:* By assumption, we may choose generators $f_{i1},\ldots,f_{im}$ of $J_i$ of degree at most $d$ with $d$ and $m$ independent of $i$. Put $f_j = \prod_{i\in I} f_{ij}/\mathcal{D}$, $j = 1,\ldots,m$. Then let $G$ be the Zariski closed subset of $\mathrm{GL}_n$ defined by $f_1,\ldots,f_m$. By Lemma 5.1, $G$ is a connected subgroup of $\mathrm{GL}_n$ defined over $F$. Moreover, $G(F) = \prod_{i\in I} G(F_i)/\mathcal{D}$.

Assume $G$ is not reductive. Then $G$ has a connected unipotent normal subgroup $U$ of positive dimension over $F$. Since $F$ is perfect, $U(F)$ is Zariski dense in $U$ [Bor2,Cor. 18.3]. Hence, $U(F)$ is infinite. Moreover, $(\mathbf{u}-1)^n = 0$ for each $\mathbf{u}\in U(F)$. Let $g_1,\ldots,g_r$ be a set of generators in $F[X_{jk}]_{1\le j,k\le n}$ for the ideal of all polynomials vanishing on $U(F)$. They satisfy for $\mathbf{x},\mathbf{y}\in \mathrm{GL}_n$

$$
\begin{aligned}
(3)\qquad & g_1(\mathbf{x}) = \ldots = g_r(\mathbf{x}) = 0,\ f_1(\mathbf{y}) = \ldots = f_m(\mathbf{y}) = 0 \\
& \qquad\qquad \Longrightarrow g_1(\mathbf{y}^{-1}\mathbf{x}\mathbf{y}) = \ldots = g_r(\mathbf{y}^{-1}\mathbf{x}\mathbf{y}) = 0
\end{aligned}
$$

Choose representatives $(g_{i1})_{i\in I},\ldots,(g_{ir})_{i\in I}$ of $g_1,\ldots,g_r$, respectively, modulo $\mathcal{D}$. For each $i\in I$ let $U_i$ be the Zariski closed subset of $G_i$ which $g_{i1},\ldots,g_{ir}$ define. Then $U = \prod_{i\in I} U_i/\mathcal{D}$. By Lemma 5.1 there is a set $I_0\in\mathcal{D}$ such that for each $i\in I_0$, $U_i$ is a connected algebraic subgroup of $G_i$ and (3) holds for the $i$-components (so, $U_i$ is normal in $G_i$), and $|U_i(F_i)|\ge 2$. Since a connected group of dimension 0 is trivial, $\dim(U_i)\ge 1$. Moreover, $(\mathbf{u}-1)^n = 0$ for each $\mathbf{u}\in U_i(F_i)$. Since $F_i$ is perfect, $(\mathbf{u}-1)^n = 0$ for each $\mathbf{u}\in U(\tilde{F_i})$. Hence, $U_i$ is unipotent. This contradicts the assumption that $G_i$ is reductive. We conclude that $G$ is reductive. ∎

*Notation 5.3: Choice of $H_1,\ldots,H_m$ and a number field $N$.* Let $n$ be a positive integer and $T$ a subtorus of $\mathrm{GL}_n$ over $\tilde{\mathbb{Q}}$. Following Proposition 3.10, we choose connected reductive subgroups $H_1,\ldots,H_m$ of $\mathrm{GL}_n(\tilde{\mathbb{Q}})$ with the following property:

(4) Let $F$ be a field which contains $\tilde{\mathbb{Q}}$ and $H$ a connected reductive subgroup of $\mathrm{GL}_n$ over $F$. Suppose $H$ splits over $F$ and $T\times_{\tilde{\mathbb{Q}}} F$ is the central torus of $H$. Then $H$ is conjugate over $F$ to $H_i$ for some $i$ between 1 and $m$.

Now choose a number field $N$ over which $H_1,\ldots,H_m$ are defined. As in Construction 2.1, let $\mathcal{L}$ be an ultrafilter of $\mathbb{P}$ which contains $\mathrm{Splt}(N')$ for every number field $N'$ and all sets of Dirichlet density 1. For each $l \in \mathbb{P}$ choose a prime divisor $\mathfrak{l}$ of $N$ as in Construction 2.3. ∎

*Definition 5.4: Special semisimple groups.* Let $l$ be a prime number and $S$ be a connected algebraic subgroup of $\mathrm{GL}_n(\tilde{\mathbb{F}}_l)$. Call $S$ a **special semisimple group** (abbreviated, $S$-**group**) if it satisfies the following condition.

(5a) $S$ is semisimple and acts semisimply on $\tilde{\mathbb{F}}_l^n$.

(5b) $S$ is generated by all elements of the form $\exp(a\mathbf{g}) = \sum_{k=0}^{l-1} \frac{1}{k!}(a\mathbf{g})^k$ where $\mathbf{g} \in S(\mathbb{F}_l)$ satisfies $\mathbf{g}^l = 0$ and $a \in \tilde{\mathbb{F}}_l^\times$. ∎

LEMMA 5.5: *Let $\mathcal{L}$ be the ultrafilter of Construction 2.1 and $\Lambda$ a set in $\mathcal{L}$. Let $N$ a number field, $n$ be a positive integer, and $T$ a subtorus of $\mathrm{GL}_n$ which is defined and split over $N$. For each $l \in \Lambda$ let $H_l$ be a connected reductive subgroup of $\mathrm{GL}_n$ over $\mathbb{F}_l$ satisfying the following conditions:*

(6a) *$H_l$ has a strongly regular $\mathbb{F}_l$-rational point $\mathbf{a}_l$ with all eigenvalues in $\mathbb{F}_l$.*

(6b) *The central torus of $H_l$ is the reduction $\bar{T}_l$ of $T$ modulo $\mathfrak{l}$ (We use the convention of Construction 2.3.)*

(6c) *The commutator subgroup $H_l'$ of $H_l$ is an $S$-group.*

*Then there is an $i$ between $1$ and $m$ and there is $\Lambda' \in \mathcal{L}$ which is contained in $\Lambda \cap \mathrm{Splt}(N)$ such that $H_i(\tilde{\mathbb{F}}_l)$ is conjugate to $H_l(\tilde{\mathbb{F}}_l)$ by an element of $\mathrm{GL}(\mathbb{F}_l)$ for each $l \in \Lambda'$.*

*Proof:* Let $F = \prod \mathbb{F}_l/\mathcal{L}$ and $C = \prod \tilde{\mathbb{F}}_l/\mathcal{L}$. Then $F$ is a pseudofinite field which contains $\tilde{\mathbb{Q}}$ (Lemma 2.2) and $C$ is an algebraically closed field which contains $F$. Let $I_l$ be the ideal of polynomials in $\mathbb{F}_l[X_{ij}]_{1\le i,j\le n}$ which defines $H_l'$. By (6c) and [Ser3, p. 62, Théorème analogue] $I_l$ has a system of generators of bounded degree. Note that the latter theorem is a consequence of [Ser3, p. 60, Théorème] which is also [Ser5, p. 38, Théorème]. Thus, by Lemma 5.2, $H' = \prod H_l'/\mathcal{L}$ is a connected reductive subgroup of $\mathrm{GL}_n$ over $F$. In particular, $H'(F) = \prod H_l'(\mathbb{F}_l)/\mathcal{L}$ and $H'(C) = \prod H'(\tilde{\mathbb{F}}_l)/\mathcal{L}$.

Since $H_l'$ is semisimple, $H''(\tilde{\mathbb{F}}_l) = H'(\tilde{\mathbb{F}}_l)$. Hence, $H''(C) = H'(C)$. By [Bor2, p. 182. Cor], $H'$ is semisimple.

By (6b), $T(F) = \prod \bar{T}_l(\mathbb{F}_l)/\mathcal{L} = \prod T(\mathbb{F}_l)/\mathcal{L}$ and $T(C) = \prod \bar{T}_l(\tilde{\mathbb{F}}_l)/\mathcal{L} = \prod T(\tilde{\mathbb{F}})/\mathcal{L}$.

Consider the subgroup $H(C) = \prod H_l(\tilde{\mathbb{F}}_l)/\mathcal{L}$ of $\mathrm{GL}_n(C)$. It satisfies $H(C)' = H'(C)$, $H(C) = T(C)H'(C)$, and $T(C)$ commutes with $H'(C)$, because these relations hold over $\tilde{\mathbb{F}}_l$ for each $l \in \Lambda$. By Remark 1.5, $H$ is a connected reductive group over $F$.

For each $m \leq n$ let $\Lambda_m = \{l \in \Lambda \mid \nu(H) = m\}$. Then $\Lambda = \bigcup_{m=0}^{n} \Lambda_m$. By the basic properties of ultrafilters, there is a unique $m$ with $\Lambda_m \in \mathcal{L}$. Replace $\Lambda$ by $\Lambda_m$, if necessary, to assume $m = \nu(H_l)$ for all $l \in \Lambda$.

By (6a), the characteristic polynomial $f_{\mathbf{a}_l} \in \mathbb{F}_l[X]$ of $\mathbf{a}_l$ has exactly $m$ roots all of whom are in $\mathbb{F}_l$. Also, $\mathbf{a} = \prod \mathbf{a}_l/\mathcal{L}$ belongs to $H(F)$. On the other hand, $f_{\mathbf{x}}$ has at most $m$ roots in $\mathbb{F}_l$ for all $l \in \Lambda$ and $\mathbf{x} \in H_l(\tilde{\mathbb{F}}_l)$. Hence, $f_{\mathbf{x}}$ has at most $m$ roots in $C$ for all $\mathbf{x} \in H(C)$. Thus, $\nu(\mathbf{a}) = m = \nu(H)$. By Lemma 4.3, $H$ splits over $F$.

Condition (4) gives $i$ in $\{1, \ldots, m\}$ and $\mathbf{b} \in \mathrm{GL}_n(F)$ with $H_i(C) = H(C)^{\mathbf{b}}$. Hence, there is a subset $\Lambda'$ of $\Lambda$ such that $\Lambda' \in \mathcal{L}$ and $H_l(\tilde{\mathbb{F}}_l)$ is conjugate to $H_i(\mathbb{F}_l)$ by an element of $\mathrm{GL}_n(\mathbb{F}_l)$ for each $l \in \Lambda'$. This concludes the proof of the lemma. ∎

## 6. Abelian Varieties over Number Fields

We extract in this section results of Serre which, together with the lemmas proved in the preceding sections, prove Assumption 2.4 for Abelian varieties over number fields. This leads to the proof of the Main Theorem.

Let $K$ be a number field and $A$ an abelian variety over $K$ of dimension $d$. As in Section 2, let $\mathbb{P}$ be the set of prime numbers. For $l \in \mathbb{P}$ choose a basis $\mathbf{a}_1, \ldots, \mathbf{a}_{2d}$ for the Tate module $T_l(A)$. Apply the canonical map $T_l(A) \to A_l$ on $\mathbf{a}_1, \ldots, \mathbf{a}_{2d}$ to get a basis $\bar{\mathbf{a}}_1, \ldots, \bar{\mathbf{a}}_{2d}$ of $A_l$. Let $\rho_{l^\infty}\colon \mathrm{Gal}(K) \to \mathrm{GL}(2d, \mathbb{Z}_l)$ and $\rho_l\colon \mathrm{Gal}(K) \to \mathrm{GL}(2d, \mathbb{F}_l)$ be the $l$-adic and the $l$-ic representations of $\mathrm{Gal}(K)$ corresponding to these bases, respectively. Write $G_K(l) = \rho_l(\mathrm{Gal}(K))$ and $G_K(l^\infty) = \rho_{l^\infty}(\mathrm{Gal}(K))$.

PROPOSITION 6.1 (Serre): *In the above notation there are a finite Galois extension $L$ of $K$, a subtorus $T$ of $\mathrm{GL}_{2d}$ which is defined over $\mathbb{Q}$, a positive integer $c$, and a cofinite subset $\mathbb{P}_0$ of $\mathbb{P}$ with the following properties:*

(a) *For each $l \in \mathbb{P}_0$ there is a connected reductive subgroup $H_l$ of $\mathrm{GL}_{2d}$ which is defined over $\mathbb{F}_l$ and satisfies:*

  (a1) *The group of homotheties $\mathbb{G}_m$ is contained in $T$.*

  (a2) *The central torus of $H_l$ is the reduction $\bar{T}_l$ of $T$ modulo $l$.*

  (a3) *$G_L(l) \le H_l(\mathbb{F}_l)$.*

  (a4) *$(H_l(\mathbb{F}_l) : G_L(l)) \le c$.*

  (a5) *The semisimple part $H_l'$ of $H_l$ is an $S$-group.*

(b) *The fields $L(A_l)$, $l \in \mathbb{P}_0$, are linearly disjoint over $L$.*

(c) *Let $H_{l^\infty}$ be the connected component of the Zariski closed subgroup of $\mathrm{GL}_n$ generated over $\mathbb{Q}_l$ by $G_K(l^\infty)$. Then $G_L(l^\infty)$ is an $l$-adically open subgroup of $H_{l^\infty}(\mathbb{Z}_l)$.*

*Proof:* Conditions (a1), (a2), (a3), and (a4) are announced in [Ser2, §2.5]. Condition (a1) is proved in [Ser5, p. 48, Lemme]. Conditions (a2), (a3), and (a4) are proved in [Ser5, p. 44, Théorème].

To prove (a5) note first that $H_l(\mathbb{F}_l)$ acts semisimply on $\mathbb{F}_l$. This follows from a well known result of Faltings [Ser2, §2.5.4 or Ser5, bottom of p. 42]. By definition [Ser2, §3.2 or Ser3, p. 72], $H_l'$ is generated by all elements $\exp(a(\mathbf{g} - 1))$ with $a \in \tilde{\mathbb{F}}_l^\times$ and

$\mathbf{g} \in G_L(l)$ of order $l$. Thus, $H_l'$ is an S-group.

Condition (b) is announced in [Ser2, §2.1, Thm. 1] and proved in [Ser3, p. 86] and [Ser6, p. 56, Cor.].

Statement (c) is due to Bogomolov [Bog]. ∎

LEMMA 6.2: *Let $p$ be a prime number, $H$ a connected subgroup of $\mathrm{GL}_n$ over $\mathbb{Z}_p$, $W$ a nonempty Zariski open subset of $H$, and $G$ a $p$-adically closed subgroup of $H(\mathbb{Z}_p)$ of finite index. Then the Haar measure of the $p$-adic boundary of $G \cap W(\mathbb{Z}_p)$ in $G$ is zero.*

*Proof:* Since $W$ is Zariski open in $H$, $W(\mathbb{Z}_p)$ is $p$-adically open in $H(\mathbb{Z}_p)$. Hence, $G \cap W(\mathbb{Z}_p)$ is $p$-adically open in $G$. Therefore, the boundary of $G \cap W(\mathbb{Z}_p)$ is contained in $G \smallsetminus W(\mathbb{Z}_p)$, hence in $H(\mathbb{Z}_p) \smallsetminus W(\mathbb{Z}_p)$.

Let $s = \dim(H)$. Since $H$ is smooth, $s$ is also the $p$-adic dimension of $H(\mathbb{Z}_p)$. Since $\dim(H \smallsetminus W) < \dim(H)$, the $p$-adic dimension of $H(\mathbb{Z}_p) \smallsetminus W(\mathbb{Z}_p)$ is smaller than the $p$-adic dimension of $H(\mathbb{Z}_p)$. This implies the Haar measure of $H(\mathbb{Z}_p) \smallsetminus W(\mathbb{Z}_p)$ in $H(\mathbb{Z}_p)$ is 0. By the preceding paragraph, the boundary of $G \cap W(\mathbb{Z}_p)$ has Haar measure 0 in $H(\mathbb{Z}_p)$. Since the Haar measure of the compact groups $H(\mathbb{Z}_p)$ and $G$ differ only by the finite factor $(H(\mathbb{Z}_p) : G)$, the Haar measure of the boundary of $G \cap W(\mathbb{Z}_p)$ in $G$ is 0. ∎

PROPOSITION 6.3 ([Ser7]): *Let $H_l$ be as in Proposition 6.1. Then, there exists a number field $N_0$ such that for each large $l \in \mathrm{Splt}(N_0)$ there is a strongly regular point $\mathbf{a}_l \in H_l(\mathbb{F}_l)$ with all eigenvalues in $\mathbb{F}_l$.*

*Proof:* Let $\mathbf{C}$ be an algebraically closed field which contains $\mathbb{Q}_l$ for all prime numbers $l$. Part A of the proof gives a bound for $\nu(H_l)$. In Part B we choose a large prime number $p$, a prime $\mathfrak{q}$ of $L$, a Frobenius element $\sigma_{\mathfrak{q},p}$ in $\mathrm{Gal}(L(A_{p^\infty})/L)$, and point out that the characteristic polynomial $f_\mathfrak{q}$ of $\sigma_{\mathfrak{q},p}$ is independent of $p$ (for $p$ large). Using the splitting field $N_0$ of $f_\mathfrak{q}$ over $\mathbb{Q}$, we show that all large $l \in \mathrm{Splt}(N_0)$ satisfy the conclusion of the Proposition.

PART A: *Bounding $\nu(H_l)$ by $\nu(H_{l^\infty})$.* The proof of [Ser5, Thm. 2] gives an absolutely irreducible variety $P$ over $\mathbb{Z}$ such that for all large $l$ we have $\mathrm{cl}(H_{l^\infty}) = P$ and $\mathrm{cl}(H_l)$

is the reduction modulo $l$ of $P$. Thus, for $l$ large, $m = \nu(H_{l^\infty}) = \nu(P)$ is independent of $l$ and $\nu(\mathrm{cl}(H_l)) \le \nu(P) = m$. Let $U$ be a nonempty Zariski open subset of $P$ with $\nu(\mathbf{c}) = m$ for all $\mathbf{c} \in U(C)$ (Lemma 4.1(f)). Let $W_{l^\infty}$ be the inverse image of $U$ under cl: $H_{l^\infty} \to P$. Then $W_{l^\infty}$ is a nonempty Zariski open subset of $H_{l^\infty}$ which is closed under conjugation. In addition, $\nu(\mathbf{a}) = m$ for each $\mathbf{a} \in W_{l^\infty}(C)$.

Part B: *Preparing use of the Chebotarev density theorem.* We choose a large prime number $p$. By Proposition 6.1(c), $G_L(p^\infty)$ is a $p$-adically closed subgroup of $H_{p^\infty}(\mathbb{Z}_p)$ of finite index. Hence, by Lemma 6.2, the boundary of $G_L(p^\infty) \cap W_{p^\infty}(\mathbb{Z}_p)$ has Haar measure 0 in $G_L(p^\infty)$.

Let $\rho$: $\mathrm{Gal}(L(A_{p^\infty})/L) \to G_L(p^\infty)$ be the isomorphism induced by $\rho_{p^\infty}$. Like every isomorphism between compact groups, $\rho$ preserves the Haar measure. Hence, the boundary of $\rho^{-1}(W_{p^\infty}(\mathbb{Z}_p))$ has Haar measure 0 in $\mathrm{Gal}(L(A_{p^\infty})/L)$ and is closed under conjugation in $\mathrm{Gal}(L(A_{p^\infty})/L)$.

Part C: *Choosing of a Frobenius element.* Denote the finite set of primes of $L$ at which $A$ has bad reduction by $\mathrm{Bad}(A)$. Let $\mathrm{Bad}(A)_p$ be the union of $\mathrm{Bad}(A)$ with the prime divisors of $p$ in $L$. Then $\mathrm{Bad}(A)_p$ is a finite set and each prime of $L$ outside $\mathrm{Bad}(A)_p$ is unramified in $L(A_{p^\infty})$ [SeT, Thm. 1]. Therefore, by Part B, the Chebotarev density theorem for infinite Galois extensions [JaJ2, Prop. 4.3] gives a prime $\mathfrak{q}$ of $L$ such that each Frobenius element of $\mathrm{Gal}(L(A_{p^\infty})/L)$ over $\mathfrak{q}$ belongs to $\rho^{-1}(W_{p^\infty}(\mathbb{Z}_p))$. Choose a Frobenius element $\sigma_{\mathfrak{q},p}$ in $\mathrm{Gal}(L(A_{p^\infty})/L)$ corresponding to $\mathfrak{q}$. Set $\mathbf{s}_{\mathfrak{q},p} = \rho(\sigma_{\mathfrak{q},p})$ and let $f_\mathfrak{q} = f_{\mathfrak{q},p}$ be the characteristic polynomial of $\sigma_{\mathfrak{q},p}$. Then $f_\mathfrak{q}$ has coefficients in $\mathbb{Z}$ which do not depend on $p$ [SeT, p. 499, Thm. 3]. Since $\mathbf{s}_{\mathfrak{q},p} \in W_{l^\infty}(\mathbb{Z}_p)$, $f_\mathfrak{q}$ has exactly $m$ distinct roots.

Part D: *The splitting field $N_0$ of $f_\mathfrak{q}$ over $\mathbb{Q}$ satisfies the conclusion of the proposition.* Consider a large $l$ in $\mathrm{Splt}(N_0)$ which lies under no prime in $\mathrm{Bad}(A)_p$ and the reduction of $f_\mathfrak{q}$ modulo $l$ has exactly $m$ distinct roots. Now choose a Frobenius element $\sigma_{\mathfrak{q},l}$ in $\mathrm{Gal}(L(A_{l^\infty})/L)$ corresponding to $\mathfrak{q}$. Let $\mathbf{s}_{\mathfrak{q},l} = \rho_{l^\infty}(\sigma_{\mathfrak{q},l}) \in G_L(l^\infty)$. By Part C, $f_\mathfrak{q}$ is the characteristic polynomial of $\mathbf{s}_{\mathfrak{q},l}$. The reduction $\bar{\mathbf{s}}_{\mathfrak{q},l}$ of $\mathbf{s}_{\mathfrak{q},l}$ modulo $l$ is a point of $G_L(l)$, hence of $H_l(\mathbb{F}_l)$. Moreover, $f_{\bar{\mathbf{s}}_{\mathfrak{q},l}}$ is the reduction modulo $l$ of $f_\mathfrak{q}$. Hence, it has exactly

$m$ roots and all of them are in $\mathbb{F}_l$. Therefore, by Part A, $\nu(\bar{\mathbf{s}}_{\mathfrak{q},l}) = \nu(H_l)$. Consequently, $\bar{\mathbf{s}}_{\mathfrak{q},l}$ is strongly regular, as required. ∎

THEOREM 6.4: *Let $A$ an Abelian variety over a number field $K$. Then $K$ has a finite Galois extension $L$ such that for almost all $\sigma \in \mathrm{Gal}(L)$ there are infinitely many prime numbers $l$ with $A_l(\tilde{\mathbb{Q}}(\sigma)) \neq 0$.*

*Proof:* Let $d = \dim(A)$. Proposition 6.1 gives a finite Galois extension $L$ of $K$, a subtorus $T$ of $\mathrm{GL}_{2d}$ over $\mathbb{Q}$, a positive integer $c$, and a cofinite subset $\mathbb{P}_0$ of $\mathbb{P}$ which satisfy (a), (b), and (c) of that Proposition. For each $l \in \mathbb{P}_0$ we may choose a connected reductive subgroup $H_l$ of $\mathrm{GL}_{2d}$ over $\mathbb{F}_l$ which satisfies Conditions (a1)-(a5) of Proposition 6.1. Making $\mathbb{P}_0$ smaller, Proposition 6.3 gives a number field $N_0$ such that for each $l \in \mathbb{P}_0 \cap \mathrm{Splt}(N_0)$ there is a strongly regular point in $H_l(\mathbb{F}_l)$ with all eigenvalues in $\mathbb{F}_l$. Thus, Conditions (6a)-(6c) of Lemma 5.5 hold for each $l \in \mathbb{P}_0 \cap \mathrm{Splt}(N_0)$. Therefore, Lemma 5.5 gives a subgroup $H$ of $\mathrm{GL}_{2d}(\tilde{\mathbb{Q}})$ and a subset $\Lambda$ of $\mathbb{P}_0 \cap \mathrm{Splt}(N_0)$ such that $H(\mathbb{F}_l)$ is conjugate to $H_l(\mathbb{F}_l)$ in $\mathrm{GL}_{2d}(\mathbb{F}_l)$ for each $l \in \Lambda$. After an appropriate change of the base of $A_l$ definining $\rho_l$ we get that $G_L(l) \le H(\mathbb{F}_l)$ for each $l \in \Lambda$.

Let $N$ be a number field which contains $N_0$ such that $H$ is defined over $N$. Thus, $K$, $A$, and $L$ satisfy Conditions (3a)-(3f) of Assumption 2.4. It follows from Proposition 2.8 that for almost all $\sigma \in \mathrm{Gal}(L)$ there exist infinitely many $l$ with $A_l(\tilde{\mathbb{Q}}(\sigma)) \neq 0$. This concludes the proof of the theorem. ∎

## 7. Special Cases

We are able to prove the Main Theorem in the stronger form with $L = K$ in several special cases:

LEMMA 7.1: *Let $L/K$ be a finite field extension. For each $i$ in a set $I$ let $K_i$ be a finite Galois extension of $K$ and put $L_i = LK_i$. Suppose, $[K_i : K] = [L_i : L]$ for each $i \in I$. Suppose in addition $L_i$, $i \in I$, are linearly disjoint over $L$. Then $K_i$, $i \in I$, are linearly disjoint over $K$.*

*Proof:* We may assume that $I$ is a finite set. Let $K' = \prod_{i \in I} K_i$ and $L' = LK'$. Then

$$[L' : L] \le [K' : K] \le \prod_{i \in I} [K_i : K] = \prod_{i \in I} [L_i : L] = [L' : L].$$

Hence, $[K' : K] = \prod_{i \in I} [K_i : K]$. Therefore, $K_i$, $i \in I$, are linearly disjoint over $K$. ∎

The following results uses the ultrafilter $\mathcal{L}$ which Construction 2.1 introduces.

PROPOSITION 7.2: *Let $A$ be an abelian variety over a field $K$. Suppose there exist a number field $N$, a set $\Lambda \in \mathcal{L}$, and an algebraic group $H$ over $K$, such that $\Lambda \subseteq \mathrm{Splt}(N)$ and $G_{K'}(l) = H(\mathbb{F}_l)$ for each finite extension $K'$ of $K$ and each sufficiently large $l \in \Lambda$. Then, for almost all $\sigma \in \mathrm{Gal}(K)$ there are infinitely many $l \in \Lambda$ with $A_l(\tilde{K}(\sigma)) \neq 0$.*

*Proof:* Proposition 6.1 gives a prime number $l_0$, such that $L(A_l)$, $l \ge l_0$, are linearly disjoint over $L$. Making $l_0$ larger, if necessary, we get $[K(A_l) : K] = [L(A_l) : L]$ for all $l \ge l_0$. Hence, by Lemma 7.1, $K(A_l)$, $l \ge l_0$, are linearly disjoint over $K$.

We may assume $l \ge l_0$ for each $l \in \Lambda$. Let $V$ be the intersection of $H$ with the hypersurface defined by $\det(1 - \mathbf{z}) = 0$ where $\mathbf{z}$ is a $2d \times 2d$ matrix of indeterminates. Let $N'$ be a finite extension of $N$ over which all absolutely irreducible components of $V$ are defined. Let $\Lambda' = \Lambda \cap \mathrm{Splt}(N')$. Write $\tilde{S}_l = \{\sigma \in \mathrm{Gal}(K) \mid A(\tilde{K}(\sigma)) \neq 0\}$. By the preceding paragraph, the sets $\tilde{S}_l$, $l \in \Lambda$, are $\mu_K$-independent. As in the introduction or in Section 2, $\sum_{l \in \Lambda'} \mu_L(\tilde{S}_l) = \infty$. By Borel-Cantelli, almost all $\sigma \in \mathrm{Gal}(K)$ belong to infinitely many $\tilde{S}_l$. Therefore, there are infinitely many $l \in \Lambda$ with $A_l(\tilde{K}(\sigma)) \neq 0$. ∎

There are at least two cases where the assumptions of Proposition 7.2 are satisfied:

THEOREM 7.3: *Let $A$ be an abelian variety of dimension $n$ over a number field $K$. Suppose one of the following conditions holds:*

(a) *$E = \mathbb{Q} \otimes \mathrm{End}_{\mathbb{C}} A$ is a totally real number field with $[E : \mathbb{Q}] = n$ and there is a prime of $K$ at which $A$ has no potential good reduction.*

(b) *$\mathrm{End}_{\mathbb{C}} A = \mathbb{Z}$ and $\dim(A)$ is 2, 6, or an odd positive integer.*

*Then, for almost all $\sigma \in \mathrm{Gal}(K)$ there are infinitely many $l$ with $A_l(\tilde{K}(\sigma)) \neq 0$.*

*Proof:* It suffices to prove that the conditions of Proposition 7.2 hold in each of the cases.

CASE (a): Let $n = [E : \mathbb{Q}]$. Define an algebraic subgroup $H$ of $\mathrm{GL}_{2n}$ over $\mathbb{Z}$ by

$$H(R) = \left\{ \begin{pmatrix} \mathrm{Diag}(\mathbf{a}) & \mathrm{Diag}(\mathbf{b}) \\ \mathrm{Diag}(\mathbf{c}) & \mathrm{Diag}(\mathbf{d}) \end{pmatrix} \in \mathrm{GL}_{2n}(R) \mid a_i d_i - b_i c_i = a_1 d_1 - b_1 c_1,\ i = 2, \ldots, n \right\}$$

for each commutative ring $R$ with 1. Here $\mathrm{Diag}(\mathbf{a})$ is the diagonal matrix in $\mathrm{GL}_n(\mathbb{F}_l)$ with entries $a_1, \ldots, a_n$ along the main diagonal. Let $O$ be the ring of integers of $E$. Then, for all large $l$

$$G_K(l) \cong \{\mathbf{g} \in \mathrm{GL}_2(O/lO) \mid \det(\mathbf{g}) \in \mathbb{F}_l^\times\}$$

[Rib, p. 752]. Then, for all large $l \in \mathrm{Splt}(E)$, $O/lO \cong \mathbb{F}_l^n$ and there is an isomorphism of $G_K(l)$ with $H(\mathbb{F}_l)$ which is compatible with the actions of the groups on $A_l(\tilde{K})$ and $\mathbb{F}_l^{2n}$, respectively.

The same statement holds for each finite extension $K'$ of $K$, where one has to exclude possibly more $l$ than for $K$. Thus, the conditions of Proposition 7.2 hold for $N = E$ and $\Lambda = \mathrm{Splt}(E)$.

CASE (b): The conditions of Proposition 7.2 hold in this case with $N = \mathbb{Q}$, $\Lambda$ cofinite in $\mathbb{P}$, and $H = \mathrm{GSp}_{2n}$ [Ser5, p. 51, Cor.]. ∎

## References


[Bog] F. Bogomolov, *Points of finite order on abelian varieties,* Math. USSR Izvestya **17 (1)** (1981), 55–72.

[Bor1] A. Borel, *Linear algebraic groups,* Proceedings of Symposia in Pure Mathematics **IX**, American Mathematical Society, Providence, 1996, pp. 3–19.

[Bor2] A. Borel, *Linear Algebraic Groups (second enlarged edition),* Graduate Texts in Mathematics **126**, Springer-Verlag, New York, 1991.

[BoS] A. Borel and T. A. Springer, *Rationality properties of linear algebraic groups II,* Tôhoku Mathematical Journal **20** (1968), 443–497.

[CaF] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory,* Academic Press, London, 1967.

[Dem] M. Demazure, *Schémas en Groups 3 III,* Lecture Notes in Mathematics **153**, Springer-Verlag, Berlin, 1970.

[FyJ] G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields,* Proceedings of the London Mathematical Society **28** (1974), 112–128.

[FrJ] M. D. Fried and M. Jarden, *Field Arithmetic,* Ergebnisse der Mathematik (3) **11**, Springer-Verlag, Heidelberg, 1986.

[GeJ] W.-D. Geyer and M. Jarden, *Torsion points of elliptic curves over large algebraic extensions of finitely generated fields,* Israel Journal of Mathematics **31** (1978), 157–197.

[HrP] E. Hrushovski and A. Pillay, *Definable subgroups of algebraic groups over finite fields,* Journal für die reine und angewandte Mathematik **462** (1995), 69–91.

[Hum] J. E. Humphreys, *Linear Algebraic Groups,* Graduate Texts in Mathematics **21**, Springer, 1975, New York.

[JaJ1] M. Jacobson and M. Jarden, *On torsion of abelian varieties over large algebraic extensions of finitely generated fields,* Mathematika **31** (1984), 110–116.

[JaJ2] M. Jacobson and M. Jarden, *Finiteness theorems for torsion of abelian varieties over large algebraic fields,* Acta Arithmetica **98** (2001), 15–31.

[Lan1] S. Lang, *Introduction to algebraic geometry,* Interscience Publishers, New York, 1958.

[Lan2] S. Lang, *Algebra, Third Edition,* Eddison-Wesely, Reading, 1993.

[LaT] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties,* American Journal of Mathematics **80** (1958), 659–684.

[LaW] S. Lang and A. Weil, *Number of points of varieties in finite fields,* American Journal of Mathematics **76** (1954), 819–827.

[Rib] K. Ribet, *Galois action on division points of abelian varieties with real multiplication,* American Journal of Mathematics **98** (1976), 751–804.

[Ric] R. W. Richardson, Jr., *A rigidity theorem for subalgebras of Lie and associative algebras,* Illinois Journal of Mathematics 11 (1967), 92–110.

[Sat] I. Satake, *On the theory of reductive algebraic groups over a perfect field,* Journal of the Mathematical Society of Japan **15** (1963), 210–235.

[Ser1] J.-P. Serre, *Résumé des cours de 1984-1985,* Annuaire du Collège de France, Paris 1985.

[Ser2] J.-P. Serre, *Résumé des cours de 1985-1986,* Annuaire du Collège de France, Paris 1986.

[Ser3] J.-P. Serre, *Groupes linéaires modulo p et points d'ordre finite des varietés abéliennes,* Notes of a course at Collège de France, January-March 1986, taken by Eva Bayer.

[Ser4] J.-P. Serre, *Galois Cohomology,* Springer, Berlin, 1997.

[Ser5] J.-P. Serre, *Lettre á Marie-France Vignèras du 10/2/1986,* Collected Papers IV, Springer-Verlag, Berlin, 2000.

[Ser6] J.-P. Serre, *Lettre à Kenneth Ribet du 7/3/1986,* Collected Papers IV, Springer-Verlag, Berlin, 2000.

[Ser7] J.-P. Serre, *Letter to Moshe Jarden,* 4 June, 2000.

[SeT] J.-P. Serre and J. Tate, *Good reduction of abelian varieties,* Annals of Mathematics **88** (1968), 492-571.

[Spr1] T. A. Springer, *Weyl's character formula for algebraic groups,* Inventiones Mathematicae **5** (1968),

[Spr2] T. A. Springer, *Linear Algebraic Groups, Second Edition,* Birkhäuser, Boston, 1998.

[Ste] R. Steinberg, *Lectures on Chevalley Groups,* Notes, Yale University, 1967.

[Tit1] J. Tits, *Classification of algebraic semisimple groups,* Proceedings of Symposia in Pure Mathematics **IX**, American Mathematical Society, Providence, 1966, pp. 33–62.

[Tit2] J. Tits, *Algebraic and abstract simple groups,* Annals of Mathematics **80** (1964), 313–329.

[Var] V. S. Varadarajan, *Lie Groups, Lie algebras, and their Representations*, Graduate Texts in Mathematics **102**, Springer, New York, 1984.