Nagoya Math. J., **234** (2019), 46–86
DOI 10.1017/nmj.2017.33

TORSION OF ABELIAN VARIETIES OVER LARGE ALGEBRAIC EXTENSIONS OF $\mathbb{Q}$

MOSHE JARDEN AND SEBASTIAN PETERSEN

Abstract. Let K be a finitely generated extension of $\mathbb{Q}$, and let A be a nonzero abelian variety over K. Let $\tilde{K}$ be the algebraic closure of K, and let $\mathrm{Gal}(K) = \mathrm{Gal}(\tilde{K}/K)$ be the absolute Galois group of K equipped with its Haar measure. For each $\sigma \in \mathrm{Gal}(K)$, let $\tilde{K}(\sigma)$ be the fixed field of σ in $\tilde{K}$. We prove that for almost all $\sigma \in \mathrm{Gal}(K)$, there exist infinitely many prime numbers l such that A has a nonzero $\tilde{K}(\sigma)$-rational point of order l. This completes the proof of a conjecture of Geyer–Jarden from 1978 in characteristic 0.

CONTENTS

Received October 2, 2016. Revised August 18, 2017. Accepted August 18, 2017.
2010 Mathematics subject classification. 12E30.

Introduction

The goal of this work is to complete the proof of an old conjecture of Geyer–Jarden in characteristic 0. The conjecture deals with a finitely generated field K of $\mathbb{Q}$. We fix an algebraic closure $\tilde{K}$ of K. Then, the *absolute Galois group* $\mathrm{Gal}(K) = \mathrm{Gal}(\tilde{K}/K)$ of K is a profinite group. It is equipped with a unique Haar measure μ_K with $\mu_K(\mathrm{Gal}(K)) = 1$ [FrJ08, p. 378, Section 18.5]. For each positive integer $e \geqslant 1$, the group $\mathrm{Gal}(K)^e$ is equipped with the product measure, which we also denote by μ_K. We say that a certain statement holds for *almost all* $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ if the set of $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ for which that statement holds has μ_K-measure 1. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(K)^e$, we consider the field

$$\tilde{K}(\boldsymbol{\sigma}) = \{x \in \tilde{K} \mid \sigma_i x = x,\ i = 1, \ldots, e\}.$$

Given an abelian variety A over K and a positive integer m, we denote the kernel of the multiplication of A by m with A_m. For a prime number l, we write $A_{l^\infty} = \bigcup_{i=1}^{\infty} A_{l^i}$.

Conjecture A. [GeJ78, p. 260, Conjecture] *Let K be a finitely generated field over $\mathbb{Q}$, let A be a nonzero abelian variety over K, and let e be a positive integer. Then, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ the following holds:*

(a) *If $e = 1$, then there exist infinitely many prime numbers l with*

$$A_l(\tilde{K}(\sigma)) \neq 0.$$

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

(c) *If $e \geqslant 1$ and l is a prime number, then $A_{l^\infty}(\tilde{K}(\boldsymbol{\sigma}))$ is finite.*

B. Previous results. Conjecture A along with its analog to positive characteristics has been proved in [GeJ78, p. 259, Theorem 1.1] when A is an elliptic curve. The analog of the conjecture is true for an arbitrary abelian variety over a finite field [JaJ84, p. 114, Proposition 4.2]. Note that the latter paper contains a proof of Part (a) of Conjecture A and its analog

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

to positive characteristic. Unfortunately, that proof is false as indicated in [JaJ85].

Part (c) of Conjecture A along with its analog to positive characteristic and Part (b) of the conjecture appear in [JaJ01, Main Theorem].

The main result of [GeJ05] considers a nonzero abelian variety A over a number field K and says that there exists a finite Galois extension L of K such that for almost all $\sigma \in \mathrm{Gal}(L)$ there exist infinitely many primes l with $A_l(\tilde{K}(\sigma)) \neq 0$.

Finally, Zywina [Zyw16] improves [GeJ05] by proving Part (a) of Conjecture A for a number field K not only for almost all $\sigma \in \mathrm{Gal}(L)$ for some L as [GeJ05] does but for almost all $\sigma \in \mathrm{Gal}(K)$.

We generalize Zywina's result to an arbitrary finitely generated extension K of $\mathbb{Q}$.

THEOREM C. *Let A be a nonzero abelian variety over a finitely generated extension K of $\mathbb{Q}$. Then, for almost all $\sigma \in \mathrm{Gal}(K)$ there exist infinitely many prime numbers l with $A_l(\tilde{K}(\sigma)) \neq 0$.*

D. ON THE PROOF. Let $g = \dim(A)$. For each prime number l let

$$\rho_{A,l} : \mathrm{Gal}(K) \to \mathrm{GL}_{2g}(\mathbb{F}_l)$$

be the l-ic representation (also called the *mod-l representation*) of $\mathrm{Gal}(K)$ induced by the action of $\mathrm{Gal}(K)$ on the vector space A_l over $\mathbb{F}_l$ of dimension $2g$.

D1. SERRE'S THEOREM. The proof of [GeJ05] uses the main result of [Ser86]. That result deals with a number field K. Among others, it gives a finite Galois extension L of K, a positive integer n, and for each l a connected reductive subgroup H_l of $\mathrm{GL}_{2g,\mathbb{F}_l}$ such that $(H_l(\mathbb{F}_l) : \rho_{A,l}(\mathrm{Gal}(L)))$ divides n. In addition, the fields $L(A_l)$ with l ranging over all prime numbers are linearly disjoint over L. Another important feature of Serre's theorem is the existence of a set Λ of prime numbers of positive Dirichlet density, such that H_l splits over $\mathbb{F}_l$ for each $l \in \Lambda$.

D2. BOREL–CANTELLI LEMMA. For each l let

$$S_l = \{\sigma \in \mathrm{Gal}(L) \mid \rho_{A,l}(\sigma) \text{ has eigenvalue } 1\}.$$

Then, [GeJ05] proves the existence of a positive constant c and a set Λ of positive Dirichlet density such that $\mu_L(S_l) > c/l$ for each $l \in \Lambda$. Thus,

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

$\sum_{l\in\Lambda}\mu_L(S_l)=\infty$. In addition, by D1, the sets S_l with l ranging over Λ are μ_L-independent. It follows from the Borel–Cantelli lemma, that almost all $\sigma\in\mathrm{Gal}(L)$ lie in infinitely many S_l's with $l\in\Lambda$. Thus, for almost all $\sigma\in\mathrm{Gal}(L)$ there exist infinitely many l's such that $A_l(\tilde{K}(\sigma))\neq 0$, which is the desired result over L.

D3. Zywina's combinatorial approach. Zywina makes a more careful use of the Borel–Cantelli lemma. In [Zyw16] he chooses a set B of representatives of $\mathrm{Gal}(K)$ modulo $\mathrm{Gal}(L)$. For each l and every $\beta\in B$ he considers the set

$$U_{\beta,l}=\{\sigma\in\beta\mathrm{Gal}(L)\mid\rho_{A,l}(\sigma)\text{ has eigenvalue }1\}.$$

Then, he constructs a positive constant c and a set Λ_β of prime numbers having positive Dirichlet density such that

$$\mu_K(U_{\beta,l})\geqslant\frac{c}{l}\quad\text{for each }l\in\Lambda_\beta. \tag{1}$$

Again, by the Borel–Cantelli lemma, this leads to the conclusion that the μ_K-measure of the set U_β of all $\sigma\in\mathrm{Gal}(K)$ that belong to infinitely many $U_{\beta,l}$ is $\frac{1}{[L:K]}$. Since the U_β's with $\beta\in B$ are disjoint, it follows that for almost all $\sigma\in\mathrm{Gal}(K)$ there are infinitely many l's such that $A_l(\tilde{K}(\sigma))\neq 0$.

D4. Function Fields. Now assume that K is a finitely generated extension of $\mathbb{Q}$ of positive transcendence degree and choose a subfield E of K such that K/E is a regular extension of transcendence degree 1. We wish to find a place of K/E with residue field $\overline{K}$ that induces a good reduction of A onto an abelian variety $\overline{A}$ over $\overline{K}$ such that

$$\mathrm{Gal}(K(A_l)/K)\cong\mathrm{Gal}(\overline{K}(\overline{A}_l)/\overline{K}) \tag{2}$$

for at least every l in a set of positive Dirichlet density.

D5. Hilbert irreducibility theorem. The first idea that comes into mind is to use the Hilbert irreducibility theorem. However, that theorem can take care of only finitely many prime numbers, so it is of no use for our problem.

D6. Openness theorem. Instead, we choose a smooth curve S over E whose function field is K such that A has a good reduction along S and set $\hat{K}=\prod_{l\in\mathbb{L}}K(A_l)$, where $\mathbb{L}$ is the set of all prime numbers. Using a

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

combination of results of Anna Cadoret and Akio Tamagawa that goes under the heading “openness theorem” (Proposition 1.6), we find a closed point $\mathbf{s}$ of S with an open decomposition group in $\mathrm{Gal}(\hat{K}/K)$. Let $\overline{K}_{\mathbf{s}}$ be the residue field of K at $\mathbf{s}$ and $\hat{K}_{\mathbf{s}} = \prod_{l\in\mathbb{L}} \overline{K}_{\mathbf{s}}(A_{\mathbf{s},l})$, where $A_{\mathbf{s}}$ is the reduction of A at $\mathbf{s}$. Then, there exists a finite extension K' of K in $\hat{K}$ such that the reduction modulo $\mathbf{s}$ induces an isomorphism $\mathrm{Gal}(\hat{K}/K') \cong \mathrm{Gal}(\hat{K}_{\mathbf{s}}/\overline{K}_{\mathbf{s}})$. This gives the desired isomorphism (2) for K' rather than for K and for all prime numbers l.

D7. Serre’s theorem over K. Now we use a result of [GaP13] and find a finite Galois extension L of K that contains K' and satisfies the same reduction conditions that K' does and in addition the fields $L(A_l)$, with l ranging over all prime numbers, are linearly disjoint over L.

Note that $\overline{K}_{\mathbf{s}}$ is again finitely generated over $\mathbb{Q}$ and the transcendence degree of $\overline{K}_{\mathbf{s}}$ over $\mathbb{Q}$ is one less than that of K. Starting with Serre’s theorem for number fields mentioned above and using induction on the transcendence degree over $\mathbb{Q}$, we now prove the theorem of Serre mentioned in D1 over our current field K.

D8. Strongly regular points. Having Serre’s theorem for our function field K at our disposal, we now follow the proof of [Zyw16] to obtain the estimates (1) for our abelian variety A/K. The proof contains a careful analysis of regular points of the reductive groups H_l mentioned in Serre’s theorem for $l \in \Lambda$. It uses Zywina’s crucial observation that if T is an $\mathbb{F}_l$-split maximal torus of H_l and $\mathbf{t} \in T(\mathbb{F}_l)$, then $\mathbf{t}^{n!} \in \rho_{A,l}(\mathrm{Gal}(L))$. Moreover, if $\mathbf{t}$ is a regular element of H_l and T is the unique maximal torus of H_l that contains $\mathbf{t}$, then the number of points $\mathbf{t}' \in T(\mathbb{F}_l)$ with $(\mathbf{t}')^{n!} = \mathbf{t}^{n!}$ is at most $(n!)^r$, where $r = \mathrm{rank}(H_l) = \dim(T)$. Finally, still following [Zyw16], we make use of the Lang–Weil estimates (or rather the more accurate version of these estimates that [Zyw16] provides) to prove that “most of the points” of $\rho_{A,l}(\mathrm{Gal}(K))$ are regular points of H_l whose characteristic polynomials have “maximal numbers of roots in $\mathbb{F}_l$.” (We may refer to these points as “strongly regular.”)

D9. Serre’s density theorem. At some point of the proof, [Zyw16] uses the Chebotarev density theorem for number fields to choose a prime of K whose Artin class is equal to a previously chosen conjugacy class in $\mathrm{Gal}(L(A_l)/K)$ (where L is the number field mentioned in Serre’s theorem for number field). Instead, we use Serre’s generalization of the Chebotarev

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

density theorem (Proposition 3.5) to our function field K in order to find a prime $\mathfrak{p}$ of K with the same properties as above.

§1. Adelic openness

Let K be a finitely generated transcendental extension of $\mathbb{Q}$, and let A be an abelian variety over K. We consider K as a function field of one variable over a field E. Using results of Cadoret and Tamagawa, we prove that there exists a finite extension K' of K in $\hat{K} = \prod_l K(A_l)$, with l ranging over all prime numbers, such that the reduction modulo "almost every valuation v of K' over E" maps the group $\mathrm{Gal}(K'(A_l)/K')$, for each l, isomorphically onto the corresponding group with respect to the reduced objects.

To be more specific, let E be a finitely generated extension of $\mathbb{Q}$, S an absolutely integral smooth curve over E, $K = E(S)$ the function field of S, and A an abelian variety over K of dimension $g > 0$ with good reduction along S [Shi98, p. 95, Proposition 25]. Let $A(\tilde{K})$ be the abelian group of all $\tilde{K}$-rational points of A. For each $m \in \mathbb{N}$, let A_m be the kernel of multiplication of A by m. By [Mil85, p. 116, Remark 8.4], $A_m(\tilde{K})$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank $2g$. Moreover, since A is defined over K, each $\sigma \in \mathrm{Gal}(K)$ gives rise to an automorphism of $A(\tilde{K})$ that leaves $A_m(\tilde{K})$ invariant.

We denote the set of all prime numbers by $\mathbb{L}$. For each $l \in \mathbb{L}$, let $T_l(A) = \varprojlim A_{l^i}(\tilde{K})$ be the Tate module of A associated with l. Then, $A_l(\tilde{K}) \cong \mathbb{F}_l^{2g}$ and $T_l(A) \cong \mathbb{Z}_l^{2g}$, so $\mathrm{Aut}(A_l) \cong \mathrm{GL}_{2g}(\mathbb{F}_l)$ and $\mathrm{Aut}(T_l(A)) \cong \mathrm{GL}_{2g}(\mathbb{Z}_l)$. Thus, the action of $\mathrm{Gal}(K)$ on $A(\tilde{K})$ mentioned in the preceding paragraph gives rise to homomorphisms

$$(1) \qquad \rho_{A,l} : \mathrm{Gal}(K) \to \mathrm{GL}_{2g}(\mathbb{F}_l), \qquad \rho_{A,l^\infty} : \mathrm{Gal}(K) \to \mathrm{GL}_{2g}(\mathbb{Z}_l).$$

Since $\mathrm{Ker}(\rho_{A,l}) = \mathrm{Gal}(K(A_l))$ and

$$\mathrm{Ker}(\rho_{A,l^\infty}) = \mathrm{Gal}(K(A_{l^\infty})) = \mathrm{Gal}\left(\bigcup_{i=1}^{\infty} K(A_{l^i})\right),$$

the homomorphism $\rho_{A,l}$ (resp. ρ_{A,l^∞}) (also called the l-ic and the l-adic representations of $\mathrm{Gal}(K)$) induces (under an abuse of notation) a homomorphism $\rho_{A,l} : \mathrm{Gal}(N/K) \to \mathrm{GL}_{2g}(\mathbb{F}_l)$ (resp. $\rho_{A,l^\infty} : \mathrm{Gal}(N/K) \to \mathrm{GL}_{2g}(\mathbb{Z}_l)$) for each Galois extension N of K that contains $K(A_l)$ (resp. $K(A_{l^\infty})$).

We denote the set of closed points of S by S_{closed}. By Hilbert Nullstellensatz, S_{closed} is an infinite set.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

Since S is a smooth curve, each $\mathbf{s} \in S_{\mathrm{closed}}$ induces a discrete valuation $v_{\mathbf{s}}$ of K with residue field $\overline{K}_{\mathbf{s}}$, which is a finite extension of E in $\tilde{E}$ [Lan58, p. 151, Theorem 1] and where $\tilde{E}$ is the algebraic closure of E in $\tilde{K}$.

Let $K_{\mathrm{ur}} = K_{\mathrm{ur},S}$ be the maximal Galois extension of K, which is unramified along S, and observe that $\tilde{E} \subseteq K_{\mathrm{ur}}$, because $\mathrm{char}(E) = 0$. Thus, $\mathrm{Gal}(K_{\mathrm{ur}}/K)$ is the étale fundamental group of S. Since $\mathrm{char}(\overline{K}_{\mathbf{s}}) = 0$ for each $\mathbf{s} \in S_{\mathrm{closed}}$, [SeT68, Theorem 1] implies that

$$K(A_m) \subseteq K_{\mathrm{ur}} \text{ for each } m \in \mathbb{N}. \tag{2}$$

By what we said above, $\rho_{A,l}$ and ρ_{A,l^∞} give rise to homomorphisms

$$\rho_l : \mathrm{Gal}(K_{\mathrm{ur}}/K) \to \mathrm{Aut}(A_l), \qquad \rho_{l^\infty} : \mathrm{Gal}(K_{\mathrm{ur}}/K) \to \mathrm{Aut}(T_l(A)).$$

Writing $\pi_l : \mathrm{Aut}(T_l(A)) \to \mathrm{Aut}(A_l)$ for the epimorphism defined by the reduction $\mathrm{GL}_{2g}(\mathbb{Z}_l) \to \mathrm{GL}_{2g}(\mathbb{F}_l)$ modulo l, we have $\rho_l = \pi_l \circ \rho_{l^\infty}$. Further, the products of the ρ_l's, the ρ_{l^∞}'s, and the π_l's, with l ranging over $\mathbb{L}$, give rise to homomorphisms that fit into the following commutative diagram:

$$\begin{tikzcd} & \mathrm{Gal}(K_{\mathrm{ur}}/K) \arrow[dl, "\rho_\infty"'] \arrow[dr, "\rho"] & \\ \prod_{l\in\mathbb{L}} \mathrm{Aut}(T_l(A)) \arrow[rr, "\pi"] & & \prod_{l\in\mathbb{L}} \mathrm{Aut}(A_l). \end{tikzcd} \tag{3}$$

Next we consider a point $\mathbf{s} \in S_{\mathrm{closed}}$ and choose an extension $v_{\mathbf{s},\mathrm{ur}}$ of $v_{\mathbf{s}}$ to K_{ur}. Since $\tilde{E} \subseteq K_{\mathrm{ur}}$, the residue field of $v_{\mathbf{s},\mathrm{ur}}$ is $\tilde{E}$. For each Galois extension L of K in K_{ur} we consider the decomposition group of $v_{\mathbf{s},\mathrm{ur}}|_L$ over K,

$$D_{\mathbf{s},L/K} = \{\sigma \in \mathrm{Gal}(L/K) \mid \text{ for all } x \in L : v_{\mathbf{s},\mathrm{ur}}(\sigma x) \geqslant 0 \Leftrightarrow v_{\mathbf{s},\mathrm{ur}}(x) \geqslant 0\}.$$

Since $v_{s,\mathrm{ur}}/v_{\mathbf{s}}$ is unramified, reduction modulo the prime ideal of the valuation ring of $v_{\mathbf{s},\mathrm{ur}}$ gives rise to an isomorphism $\varphi_{\mathbf{s}} : D_{\mathbf{s},K_{\mathrm{ur}}/K} \to \mathrm{Gal}(\overline{K}_{\mathbf{s}})$ [EnP10, second paragraph of p. 123 and the “first exact sequence” on p. 124].

(4) Let $\psi_{\mathbf{s}} : \mathrm{Gal}(\overline{K}_{\mathbf{s}}) \to D_{\mathbf{s},K_{\mathrm{ur}}/K}$ be the inverse of $\varphi_{\mathbf{s}}$. For each $l \in \mathbb{L}$ we consider the homomorphism $\rho_{l^\infty,\mathbf{s}} = \rho_{l^\infty} \circ \psi_{\mathbf{s}} : \mathrm{Gal}(\overline{K}_{\mathbf{s}}) \to \mathrm{Aut}(T_l(A))$. It satisfies $\rho_{l^\infty,\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}})) = \rho_{l^\infty}(D_{\mathbf{s},K_{\mathrm{ur}}/K})$. We also consider the homomorphisms

$$\rho_s = \rho \circ \psi_{\mathbf{s}} : \mathrm{Gal}(\overline{K}_{\mathbf{s}}) \to \prod_{l\in\mathbb{L}} \mathrm{Aut}(A_l)$$

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

and

$$\rho_{\infty,\mathbf{s}} = \rho_\infty \circ \psi_{\mathbf{s}} : \mathrm{Gal}(\overline{K}_{\mathbf{s}}) \to \prod_{l\in\mathbb{L}} \mathrm{Aut}(T_l(A)).$$

They satisfy

$$\rho_s(\mathrm{Gal}(\overline{K}_{\mathbf{s}})) = \rho(D_{\mathbf{s},K_{\mathrm{ur}}/K}) \quad \text{and} \quad \rho_{\infty,\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}})) = \rho_\infty(D_{\mathbf{s},K_{\mathrm{ur}}/K}).$$

The following result of Anna Cadoret is the main theorem of [Cad15], rewritten in our notation:

PROPOSITION 1.1. *We consider a point $\mathbf{s} \in S_{\mathrm{closed}}$. If there exists $l \in \mathbb{L}$ such that the group $\rho_{l^\infty,\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$ is open in $\rho_{l^\infty}(\mathrm{Gal}(K_{\mathrm{ur}}/K))$, then $\rho_{\infty,\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$ is open in $\rho_\infty(\mathrm{Gal}(K_{\mathrm{ur}}/K))$.*

Our goal is to prove the assumption of Proposition 1.1, hence to make the consequence of that theorem valid. To this end, we combine two theorems of Cadoret and Tamagawa.

PROPOSITION 1.2. (Cadoret–Tamagawa) *Given $l \in \mathbb{L}$ and $d \in \mathbb{N}$, we set $S^{(d)} = \{\mathbf{s} \in S_{\mathrm{closed}} \mid [\overline{K}_{\mathbf{s}} : E] \leqslant d\}$ and consider the set*

$$S_l = \{\mathbf{s} \in S_{\mathrm{closed}} \mid \rho_{l^\infty,\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}})) \textit{ is not open in } \rho_{l^\infty}(\mathrm{Gal}(K_{\mathrm{ur}}/K))\}.$$

Then, $S_l \cap S^{(d)}$ is finite.

Proof. By [CaT12, Theorem 5.1], ρ_{l^∞} is a *GSRP representation*. In other words, the maximal abelian quotient of each open subgroup of the group $\rho_{l^\infty}(\mathrm{Gal}(K_{\mathrm{ur}}/\tilde{E}K))$ is finite. It follows from [CaT13, Theorem 1.1] that $S_l \cap S^{(d)}$ is finite, as claimed. ∎

COROLLARY 1.3. *There exists $\mathbf{s} \in S_{\mathrm{closed}}$ such that the group $\rho_{\infty,\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$ is open in $\rho_\infty(\mathrm{Gal}(K_{\mathrm{ur}}/K))$.*

Proof. Since K is the function field of the curve S over E, there exists $t \in K$, which is transcendental over E such that $d = [K : E(t)] < \infty$. For all but finitely many elements $\bar{t} \in E$, the map $t \to \bar{t}$ gives rise to a point $\mathbf{s} \in S_{\mathrm{closed}}$ such that $[\overline{K}_{\mathbf{s}} : E] \leqslant d$. Hence, $S^{(d)}$ is infinite.

Now we choose $l \in \mathbb{L}$. By Proposition 1.2 and the preceding paragraph, the set $S^{(d)} \smallsetminus S_l$ is infinite. Thus, there exists $\mathbf{s} \in S_{\mathrm{closed}}$ such that $\rho_{l^\infty,\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$ is open in $\rho_{l^\infty}(\mathrm{Gal}(K_{\mathrm{ur}}/K))$. It follows from Proposition 1.1 that $\rho_{\infty,\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$ is open in $\rho_\infty(\mathrm{Gal}(K_{\mathrm{ur}}/K))$, as claimed. ∎

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

COROLLARY 1.4. *There exists* $\mathbf{s} \in S_{\mathrm{closed}}$ *such that the group* $\rho_{\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$ *is open in* $\rho(\mathrm{Gal}(K_{\mathrm{ur}}/K))$.

Proof. Let $\mathbf{s}$ be a point in S_{closed} that satisfies the conclusion of Corollary 1.3. Then, by (4), the commutative diagram (3) extends to a commutative diagram

$$\begin{tikzcd}
 & \mathrm{Gal}(\overline{K}_{\mathbf{s}}) \arrow[d, "\psi_{\mathbf{s}}"] \arrow[ddl, "\rho_{\infty,\mathbf{s}}"'] \arrow[ddr, "\rho_{\mathbf{s}}"] & \\
 & \mathrm{Gal}(K_{\mathrm{ur}}/K) \arrow[dl, "\rho_{\infty}"'] \arrow[dr, "\rho"] & \\
\prod_{l \in \mathbb{L}} \mathrm{Aut}(T_l(A)) \arrow[rr, "\pi"] & & \prod_{l \in \mathbb{L}} \mathrm{Aut}(A_l)\,.
\end{tikzcd} \tag{5}$$

In particular,

$$\pi(\rho_{\infty,\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))) = \rho_{\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$$

and

$$\pi(\rho_{\infty}(\mathrm{Gal}(K_{\mathrm{ur}}/K))) = \rho(\mathrm{Gal}(K_{\mathrm{ur}}/K)).$$

By Corollary 1.3, $\rho_{\infty,\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$ is open in $\rho_{\infty}(\mathrm{Gal}(K_{\mathrm{ur}}/K))$. By [FrJ08, p. 5], π is an open map. Therefore, $\rho_{\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$ is open in $\rho(\mathrm{Gal}(K_{\mathrm{ur}}/K))$. □

Setup 1.5. We interpret Corollary 1.4 in terms of Galois groups. To this end, we fix a point $\mathbf{s} \in S_{\mathrm{closed}}$ such that $\rho_{\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$ is open in $\rho(\mathrm{Gal}(K_{\mathrm{ur}}/K))$. Since A has good reduction at $\mathbf{s}$, its reduction $A_{\mathbf{s}}$ with respect to $v_{\mathbf{s}}$ is an abelian variety over $\overline{K}_{\mathbf{s}}$; in particular, it is nonempty and absolutely integral [Shi98, p. 83, Section 11.1]. Moreover, by the last paragraph of [Shi98, p. 70], $\dim(A_{\mathbf{s}}) = \dim(A) = g$. We write $\hat{K} = \prod_{l \in \mathbb{L}} K(A_l)$ and $\hat{K}_{\mathbf{s}} = \prod_{l \in \mathbb{L}} \overline{K}_{\mathbf{s}}(A_{\mathbf{s},l})$. By (2), $\hat{K} \subseteq K_{\mathrm{ur}}$. Moreover, by [SeT68, p. 495, Lemma 2], for each $l \in \mathbb{L}$, reduction modulo $\mathbf{s}$ induces an isomorphism $A_l(\tilde{K}) \to A_{\mathbf{s},l}(\widetilde{\overline{K}_{\mathbf{s}}})$.

We denote the restriction of $v_{\mathbf{s},\mathrm{ur}}$ to $\hat{K}$ by $\hat{v}_{\mathbf{s}}$. Then, $\hat{K}_{\mathbf{s}}$ is the residue field of $\hat{K}$ with respect to $\hat{v}_{\mathbf{s}}$. Also, $D_{\mathbf{s},\hat{K}/K}$ is the image of $D_{\mathbf{s},K_{\mathrm{ur}}/K}$ under the restriction map $\mathrm{res}: \mathrm{Gal}(K_{\mathrm{ur}}/K) \to \mathrm{Gal}(\hat{K}/K)$. We write K' for the fixed field of $D_{\mathbf{s},\hat{K}/K}$ in $\hat{K}$ (and note that K' depends on $\mathbf{s}$). Then, $\psi_{\mathbf{s}}$ induces a monomorphism $\hat{\psi}_{\mathbf{s}}: \mathrm{Gal}(\hat{K}_{\mathbf{s}}/\overline{K}_{\mathbf{s}}) \to \mathrm{Gal}(\hat{K}/K)$ whose image is

$\mathrm{Gal}(\hat{K}/K')$. Let $\hat{\varphi}_{\mathbf{s}} : \mathrm{Gal}(\hat{K}/K') \to \mathrm{Gal}(\hat{K}_{\mathbf{s}}/\overline{K}_{\mathbf{s}})$ be the inverse of $\hat{\psi}_{\mathbf{s}}$. Again, by [SeT68, p. 495, Lemma 2], the isomorphism $A_l(\tilde{K}) \to A_{\mathbf{s},l}(\widetilde{\overline{K}_{\mathbf{s}}})$ induces an isomorphism $\alpha_l : \mathrm{Aut}(A_l) \to \mathrm{Aut}(A_{\mathbf{s},l})$ that commutes with the action of $\mathrm{Gal}(\hat{K}/K')$. Thus, $\alpha_l \circ \rho_{A,l}|_{\mathrm{Gal}(\hat{K}/K')} = \rho_{A_{\mathbf{s}},l} \circ \hat{\varphi}_{\mathbf{s}}|_{\mathrm{Gal}(\hat{K}_{\mathbf{s}}/\overline{K}_{\mathbf{s}})}$ for each $l \in \mathbb{L}$. The product of the α_l's gives rise to an isomorphism $\alpha : \prod_{l\in\mathbb{L}} \mathrm{Aut}(A_l) \to \prod_{l\in\mathbb{L}} \mathrm{Aut}(A_{\mathbf{s},l})$.

PROPOSITION 1.6. *In the notation of Setup 1.5 and in particular with the choice of the closed point* $\mathbf{s}$ *of* S *made in the Setup,* K' *is a finite extension of* K *in* $\hat{K}$*.*

Proof. Observe that $\rho : \mathrm{Gal}(K_{\mathrm{ur}}/K) \to \prod_{l\in\mathbb{L}} \mathrm{Aut}(A_l)$ naturally decomposes as $\rho = \hat{\rho} \circ \mathrm{res}_{K_{\mathrm{ur}}/\hat{K}}$, where $\hat{\rho} : \mathrm{Gal}(\hat{K}/K) \to \prod_{l\in\mathbb{L}} \mathrm{Aut}(A_l)$ is defined by the action of $\mathrm{Gal}(\hat{K}/K)$ on the A_l's. Since $\hat{K} = \prod_{l\in\mathbb{L}} K(A_l)$, the homomorphism $\hat{\rho}$ is injective.

Similarly, we write $\rho'_{\mathbf{s}} : \mathrm{Gal}(\hat{K}_{\mathbf{s}}/\overline{K}_{\mathbf{s}}) \to \prod_{l\in\mathbb{L}} \mathrm{Aut}(A_{\mathbf{s},l})$ for the corresponding monomorphism associated with $\overline{K}_{\mathbf{s}}$ and $A_{\mathbf{s}}$. It fits into the following commutative diagram:

(6)
$$\begin{tikzcd}
\mathrm{Gal}(K_{\mathrm{ur}}/K) \arrow[r, "\mathrm{res}"] \arrow[rr, bend left, "\rho"] & \mathrm{Gal}(\hat{K}/K) \arrow[r, "\hat{\rho}"] & \prod_{l\in\mathbb{L}} \mathrm{Aut}(A_l) \arrow[d, "\alpha"] \\
\mathrm{Gal}(\overline{K}_s) \arrow[u, "\psi_{\mathbf{s}}"] \arrow[r, "\mathrm{res}"] \arrow[rr, bend right, "\rho_{\mathbf{s}}"'] & \mathrm{Gal}(\hat{K}_{\mathbf{s}}/\overline{K}_{\mathbf{s}}) \arrow[u, "\hat{\psi}_{\mathbf{s}}"] \arrow[r, "\rho'_{\mathbf{s}}"] & \prod_{l\in\mathbb{L}} \mathrm{Aut}(A_{\mathbf{s},l}).
\end{tikzcd}$$

Note that in the notation of Corollary 1.4, $\rho'_{\mathbf{s}} \circ \mathrm{res}_{\widetilde{\overline{K}_{\mathbf{s}}}/\hat{K}_{\mathbf{s}}} = \rho_{\mathbf{s}}$. We use Corollary 1.4 in order to choose $\mathbf{s} \in S(\tilde{E})$ such that the group $\rho_{\mathbf{s}}(\mathrm{Gal}(\overline{K}_{\mathbf{s}}))$ is open in $\rho(\mathrm{Gal}(K_{\mathrm{ur}}/K))$. Since both restriction maps in (6) are surjective, $\alpha^{-1}(\rho'_{\mathbf{s}}(\mathrm{Gal}(\hat{K}_{\mathbf{s}}/\overline{K}_{\mathbf{s}})))$ is open in $\hat{\rho}(\mathrm{Gal}(\hat{K}/K))$. Since $\hat{\psi}_{\mathbf{s}}$ is injective, since α is bijective, and since both $\rho'_{\mathbf{s}}$ and $\hat{\rho}$ are injective, the group $D_{\mathbf{s},\hat{K}/K} = \hat{\psi}_{\mathbf{s}}(\mathrm{Gal}(\hat{K}_{\mathbf{s}}/\overline{K}_{\mathbf{s}}))$ is open in $\mathrm{Gal}(\hat{K}/K)$. It follows that K', which is the fixed field of $D_{\mathbf{s},\hat{K}/K}$ in $\hat{K}$, is a finite extension of K in $\hat{K}$, as claimed. □

§2. Independent homomorphisms

Let Γ be a profinite group, and let I be a set. For each $i \in I$ let ρ_i be a homomorphism of Γ into a profinite group Γ_i. Here we follow the usual

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

convention and always assume that a homomorphism between profinite groups is continuous. In addition, every finite group is equipped with the discrete topology. Let $\rho = \prod_{i\in I} \rho_i$ be the *direct product* of the ρ_i's. That is, ρ is the homomorphism from Γ to $\prod_{i\in I} \Gamma_i$ defined by $\rho(x) = (\rho_i(x))_{i\in I}$. Following [Ser13] and [GaP13], we say that the family $(\rho_i)_{i\in I}$ is *independent* if $\rho(\Gamma) = \prod_{i\in I} \rho_i(\Gamma)$.

Note that if a family $(\rho_i)_{i\in I}$ of homomorphisms as in the preceding paragraph is independent and $\alpha : \Gamma' \to \Gamma$ is an epimorphism of profinite groups, then the family $(\rho_i \circ \alpha)_{i\in I}$ is also independent.

LEMMA 2.1. *Let $(G_i)_{i\in I}$ be a family of closed subgroups of a profinite group G, and let H be an open subgroup of G. Suppose that $\bigcap_{i\in I} G_i = 1$. Then, I has a finite subset J such that $\bigcap_{i\in J} G_i \leqslant H$.*

Proof. Assume toward contradiction that the lemma does not hold. Then, for each finite subset J of I the closed subset $\bigcap_{j\in J} G_j \smallsetminus H$ is nonempty. If J' is a finite subset of I that contains J, then $\bigcap_{j\in J'} G_j \smallsetminus H \subseteq \bigcap_{j\in J} G_j \smallsetminus H$. It follows from the compactness of G that the set $\bigcap_{i\in I} G_i \smallsetminus H$ is nonempty. This contradicts the assumption that $\bigcap_{i\in I} G_i = 1 \in H$. □

One of the ingredients of the proof of the following lemma appears in [GaP13, Remark 3.2(b)(ii)].

LEMMA 2.2. *Let Γ be a profinite group. For each i in a set I, let ρ_i be a homomorphism of Γ into a finite group Γ_i. Suppose that the family $(\rho_i)_{i\in I}$ is independent, $\bigcap_{i\in I} \mathrm{Ker}(\rho_i) = 1$, and Δ is an open subgroup of Γ. Then, Δ has an open subgroup Δ', which is normal in Γ such that the family $(\rho_i|_{\Delta'})_{i\in I}$ is independent.*

Proof. By assumption, the homomorphism $\rho = \prod_{i\in I} \rho_i$ satisfies $\rho(\Gamma) = \prod_{i\in I} \rho_i(\Gamma)$. Since Δ is open in Γ, the subgroup $\rho(\Delta)$ of $\prod_{i\in I} \rho_i(\Gamma)$ is open [FrJ08, p. 6, Remark 1.2.1(f)]. Thus, I has a finite subset J such that $\prod_{i\in J} \mathbf{1} \times \prod_{i\in I\smallsetminus J} \rho_i(\Gamma) \leqslant \rho(\Delta)$.

Since $\bigcap_{i\in I} \mathrm{Ker}(\rho_i) = \mathbf{1}$, we may use Lemma 2.1 to enlarge J such that $\Delta' = \bigcap_{i\in J} \mathrm{Ker}(\rho_i) \leqslant \Delta$. In particular, Δ' is normal in Γ. Since the Γ_i's are finite, Δ' is open in Δ.

Given a family $(x_i)_{i\in I}$ in $(\Delta')^I$, we have $\rho_i(x_i) = 1$ for each $i \in J$. Thus, $(\rho_i(x_i))_{i\in I} \in \prod_{i\in J} \mathbf{1} \times \prod_{i\in I\smallsetminus J} \rho_i(\Gamma) \leqslant \rho(\Delta)$. Hence, there exist $x \in \Delta$ with $\rho(x) = (\rho_i(x_i))_{i\in I}$. In particular, $\rho_i(x) = \rho_i(x_i) = 1$ for each $i \in J$, so $x \in \Delta'$. It follows that $\rho(\Delta') = \prod_{i\in I} \rho_i(\Delta')$. This means that the family $(\rho_i|_{\Delta'})_{i\in I}$ is independent, as claimed. □

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

REMARK 2.3. Let K be a field. For each $i \in I$ let $\rho_i : \mathrm{Gal}(K) \to G_i$ be a homomorphism of profinite groups, and let K_i be the fixed field of $\mathrm{Ker}(\rho_i)$ in $\tilde{K}$. Consider a Galois extension $\hat{K}$ of K in $\tilde{K}$ that contains each K_i and let $\hat{\rho}_i : \mathrm{Gal}(\hat{K}/K) \to G_i$ be the homomorphism induced by ρ_i. As noticed in [GaP13, Remark 3.1], the family $(K_i)_{i \in I}$ is linearly disjoint over K if and only if the restriction maps

$$\hat{\rho}_i : \mathrm{Gal}(\hat{K}/K) \to G_i, \quad i \in I$$

are independent (see also [FrJ08, Lemma 2.5.6]).

§3. Serre's density theorem

We give in this section an account of a generalization of the Chebotarev density theorem to finitely generated extensions of $\mathbb{Q}$ due to Jean-Pierre Serre. We call this generalization "Serre's density theorem."

3.1 Nagata rings

Recall that a Noetherian ring A (commutative with 1) is called a *Nagata ring* if for every prime ideal P of A and for every finite extension L of $\mathrm{Quot}(A/P)$ the integral closure of A/P in L is a finitely generated A/P-module (see [Mat80, p. 231] or [Liu06, p. 340, Definition 2.27]). In particular, every field and every Dedekind domain of characteristic 0 are Nagata rings [Liu06, p. 340, Example 2.28]. It follows from the definition that if A is a Nagata ring and U is a multiplicative subset of A, then $U^{-1}A$ is also a Nagata ring. The main theorem about Nagata rings, due to Nagata, says that each finitely generated ring extension of a Nagata ring is again a Nagata ring [Mat80, p. 240, Theorem 72]. In particular, every finitely generated $\mathbb{Z}$-algebra is a Nagata ring.

3.2 Regular rings

Let K be a finitely generated extension of $\mathbb{Q}$ and let L be a finite Galois extension of K, and choose a transcendence base $(t_1, \ldots, t_r)$ for $K/\mathbb{Q}$. By Section 3.1, $R_0 = \mathbb{Z}[t_1, \ldots, t_r]$ is a Nagata ring and the Krull dimension, $\dim(R_0)$, of R_0 is $r + 1 = \mathrm{trans.deg}(K/\mathbb{Q}) + 1$. Therefore, the integral closure R of R_0 in K is a finitely generated R_0-module with $\mathrm{Quot}(R) = K$. Thus, $R = \mathbb{Z}[x_1, \ldots, x_k]$ for some $x_1, \ldots, x_k \in K$ and R is a Nagata ring with $\dim(R) = \dim(R_0) = \mathrm{trans.deg}(K/\mathbb{Q}) + 1$. The set

$$U = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid R_{\mathfrak{p}} \text{ is a regular ring}\}$$

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

is open in $\mathrm{Spec}(R)$ [Gro65, p. 166, Corollary 6.12.6]. Moreover, U is nonempty, because it contains the generic point of $\mathrm{Spec}(R)$. Therefore, there exists a nonzero element $f \in R$ such that $\mathrm{Spec}(R[f^{-1}]) \subseteq U$. In particular, the ring $R[f^{-1}]$ is regular. Adding f^{-1} to the set $\{x_1, \ldots, x_k\}$, if necessary, we may assume that $\mathrm{Spec}(R)$ is smooth, so R is a regular ring.

Since R is a Nagata ring, its integral closure R_L in L is a finitely generated R-module, hence a finitely generated ring extension of $\mathbb{Z}$. Moreover, the fixed ring of R_L under $\mathrm{Gal}(L/K)$ is R. Hence, $\mathrm{Spec}(R)$ is isomorphic to the quotient scheme of $\mathrm{Spec}(R_L)$ modulo $\mathrm{Gal}(L/K)$, where $\mathrm{Gal}(L/K)$ acts on $\mathrm{Spec}(R_L)$ in the natural way [GoW10, p. 331, Proposition 12.27]. Finally, we replace R and R_L by $R[u]$ and $R_L[u]$, if necessary, where u is an appropriate element of $K^\times$, to assume that R_L is a *ring cover* of R in the terminology of [FrJ08, p. 109, Remark 6.1.5]. This means that $R_L = R[z]$, where $\mathrm{discr}(\mathrm{irr}(z, K))$ is a unit of R and $\mathrm{irr}(z, K)$ is the monic irreducible polynomial of z over K. In particular, R_L is *standard étale* over R [Ray70, p. 19, (2)].

3.3 Dirichlet density

We denote the set of maximal ideals of R by $\mathrm{Max}(R)$. For each $\mathfrak{p} \in \mathrm{Max}(R)$, the residue ring $R/\mathfrak{p}$ is a finite field (see [Ser65, p. 83, Section 1.3] or [Eis95, p. 132, Theorem 4.19]) and we set $N\mathfrak{p} = |R/\mathfrak{p}|$. Note that $\mathrm{Max}(R)$ (resp. $\mathrm{Max}(R_L)$) is the set of closed points of $\mathrm{Spec}(R)$ (resp. $\mathrm{Spec}(R_L)$).

This allows us to use the notation and the results of [Ser65, Section 2.7] for $X = \mathrm{Spec}(R_L)$, $G = \mathrm{Gal}(L/K)$, and $Y = \mathrm{Spec}(R)$. Let $d = \dim(Y)$. Then, $d = \mathrm{trans.deg}(K) + 1$. Accordingly, the *Dirichlet density* of a subset B of $\mathrm{Max}(R)$ is defined as the limit

$$\delta(B) = \lim_{s \to d^+} \frac{\sum_{\mathfrak{p} \in B} (1/N\mathfrak{p}^s)}{\sum_{\mathfrak{p} \in \mathrm{Max}(R)} (1/N\mathfrak{p}^s)}, \tag{1}$$

if it exists. By [Ser65, p. 84, Corollary 2], the denominator of the fraction in (1) diverges as $s \to d^+$. Hence, $\delta(B) = 0$ if B is finite. In other words, if $\delta(B) > 0$, then B is infinite.

3.4 Artin symbols

Next we consider $\mathfrak{p} \in \mathrm{Max}(R)$ and choose $\mathfrak{p}_L \in \mathrm{Max}(R_L)$ over $\mathfrak{p}$. Then, $R_L/\mathfrak{p}_L$ is a finite Galois extension of the finite field $R/\mathfrak{p}$. By our choice of R and R_L, the maximal ideal $\mathfrak{p}_L$ is unramified over R, so the decomposition group $D = D_{\mathfrak{p}_L/\mathfrak{p}}$ of $\mathfrak{p}_L$ over $\mathfrak{p}$ is isomorphic to $\overline{D} = \mathrm{Gal}((R_L/\mathfrak{p}_L)/(R/\mathfrak{p}))$ [FrJ08, p. 109, Lemma 6.1.4]. As usual we denote the element of D that corresponds to the Frobenius element of $\overline{D}$ by $[\frac{L/K}{\mathfrak{p}_L}]$ and the conjugacy class of $[\frac{L/K}{\mathfrak{p}_L}]$ in $G = \mathrm{Gal}(L/K)$ by $(\frac{L/K}{\mathfrak{p}})$. This conjugacy class does not depend on the choice of $\mathfrak{p}_L$. If L' is a finite Galois extension of K that contains L and $\mathfrak{p}$ is unramified in $R_{L'}$, then our definition implies that $(\frac{L'/K}{\mathfrak{p}})|_L = (\frac{L/K}{\mathfrak{p}})$.

With this notation, we may now state the *Serre density theorem* (that Serre calls the "Artin–Chebotarev density theorem").

PROPOSITION 3.5. [Ser65, p. 258, Theorem 7] *In the above notation, let C be a conjugacy class of G. Then, the Dirichlet density of the set of all $\mathfrak{p} \in \mathrm{Max}(R)$ such that $(\frac{L/K}{\mathfrak{p}}) = C$ is equal to $|C|/|G|$. In particular, that set is infinite.*

In the case where K is a number field, Proposition 3.5 reduces to the usual Chebotarev density theorem.

§4. Images of l-ic representations

Let A be an abelian variety over a number field K. Using previous results of Faltings and Nori, Serre proved the existence of a finite Galois extension L of K with a great amount of information about the groups $\rho_{A,l}(\mathrm{Gal}(L))$. We use Proposition 1.6 to generalize Serre's result to finitely generated extensions of $\mathbb{Q}$, but limit our generalization only to properties we need in what follows.

PROPOSITION 4.1. *Let A be an abelian variety of positive dimension g over a finitely generated extension K of $\mathbb{Q}$. Then, there exist positive integers n, r, l_0 and for each $l \geqslant l_0$ there exists a connected reductive subgroup H_l of $\mathrm{GL}_{2g,\mathbb{F}_l}$ of rank r with the following properties:*

(a) *There exist a number field K_0, an abelian variety A_0 over K_0 of dimension g, a finite Galois extension L_0 of K_0, and a positive integer n_0 that divides n such that $\rho_{A_0,l}(\mathrm{Gal}(L_0))$ is a subgroup of $H_l(\mathbb{F}_l)$ of index $\leqslant n_0$. Moreover, H_l contains the group $\mathbb{G}_m$ of homotheties of $\mathrm{GL}_{2g,\mathbb{F}_l}$. Furthermore, the family $(\rho_{A_0,l}|_{\mathrm{Gal}(L_0)})_{l \geqslant l_0}$ of homomorphisms is independent.*

(b) *There exists a finite Galois extension L of K such that the group $\rho_{A,l}(\mathrm{Gal}(L))$ is contained in $H_l(\mathbb{F}_l)$ with index $\leqslant n$. Moreover, the family $(\rho_{A,l}|_{\mathrm{Gal}(L)})_{l \geqslant l_0}$ of homomorphisms is independent.*

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

Proof. First suppose that K is a number field. By Serre, there exist positive integers n_0, r, l_0 and for each $l \geqslant l_0$ there exists a connected reductive subgroup H_l of $\mathrm{GL}_{2g,\mathbb{F}_l}$ of rank r such that (a) holds with $K_0 = K$, $A_0 = A$, $L_0 = L$, and $n = n_0$ (see [Zyw16, Theorem 3.1] for the statement). A full account of statement (a) and the proof can be found in [Ser86] (see also letters from Serre to M.-F. Vignéra [Ser00, #137] and K. Ribet [Ser00, #138]). Finally, the statement about the independence of the family $(\rho_{A,l}|_{l \geqslant l_0})$ is proved in [Ser13, Theorem 1].

Thus, (a) and (b) hold when K is a number field.

Now assume that the transcendence degree of K over $\mathbb{Q}$ is positive. In Section 1 and in particular in Setup 1.5 we have introduced the following objects: E is a finitely generated extension of $\mathbb{Q}$, S is a smooth curve over E whose function field is K, $\mathbf{s}$ is a closed point of S, K_{ur} is the maximal unramified extension of K along S (it contains $K(A_l)$ for each $l \in \mathbb{L}$), $\overline{K}_{\mathbf{s}}$ is the residue field of K at $\mathbf{s}$ (it is a finite extension of E with $\mathrm{trans.deg}(\overline{K}_{\mathbf{s}}/\mathbb{Q}) = \mathrm{trans.deg}(K/\mathbb{Q}) - 1$), $A_{\mathbf{s}}$ is an abelian variety over $\overline{K}_{\mathbf{s}}$ of dimension g, K' is a finite extension of K (Proposition 1.6), $\hat{\psi}_{\mathbf{s}} : \mathrm{Gal}(\hat{K}_{\mathbf{s}}/\overline{K}_{\mathbf{s}}) \to \mathrm{Gal}(\hat{K}/K')$ is an isomorphism, and $\hat{\varphi}_{\mathbf{s}} : \mathrm{Gal}(\hat{K}/K') \to \mathrm{Gal}(\hat{K}_{\mathbf{s}}/\overline{K}_{\mathbf{s}})$ is the inverse of $\hat{\psi}_{\mathbf{s}}$.

An induction hypothesis on the transcendence degree over $\mathbb{Q}$ applied to $\overline{K}_{\mathbf{s}}$ and $A_{\mathbf{s}}$ gives a number field K_0, an abelian variety A_0 over K_0, a finite Galois extension L_0 of K_0 and positive integers n_0, r, l_0 such that

(1a) For each prime number $l \geqslant l_0$ there is a connected reductive subgroup H_l of $\mathrm{GL}_{2g,\mathbb{F}_l}$ such that $\rho_{A_0,l}(\mathrm{Gal}(L_0))$ is a subgroup of $H_l(\mathbb{F}_l)$ of index $\leqslant n_0$. Moreover H_l is of rank r and contains the center $\mathbb{G}_m$ of $\mathrm{GL}_{2g,\mathbb{F}_l}$.

(1b) The family $(\rho_{A_0,l}|_{\mathrm{Gal}(L_0)})_{l \geqslant l_0}$ of homomorphisms is independent.

Moreover, there exists a finite Galois extension $L_{\mathbf{s}}$ of $\overline{K}_{\mathbf{s}}$ and a positive integral multiple $n_{\mathbf{s}}$ of n_0 with the following properties:

(2a) For all $l \geqslant l_0$, $\rho_{A_{0,l}}(\mathrm{Gal}(L_{\mathbf{s}})) \leqslant H_l(\mathbb{F}_l)$, and $(H_l(\mathbb{F}_l) : \rho_{A_{\mathbf{s}},l}(\mathrm{Gal}(L_{\mathbf{s}}))) \leqslant n_{\mathbf{s}}$.

(2b) The family $(\rho_{A_{\mathbf{s}},l}|_{\mathrm{Gal}(L_{\mathbf{s}})})_{l \geqslant l_0}$ of homomorphisms is independent.

Let L' be the fixed field in K_{ur} of $\psi_{\mathbf{s}}(\mathrm{Gal}(L_{\mathbf{s}}))$. Then, L' is a finite Galois extension of K' in K_{ur} and, by the last statement of Setup 1.5, we have the

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

following commutative diagram:

$$\begin{tikzcd}
\mathrm{Gal}(K') \arrow[r, "\mathrm{res}"] \arrow[rrr, bend left, "\rho_{A,l}|_{\mathrm{Gal}(K')}"] & \mathrm{Gal}(K_{\mathrm{ur}}/K') \arrow[r, "\varphi_{\mathbf{s}}"] & \mathrm{Gal}(\overline{K}_{\mathbf{s}}) \arrow[r, "\rho_{A_{\mathbf{s}},l}"] & H_l(\mathbb{F}_l) \\
\mathrm{Gal}(L') \arrow[r, "\mathrm{res}"] \arrow[u] & \mathrm{Gal}(K_{\mathrm{ur}}/L') \arrow[r, "\varphi_{\mathbf{s}}"] \arrow[u] & \mathrm{Gal}(L_{\mathbf{s}}) \arrow[r, "\rho_{A_{\mathbf{s}},l}"] \arrow[u] & H_l(\mathbb{F}_l). \arrow[u, equal]
\end{tikzcd}$$

Since $\varphi_{\mathbf{s}}$ maps $\mathrm{Gal}(K_{\mathrm{ur}}/L')$ surjectively onto $\mathrm{Gal}(L_{\mathbf{s}})$, it follows from (2b) that the family $(\rho_{A,l}|_{\mathrm{Gal}(L')})_{l\geqslant l_0}$ of homomorphisms is independent (Section 2, second paragraph).

Since K' is a finite extension of K, so is L'. However, L' need not be Galois over K. Nevertheless, by Lemma 2.2, K has a finite Galois extension L in K_{ur} that contains L' such that the family $(\rho_{A,l}|_{\mathrm{Gal}(L)})_{l\geqslant l_0}$ is independent. Moreover, for each $l \geqslant l_0$ we have $\rho_{A,l}(\mathrm{Gal}(L)) \leqslant \rho_{A,l}(\mathrm{Gal}(L')) \leqslant H_l(\mathbb{F}_l)$ and, by (2a),

$$\begin{aligned}
&(H_l(\mathbb{F}_l) : \rho_{A,l}(\mathrm{Gal}(L))) \\
&\quad = (H_l(\mathbb{F}_l) : \rho_{A,l}(\mathrm{Gal}(L'))) \cdot (\rho_{A,l}(\mathrm{Gal}(L')) : \rho_{A,l}(\mathrm{Gal}(L))) \\
&\quad \leqslant (H_l(\mathbb{F}_l) : \rho_{A_{\mathbf{s}},l}(\mathrm{Gal}(L_{\mathbf{s}}))) \cdot [L : L'] \leqslant n_{\mathbf{s}}[L : L'].
\end{aligned}$$

Thus, L satisfies Conditions (a) and (b) of the proposition with $n = n_{\mathbf{s}}[L : L']$. ∎

4.2 Tori in reductive groups

Let H be a connected reductive group over a field F and let T be a maximal torus of H over F. Then, $T(\tilde{F})$ is isomorphic to $(\tilde{F}^{\times})^r$ for some positive integer r, called the *rank* of H [Spr98, p. 117, Section 7.2.1]. In particular, T is absolutely integral. By [Spr98, p. 108, Proposition 6.4.2], all maximal tori of H are conjugate, so the rank of H is independent of T.

We say that T *F-splits* if T is isomorphic over F to the group $\mathbb{D}_r$ of diagonal matrices. Thus, in this case $T(F) \cong (F^{\times})^r$. We say that H *F-splits* if H has a maximal F-split torus [Spr98, p. 271, Section 16.2.1]. By [Spr98, p. 256, Theorem 15.2.6], all F-split maximal tori are conjugate by an element of $H(F)$.

A result of Zywina gives additional information on the groups H_l mentioned in Proposition 4.1.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

LEMMA 4.3. *Let A, g, K, L, n, r, l_0, and H_l with $l \geqslant l_0$, be as in Proposition 4.1. Then, there is a finite Galois extension M of $\mathbb{Q}$ such that if $l \in \mathbb{L}$ splits completely in M and is sufficiently large, then the following holds:*

(a) *The reductive group H_l $\mathbb{F}_l$-splits.*

(b) *Let $(X_{ij}, Y)_{1 \leqslant i,j \leqslant 2g}$ be independent variables. We identify $\mathrm{GL}_{2g}(\mathbb{F}_l)$ with the closed subvariety of $\mathrm{Spec}(\mathbb{F}_l[X_{ij}, Y]_{1 \leqslant i,j \leqslant 2g}) = \mathbb{A}_{\mathbb{F}_l}^{4g^2+1}$ defined by the equation $\det((X_{ij})_{1 \leqslant i,j \leqslant 2g})Y = 1$.*

Let T be an $\mathbb{F}_l$-split maximal torus of H_l. Then, the torus T, viewed as a closed subvariety of $\mathbb{A}_{\mathbb{F}_l}^{4g^2+1}$, is defined by at most c_1 polynomials of degree at most c_2, where c_1 and c_2 are constants that do not depend on l.

Proof. By Proposition 4.1, the subgroups H_l satisfy Conditions (a) and (b) of that proposition with respect to an abelian variety A_0 of dimension g defined over a number field K_0 and with respect to a finite Galois extension L_0 of K_0. Therefore, our lemma follows from [Zyw16, Lemma 3.2] (in which $A = A_0$, $K = K_0$, and $L = L_0$). □

Another auxiliary tool that we quote from [Zyw16] is the following variant of a theorem of Lang–Weil.

PROPOSITION 4.4. [Zyw16, Theorem 2.1] *Let q be a power of a prime number and consider a Zariski-closed subset V of $\mathbb{A}_{\mathbb{F}_q}^k$ with $k > 1$ defined by the simultaneous vanishing of s polynomials $f_1, \ldots, f_s$ in $\mathbb{F}_q[X_1, \ldots, X_k]$, each of which is of degree at most e. Let $V_1, \ldots, V_m$ be the irreducible components of $V_{\tilde{\mathbb{F}}_q}$, which have the same dimension as V. Then,*

$$\text{(a)} \qquad |V(\mathbb{F}_q)| \leqslant mq^{\dim(V)} + 6(3 + se)^{k+1} 2^s q^{\dim(V) - \frac{1}{2}}.$$

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

$$\text{(b)} \qquad ||V(\mathbb{F}_q)| - mq^{\dim(V)}| \leqslant 6(3 + se)^{k+1} 2^s q^{\dim(V) - \frac{1}{2}}.$$

In the rest of this section we bound the constant m that appears in Proposition 4.4 in terms of the degrees of $f_1, \ldots, f_s$.

LEMMA 4.5. *Let F be an algebraically closed field, Y an irreducible algebraic variety in $\mathbb{A}_F^n$, H a hypersurface in $\mathbb{A}_F^n$, and $Z_1, \ldots, Z_s$ the irreducible components of $Y \cap H$. Then, $\sum_{j=1}^s \deg(Z_j) \leqslant \deg(Y)\deg(H)$.*

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

Proof. The degrees of Y and H do not change by taking the Zariski closures of these varieties in $\mathbb{P}_F^n$. The number of the components of $Y \cap H$ may only increase. Hence, we may assume that Y and H are projective.

If $Y \subseteq H$, then $Y = Y \cap H$ is the unique irreducible component of $Y \cap H$ and $\deg(Y) \leqslant \deg(Y)\deg(H)$. If on the other hand $Y \not\subseteq H$, then by [Har77, p. 53, Theorem 7.7],

$$\sum_{j=1}^{s} i(Y, H; Z_j)\deg(Z_j) = \deg(Y)\deg(H). \tag{3}$$

Since the intersection multiplicities $i(Y, H; Z_j)$ are positive integers, the conclusion of the lemma follows from (3). □

Lemma 4.6. *Let F be an algebraically closed field and let $f_1, \ldots, f_k \in F[X_1, \ldots, X_n]$ be nonzero polynomials. Let*

$$V = V(f_1, \ldots, f_k) = \mathrm{Spec}(F[X_1, \ldots, X_n] / \sum_{i=1}^{n} F[X_1, \ldots, X_n] f_i)$$

be the algebraic variety in $\mathbb{A}_F^n$ defined by $f_1, \ldots, f_k$ and let $Z_1, \ldots, Z_m$ be the irreducible components of V. Then, $m \leqslant \sum_{i=1}^{m}\deg(Z_i) \leqslant \prod_{i=1}^{k}\deg(f_i)$.

Proof. Since $\deg(Z_i) \geqslant 1$ for all i, the left inequality is clear. We prove the right inequality.

First we consider the case where $k = 1$. Let $f_1 = c g_1^{d_1} \cdots g_m^{d_m}$ be the decomposition of f_1 into a product of powers of irreducible polynomials in $F[X_1, \ldots, X_n]$, no one of which is a product of the other with an element of $K^\times$, and $c \in K^\times$. Then, $V(g_1), \ldots, V(g_m)$ are the irreducible components of $V(f_1)$. By [Har77, p. 52, Proposition 7.6(d)], we have $\sum_{i=1}^{m}\deg(V(g_i)) = \sum_{i=1}^{m}\deg(g_i) \leqslant \sum_{i=1}^{m} d_i \deg(g_i) = \deg(f_1)$.

Now we assume that $k \geqslant 2$, set $V_{k-1} = V(f_1, \ldots, f_{k-1})$, and let $W_1, \ldots, W_{m'}$ be the irreducible components of V_{k-1}. An induction assumption implies that

$$\sum_{i=1}^{m'}\deg(W_i) \leqslant \deg(f_1)\cdots\deg(f_{k-1}). \tag{4}$$

For each $1 \leqslant i \leqslant m'$ let $Z_{i,1}, \ldots, Z_{i,m'_i}$ be the irreducible components of $W_i \cap V(f_k)$. Then, the Z_{ij} with $i = 1, \ldots, m'$ and $j = 1, \ldots, m'_i$ are the irreducible components of V (eventually with repetitions). By Lemma 4.5,

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

$\sum_{j=1}^{m_i'} \deg(Z_{ij}) \leqslant \deg(W_i)\deg(f_k)$. It follows from (4) that

$$\sum_{i=1}^{m'}\sum_{j=1}^{m_i'} \deg(Z_{ij}) \leqslant \sum_{i=1}^{m'} \deg(W_i)\deg(f_k) \leqslant \deg(f_1)\cdots\deg(f_{k-1})\deg(f_k),$$

and this implies the desired inequality. □

§5. Good reduction of abelian varieties

We generalize results of Serre and Tate in [SeT68] about good reduction of abelian schemes over discrete valuation rings to results about good reduction of abelian schemes over more general integral domains.

5.1 Abelian scheme over a domain

Let R be a Noetherian integrally closed domain with quotient field K and let $\pi : \mathcal{A} \to \mathrm{Spec}(R)$ be an abelian scheme. Thus, π is a proper and smooth morphism with connected geometric fibers [Mil85, p. 145, first paragraph of Section 20].

Moreover, for each $\mathfrak{p} \in \mathrm{Spec}(R)$ let $\overline{K}_\mathfrak{p} = \mathrm{Quot}(R/\mathfrak{p})$ and set $\tilde{K}_\mathfrak{p}$ for the algebraic closure of $\overline{K}_\mathfrak{p}$. Also, let $A_\mathfrak{p} = \mathcal{A} \times_R \mathrm{Spec}(\overline{K}_\mathfrak{p})$. Then, $\pi_\mathfrak{p} : A_\mathfrak{p} \to \mathrm{Spec}(\overline{K}_\mathfrak{p})$ is a proper and smooth morphism with a connected geometric fiber, so $A_\mathfrak{p}$ is an abelian variety over $\overline{K}_\mathfrak{p}$ that we call the *reduction of* $\mathcal{A}$ *modulo* $\mathfrak{p}$.

Note that π is of finite type and set $g = \dim(\mathcal{A}) - \dim(R)$ for the relative dimension of $\mathcal{A}$. Then, $\dim(A_\mathfrak{p}) = g$ for each $\mathfrak{p} \in \mathrm{Spec}(R)$ [Mum88, p. 304, Theorem III.10.3’].

In particular, let $\mathfrak{o}$ be the zero ideal of R. Then, the *generic fiber* $A = A_\mathfrak{o}$ of $\mathcal{A}$ is an abelian variety over K of dimension g.

5.2 Multiplication with m

By [Mil85, p. 116, Remark 8.4], multiplication of $\mathcal{A}$ by a positive integer m is a finite and flat morphism of $\mathcal{A}$ onto $\mathcal{A}$. Moreover, the kernel $\mathcal{A}_m$ of that morphism is a finite flat group scheme over $\mathrm{Spec}(R)$ of order m^{2g}. In particular, the finiteness of the morphism $\mathcal{A}_m \to \mathrm{Spec}(R)$ implies that $\mathcal{A}_m = \mathrm{Spec}(B)$, where $B = B_m$ is a ring extension of R, which is finitely generated as an R-module [Mum88, p. 172, Definition II.7.3]. In other words, B is an integral extension of R.

REMARK 5.3. If none of the residue characteristics of R divides m (equivalently, $m \notin \mathfrak{p}$ for each $\mathfrak{p} \in \mathrm{Spec}(R)$; equivalently, m is a unit of R),

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

then multiplication of $\mathcal{A}$ by m as well as $\mathcal{A}_m \to \mathrm{Spec}(R)$ are étale morphisms [Mil85, p. 147, Proposition 20.7]. Hence, B is étale over R.

5.4 Reduction modulo $\mathfrak{p}$

We consider a prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$ and compose each $\beta \in \mathrm{Hom}_R(B, R)$ with the quotient map $R \to R/\mathfrak{p}$ followed by the inclusion $R/\mathfrak{p} \to \overline{K}_{\mathfrak{p}}$ to get a homomorphism $\beta_{\mathfrak{p}}$ as in the following commutative diagram

$$\begin{tikzcd} B \arrow[r, "\beta"] \arrow[rrr, bend left, "\beta_{\mathfrak{p}}"] & R \arrow[r] & R/\mathfrak{p} \arrow[r] & \overline{K}_{\mathfrak{p}}. \end{tikzcd}$$

The map $\beta \mapsto \beta_{\mathfrak{p}}$ gives rise to a *reduction map modulo* $\mathfrak{p}$:

$$\mathrm{Hom}_R(B, R) \to \mathrm{Hom}_R(B, \overline{K}_{\mathfrak{p}}). \tag{1}$$

There is a natural bijection $\mathrm{Hom}_R(B, R) \to \mathrm{Mor}_R(\mathrm{Spec}(R), \mathrm{Spec}(B))$ that maps each $\beta \in \mathrm{Hom}_R(B, R)$ onto the R-morphism $\mathrm{Spec}(R) \to \mathrm{Spec}(B)$ that maps each prime ideal of R onto its inverse image in B under β [Liu06, p. 48, Proposition 2.3.25]. By definition, $\mathcal{A}_m(R) = \mathrm{Mor}_R(\mathrm{Spec}(R), \mathrm{Spec}(B))$. An analogous rule applies to $\overline{K}_{\mathfrak{p}}$ rather than to R. This gives a commutative diagram

$$\begin{tikzcd} \mathcal{A}_m(R) \arrow[r, "f_{\mathfrak{p}}"] \arrow[d, equal] & A_{\mathfrak{p},m}(\overline{K}_{\mathfrak{p}}) \arrow[d, equal] \\ \mathrm{Mor}_R(\mathrm{Spec}(R), \mathrm{Spec}(B)) \arrow[r, "f_{\mathfrak{p}}"] & \mathrm{Mor}_R(\mathrm{Spec}(\overline{K}_{\mathfrak{p}}), \mathrm{Spec}(B)) \\ \mathrm{Hom}_R(B, R) \arrow[r] \arrow[u] & \mathrm{Hom}_R(B, \overline{K}_{\mathfrak{p}}), \arrow[u] \end{tikzcd} \tag{2}$$

where the vertical arrows are bijections. Note that if

$$s \in \mathrm{Mor}_R(\mathrm{Spec}(R), \mathrm{Spec}(B)),$$

then $f_{\mathfrak{p}}(s) = s \circ i_{\mathfrak{p}}$, where $i_{\mathfrak{p}}$ is the natural map $\mathrm{Spec}(\overline{K}_{\mathfrak{p}}) \to \mathrm{Spec}(R/\mathfrak{p}) \to \mathrm{Spec}(R)$ that maps the zero ideal of $\overline{K}_{\mathfrak{p}}$ onto $\mathfrak{p}$. Thus,

(3) if $s, s' \in \mathrm{Mor}_R(\mathrm{Spec}(R), \mathrm{Spec}(B))$ and $f_{\mathfrak{p}}(s) = f_{\mathfrak{p}}(s')$, then $s(\mathfrak{p}) = s'(\mathfrak{p})$.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

LEMMA 5.5. *Let R and $\mathcal{A}$ be as in Section 5.1 and let m be a positive integer. Consider a prime ideal $\mathfrak{p}$ of R and let $\mathfrak{o}$ be the zero ideal of R. Then, the following statements about the objects introduced in this section are true:*

(a) *the map $f_{\mathfrak{o}} : \mathcal{A}_m(R) \to A_m(K)$ is bijective;*

(b) *let $\mathfrak{p}$ be a prime ideal of R such that $\mathrm{char}(\overline{K}_{\mathfrak{p}}) \nmid m$. Then, the map $f_{\mathfrak{p}} : \mathcal{A}_m(R) \to A_{\mathfrak{p},m}(\overline{K}_{\mathfrak{p}})$ is injective, hence*

(c) *the specialization map $A_m(K) \xrightarrow{f_{\mathfrak{o}}^{-1}} \mathcal{A}_m(R) \xrightarrow{f_{\mathfrak{p}}} A_{\mathfrak{p},m}(\overline{K}_{\mathfrak{p}})$ is injective.*

Proof of (a). We consider Diagram (2) in the case where $\mathfrak{p}$ is the zero ideal $\mathfrak{o}$ of R. In this case, $\overline{K}_{\mathfrak{p}} = K$. Let $\iota : R \to K$ be the inclusion map. By the commutativity of that diagram, it suffices to prove that the map $\mathrm{Hom}_R(B, R) \to \mathrm{Hom}_R(B, K)$ defined by $\alpha \mapsto \iota \circ \alpha$ is bijective.

Indeed, the map $\alpha \mapsto \iota \circ \alpha$ is injective, because ι is injective. In order to prove that the map is surjective it suffices to prove that $\beta(B) \subseteq R$ for each $\beta \in \mathrm{Hom}_R(B, K)$.

Indeed, if $x \in B$, then x is integral over R (by Section 5.2). Hence, so is $\beta(x)$. Since R is integrally closed, $\beta(x) \in R$, as has to be proved.

Proof of (b). Since $\mathrm{char}(\overline{K}_{\mathfrak{p}}) \nmid m$, we have $\mathrm{char}(K) \nmid m$. Hence, we may consider the integrally closed integral domain $R' = R[m^{-1}]$. Then we make a base change from R to R' and consider the prime ideal $\mathfrak{p}' = \mathfrak{p}R'$ of R'. We also set $\mathcal{A}' = \mathcal{A}_{R'}$ and $B' = B[m^{-1}]$. Then, $\mathrm{Quot}(R') = \mathrm{Quot}(R) = K$, $\mathrm{Quot}(R'/\mathfrak{p}') = \mathrm{Quot}(R/\mathfrak{p}) = \overline{K}_{\mathfrak{p}}$, $\mathcal{A}'_m = \mathrm{Spec}(B')$. Finally, we may identify $\mathrm{Hom}_R(B, \overline{K}_{\mathfrak{p}})$ with $\mathrm{Hom}_{R'}(B', \overline{K}_{\mathfrak{p}})$. Hence, by Diagram (2), we may identify $A_{\mathfrak{p},m}(\overline{K}_{\mathfrak{p}})$ with $A'_{\mathfrak{p}',m}(\overline{K}_{\mathfrak{p}})$.

By (a) (applied to R and to R'), we may identify $\mathcal{A}_m(R)$ and $\mathcal{A}'_m(R')$ with $A_m(K)$; hence we may identify $\mathcal{A}_m(R)$ with $\mathcal{A}_m(R')$. Let $f'_{\mathfrak{p}'} : \mathcal{A}'_m(R') \to A_{\mathfrak{p},m}(\overline{K}_{\mathfrak{p}}) = A'_{\mathfrak{p}',m}(\overline{K}_{\mathfrak{p}})$ be the analogous map to $f_{\mathfrak{p}} : \mathcal{A}_m(R) \to A_{\mathfrak{p},m}(\overline{K}_{\mathfrak{p}})$. Then, the following diagram commutes:

$$\begin{tikzcd}
 & \mathcal{A}'_m(R') \arrow[dl, equal] \arrow[d, equal] \arrow[r, "f'_{\mathfrak{p}'}"] & A'_{\mathfrak{p}',m}(\overline{K}_{\mathfrak{p}}) \arrow[d, equal] \\
\mathcal{A}_m(K) \arrow[r, equal] & \mathcal{A}_m(R) \arrow[r, "f_{\mathfrak{p}}"] & A_{\mathfrak{p},m}(\overline{K}_{\mathfrak{p}}).
\end{tikzcd}$$

Thus, it suffices to prove that the morphism $f'_{\mathfrak{p}'}$ is injective.

Let s, t be elements of $\mathcal{A}'_m(R')$ such that $f'_{\mathfrak{p}'}(s) = f'_{\mathfrak{p}'}(t)$. By (3) for R' rather than for R, $s(\mathfrak{p}') = t(\mathfrak{p}')$. Diagram (2) identifies both s and t as elements of $\mathrm{Mor}_{R'}(\mathrm{Spec}(R'), \mathrm{Spec}(B'))$, that is, as sections of the morphism $h : \mathrm{Spec}(B') \to \mathrm{Spec}(R')$ induced from the inclusion $R' \subseteq B'$. Since m is a unit of R', Remark 5.3 implies that B' is étale over R'. Since h is affine, it is separated [Liu06, p. 100, Proposition 3.3.4]. Hence, by [Mil80, p. 25, Corollary 3.12] or [Gro71, Exposé 1, p. 6, Corollary 5.3], $s = t$, as claimed.

Proof of (c). This follows from (b) and from (a). □

Let $\pi : \mathcal{A} \to \mathrm{Spec}(R)$ be as in Section 5.1 and let m be a positive integer. We use Lemma 5.5(a) to identify $\mathcal{A}_m(R)$ and $A_m(K)$.

If $\mathrm{char}(\overline{K}_{\mathfrak{p}}) \nmid m$, then by Lemma 5.5(c), the injective map $f_{\mathfrak{p}} : \mathcal{A}_m(R) \to A_{\mathfrak{p},m}(\overline{K}_{\mathfrak{p}})$ can be considered as an injective homomorphism $f_{\mathfrak{p}} : A_m(K) \to A_{\mathfrak{p},m}(\overline{K}_{\mathfrak{p}})$ that we call *the reduction map modulo* $\mathfrak{p}$. If m' is a multiple of m and $m' \notin \mathfrak{p}$, then the reduction map modulo $\mathfrak{p}$ with respect to m' extends the reduction map modulo $\mathfrak{p}$ with respect to m.

LEMMA 5.6. *Let R and $\mathcal{A}$ be as in Section 5.1. Let m be a positive integer and N an algebraic extension of K that contains $K(A_m)$. We denote the integral closure of R in N by R_N. Consider a prime ideal $\mathfrak{p}$ of R that does not contain m. Then, for each $\mathfrak{P} \in \mathrm{Spec}(R_N)$ over $\mathfrak{p}$, reduction modulo $\mathfrak{P}$ maps $A_m(N)$ isomorphically onto $A_{\mathfrak{p},m}(\overline{N}_{\mathfrak{P}})$.*

Proof. By Section 5.1, $\dim(A_{\mathfrak{p}})$ is equal to the relative dimension g of $\mathcal{A}$ over R. Hence, by [Mil85, p. 116, Remark 8.4], $|A_m(N)| = m^{2g}$ and $|A_{\mathfrak{P},m}(\overline{N}_{\mathfrak{P}})| = |A_{\mathfrak{p},m}(\overline{N}_{\mathfrak{P}})| \leqslant m^{2g}$. By Lemma 5.5(c) for R_N and N rather than R and K, the reduction map $A_m(N) \to A_{\mathfrak{P},m}(\overline{N}_{\mathfrak{P}})$ is injective. Hence, that map is bijective, so it is an isomorphism. □

5.7 Good reduction of representations

Again, let R, $\mathcal{A}$, B, and m be as in Section 5.2. In particular, $B = R[x_1, \ldots, x_k]$ is a finitely generated ring extension of R. Let I be the kernel of the R-homomorphism $R[X_1, \ldots, X_k] \to B$ that maps X_i onto x_i for $i = 1, \ldots, k$.

We consider again a Galois extension N of K that contains $K(A_m)$, a prime ideal $\mathfrak{p}$ of R that does not contain m, and a prime ideal $\mathfrak{P}$ of the integral closure R_N of R in N that lies over $\mathfrak{p}$. Then, $A_{\mathfrak{p},m}(\overline{N}_{\mathfrak{P}}) = \mathrm{Hom}_R(B, \overline{N}_{\mathfrak{P}})$. As usual, we identify each element of $\mathrm{Hom}_R(B, \overline{N}_{\mathfrak{P}})$

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

with a k-tuple

$$(x_{1,\mathfrak{P}}, \ldots, x_{k,\mathfrak{P}})$$

with coordinates in $\overline{N}_{\mathfrak{P}}$ at which every $h \in I$ vanishes. Then, $x_1, \ldots, x_k$ lie in R_N and reduction modulo $\mathfrak{P}$ maps $x_1, \ldots, x_k$ onto $x_{1,\mathfrak{P}}, \ldots, x_{k,\mathfrak{P}}$, respectively. This gives another presentation to the reduction modulo $\mathfrak{P}$ of $A_m(N)$ mentioned in Lemma 5.6 and its proof.

Next, we recall that B is étale over R (Section 5.3) and assume that R_N is also étale over R, at least locally over $\mathfrak{p}$ (e.g., $N = K(A_{m'})$, where m' is a multiple of m that does not belong to $\mathfrak{p}$). Let $D_{\mathfrak{P}/\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(N/K) \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ be the decomposition group of $\mathfrak{P}$ over $\mathfrak{p}$. Then, the reduction $x \mapsto \bar{x}$ modulo $\mathfrak{P}$ (with $x \in R_N$) induces an isomorphism $\sigma \to \bar{\sigma}$ of $D_{\mathfrak{P}/\mathfrak{p}}$ onto $\mathrm{Gal}(\overline{N}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}})$ defined by $\bar{\sigma}\,\bar{x} = \overline{\sigma x}$. Indeed, if N/K is finite, then R_N/R is locally *standard étale* in a Zariski-open neighborhood of $\mathfrak{p}$ [Mil80, p. 26, Theorem 3.14]. Thus, there exists $z \in N$ such that $R_{N,\mathfrak{P}} = R_{\mathfrak{p}}[z]$, where the discriminant of $\mathrm{irr}(z, K)$ is a unit of $R_{\mathfrak{p}}$ (Section 3.2). Now apply [FrJ08, p. 109, Lemma 6.1.4].

This isomorphism is then compatible with the isomorphism $A_m(N) \to A_{\mathfrak{p},m}(\overline{N}_{\mathfrak{P}})$ given by Lemma 5.6, which leads to the following commutative triangle:

$$\begin{tikzcd}
D_{\mathfrak{P}/\mathfrak{p}} \arrow[r] \arrow[d, "\rho_{A,m}"'] & \mathrm{Gal}(\overline{N}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}}) \arrow[dl, "\rho_{A_{\mathfrak{p}},m}"] \\
\mathrm{GL}_{2g}(\mathbb{Z}/m\mathbb{Z}), &
\end{tikzcd}$$

where $\rho_{A,m}$ is the *m-ic representation* induced by the action of $\mathrm{Gal}(K)$ on $A_m(\tilde{K})$. If l is a prime number that does not belong to $\mathfrak{p}$ and if $K(A_{l^\infty}) \subseteq N$, the preceding diagram applied to $l, l^2, l^3, \ldots$ gives rise to a commutative diagram for the l-adic representations:

$$\begin{tikzcd}
D_{\mathfrak{P}/\mathfrak{p}} \arrow[r] \arrow[d, "\rho_{A,l^\infty}"'] & \mathrm{Gal}(\overline{N}_{\mathfrak{P}}/\overline{K}_{\mathfrak{p}}) \arrow[dl, "\rho_{A_{\mathfrak{p}},l^\infty}"] \\
\mathrm{GL}_{2g}(\mathbb{Z}_l). &
\end{tikzcd}$$

§6. Bounds on degrees

Given a field F and a nonzero polynomial $f \in F[X]$, we denote the number of distinct roots of $f(X)$ in $\tilde{F}$ by $\nu(f(X))$. We prove that the condition

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

"$\nu(f(X)) \leqslant d$" is equivalent to a "Zariski-closed condition on the coefficients of f."

LEMMA 6.1. *Let F be a field, $t_1, \ldots, t_e$ elements of a field extension of F, $T = \mathrm{Spec}(F[\mathbf{t}])$ (with $\mathbf{t} = (t_1, \ldots, t_e)$), $f \in F[\mathbf{t}][X]$ a monic polynomial in X of degree m with coefficients in $F[\mathbf{t}]$, and d an integer between 1 and m. Then, there exists a Zariski-closed subset V of T such that $V(\tilde{F}) = \{\mathbf{t}' \in T(\tilde{F}) \mid \nu(f(\mathbf{t}', X)) \leqslant d\}$.*

Proof. Let $f(\mathbf{t}, X) = \prod_{i=1}^m (X - x_i)$ be the decomposition of $f(\mathbf{t}, X)$ in $\widetilde{F(\mathbf{t})}$. We set $\mathbf{x} = (x_1, \ldots, x_m)$. Then, $F(\mathbf{t}, \mathbf{x})/F(\mathbf{t})$ is a finite normal extension of fields. Moreover, $F[\mathbf{t}, \mathbf{x}]/F[\mathbf{t}]$ is an integral extension of integral domains. Hence, by [Mum88, p. 171, Proposition II.7.4], the corresponding morphism $\varphi : U = \mathrm{Spec}(F[\mathbf{t}, \mathbf{x}]) \to \mathrm{Spec}(F[\mathbf{t}])$ is closed.

Let I be the set of all d-tuples $\mathbf{i} = (i_1, \ldots, i_d)$ of integers between 1 and m. For each $\mathbf{i} \in I$ and $1 \leqslant j \leqslant m$ we consider the Zariski-closed subset $W_{\mathbf{i},j}$ of U defined by the equation $(X_j - X_{i_1}) \cdots (X_j - X_{i_d}) = 0$.

Since $F[\mathbf{t}, \mathbf{x}]/F[\mathbf{t}]$ is an integral extension, for each $\mathbf{t}' \in T(\tilde{F})$ the map $\mathbf{t} \mapsto \mathbf{t}'$ extends to an F-homomorphism $F[\mathbf{t}, \mathbf{x}] \to F[\mathbf{t}', \mathbf{x}']$ that maps $\mathbf{x}$ onto $\mathbf{x}' = (x_1', \ldots, x_m')$ with $x_1', \ldots, x_m' \in \tilde{F}$ such that $f(\mathbf{t}', X) = \prod_{i=1}^m (X - x_i')$. If $\mathbf{x}'' = (x_1'', \ldots, x_m'')$ is another m-tuple in $\tilde{F}^m$ such that the map $\mathbf{t} \mapsto \mathbf{t}'$ extends to an F-homomorphism $F[\mathbf{t}, \mathbf{x}] \to F[\mathbf{t}', \mathbf{x}'']$ that maps $\mathbf{x}$ onto $\mathbf{x}''$, then there exists $\sigma \in \mathrm{Aut}(\tilde{F}/F(\mathbf{t}'))$ such that $(\mathbf{x}')^\sigma = \mathbf{x}''$. Hence, $\tilde{V}_{\mathbf{i},j} = \{\mathbf{t}' \in T(\tilde{F}) \mid (x_j' - x_{i_1}') \cdots (x_j' - x_{i_d}') = 0\}$ is a well-defined subset of $T(\tilde{F})$. It follows that the set $\tilde{V} = \{\mathbf{t}' \in T(\tilde{F}) \mid \nu(f(\mathbf{t}', X)) \leqslant d\}$ satisfies the following condition:

$$\begin{aligned}
\tilde{V} &= \bigcup_{\mathbf{i} \in I} \{\mathbf{t}' \in T(\tilde{F}) \mid \{x_1', \ldots, x_m'\} \subseteq \{x_{i_1}', \ldots, x_{i_d}'\}\} \\
&= \bigcup_{\mathbf{i} \in I} \bigcap_{j=1}^m \{\mathbf{t}' \in T(\tilde{F}) \mid x_j' = x_{i_1}' \vee \cdots \vee x_j' = x_{i_d}'\} \\
&= \bigcup_{\mathbf{i} \in I} \bigcap_{j=1}^m \{\mathbf{t}' \in T(\tilde{F}) \mid (x_j' - x_{i_1}') \cdots (x_j' - x_{i_d}') = 0\} \\
&= \bigcup_{\mathbf{i} \in I} \bigcap_{j=1}^m \tilde{V}_{\mathbf{i},j}. \qquad (1)
\end{aligned}$$

Since φ is a closed map, $V_{\mathbf{i},j} = \varphi(W_{\mathbf{i},j})$ is a Zariski-closed subset of T. Moreover, $W_{\mathbf{i},j}(\tilde{F}) = \{(\mathbf{t}', \mathbf{x}') \in U(\tilde{F}) \mid (x_j' - x_{i_1}') \cdots (x_j' - x_{i_d}') = 0\}$, so

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

$V_{\mathbf{i},j}(\tilde{F}) = \tilde{V}_{\mathbf{i},j}$. It follows that $V = \bigcup_{\mathbf{i}\in I} \bigcap_{j=1}^{m} V_{\mathbf{i},j}$ is a Zariski-closed subset of T defined by polynomials with coefficients in F. Moreover, by (1), $V(\tilde{F}) = \bigcup_{\mathbf{i}\in I} \bigcap_{j=1}^{m} V_{\mathbf{i},j}(\tilde{F}) = \bigcup_{\mathbf{i}\in I} \bigcap_{j=1}^{m} \tilde{V}_{\mathbf{i},j} = \tilde{V}$, as desired. $\square$

Given a polynomial f with coefficients in $\mathbb{Z}$ we consider f for each l also as a polynomial with coefficients in $\mathbb{F}_l$ with the original coefficients replaced by their residues modulo l. We say that a scheme S over $\mathbb{Z}$ is *absolutely integral* if $S_{\tilde{\mathbb{Q}}} = S \times_{\mathbb{Z}} \mathrm{Spec}(\tilde{\mathbb{Q}})$ is integral.

LEMMA 6.2. *Let S be an absolutely integral affine scheme in $\mathbb{A}^e_{\mathbb{Z}}$ defined by polynomials in $\mathbb{Z}[\mathbf{S}]$, where $\mathbf{S} = (S_1, \ldots, S_e)$ is an e-tuple of variables. Let T be an absolutely integral affine scheme in $\mathbb{A}^k_{\mathbb{Z}}$ defined by polynomials in $\mathbb{Z}[\mathbf{T}]$, where $\mathbf{T} = (T_1, \ldots, T_k)$ is a k-tuple of variables. Let $f \in \mathbb{Z}[\mathbf{S}, \mathbf{T}][X]$ be a monic polynomial in X of degree m with coefficients in $\mathbb{Z}[\mathbf{S}, \mathbf{T}]$ and let d be an integer between 1 and m. Then, for every large prime number l the reductions $S_{\mathbb{F}_l}$ and $T_{\mathbb{F}_l}$ modulo l are absolutely integral and for each $\mathbf{s} \in S(\tilde{\mathbb{F}}_l)$ there exists a Zariski-closed subset $U_{l,\mathbf{s}}$ of $T_{\mathbb{F}_l(\mathbf{s})}$ defined by polynomials in $\mathbb{F}_l(\mathbf{s})[\mathbf{T}]$ such that $U_{l,\mathbf{s}}(\tilde{\mathbb{F}}_l) = \{\mathbf{t} \in T(\tilde{\mathbb{F}}_l) \mid \nu(f(\mathbf{s}, \mathbf{t}, X)) \leqslant d\}$.*

Moreover, the number and the degrees of the polynomials in $\mathbb{F}_l(\mathbf{s})[\mathbf{T}]$ that define $U_{l,\mathbf{s}}$ as a Zariski-closed subset of $T_{\mathbb{F}_l(\mathbf{s})}$ are bounded by constants that depend neither on l nor on $\mathbf{s}$.

Proof. Let $S_{\mathbb{Q}} = S \times_{\mathbb{Z}} \mathrm{Spec}(\mathbb{Q})$ and $T_{\mathbb{Q}} = T \times_{\mathbb{Z}} \mathrm{Spec}(\mathbb{Q})$ be the generic fibers of S and T. We may write $S = \mathrm{Spec}(\mathbb{Z}[\hat{\mathbf{s}}])$ and $T = \mathrm{Spec}(\mathbb{Z}[\hat{\mathbf{t}}])$, where $\hat{\mathbf{s}} = (\hat{s}_1, \ldots, \hat{s}_e)$ and $\hat{\mathbf{t}} = (\hat{t}_1, \ldots, \hat{t}_k)$ are tuples of some field extension of $\mathbb{Q}$ such that $\mathbb{Q}(\hat{\mathbf{s}})$ and $\mathbb{Q}(\hat{\mathbf{t}})$ are algebraically independent regular extensions of $\mathbb{Q}$ [FrJ08, p. 175, Corollary 10.2.2(a)]. By [FrJ08, p. 41, Lemma 2.6.7], $\mathbb{Q}(\hat{\mathbf{s}})$ and $\mathbb{Q}(\hat{\mathbf{t}})$ are linearly disjoint over $\mathbb{Q}$, so $\mathbb{Z}[\hat{\mathbf{s}}] \otimes \mathbb{Z}[\hat{\mathbf{t}}] \cong \mathbb{Z}[\hat{\mathbf{s}}, \hat{\mathbf{t}}]$. Hence, $S \times_{\mathbb{Z}} T \cong \mathrm{Spec}(\mathbb{Z}[\hat{\mathbf{s}}, \hat{\mathbf{t}}])$ and $S_{\mathbb{Q}} \times_{\mathbb{Q}} T_{\mathbb{Q}} \cong \mathrm{Spec}(\mathbb{Q}[\hat{\mathbf{s}}, \hat{\mathbf{t}}])$.

By Lemma 6.1, there exists a Zariski-closed subvariety V of $S_{\mathbb{Q}} \times_{\mathbb{Q}} T_{\mathbb{Q}}$ defined by polynomials $h_1, \ldots, h_r$ in $\mathbb{Z}[\mathbf{S}, \mathbf{T}]$ such that

$$V(\tilde{\mathbb{Q}}) = \{(\mathbf{s}, \mathbf{t}) \in S(\tilde{\mathbb{Q}}) \times T(\tilde{\mathbb{Q}}) \mid \nu(f(\mathbf{s}, \mathbf{t}, X)) \leqslant d\}. \tag{2}$$

We also have

$$V(\tilde{\mathbb{Q}}) = \{(\mathbf{s}, \mathbf{t}) \in S(\tilde{\mathbb{Q}}) \times T(\tilde{\mathbb{Q}}) \mid h_1(\mathbf{s}, \mathbf{t}) = 0, \ldots, h_r(\mathbf{s}, \mathbf{t}) = 0\}. \tag{3}$$

Thus, the following statement about $\tilde{\mathbb{Q}}$ is true.

(4) For all $\mathbf{s}$ and $\mathbf{t}$, the polynomial $f(\mathbf{s}, \mathbf{t}, X)$ has at most d distinct roots if and only if $h_1(\mathbf{s}, \mathbf{t}) = 0, \ldots, h_r(\mathbf{s}, \mathbf{t}) = 0$.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

Note that Statement (4) is elementary. In other words, the statement is equivalent to a sentence in the language of rings $\mathcal{L}(\mathrm{ring}, \mathbb{Z})$ with parameters in $\mathbb{Z}$ [FrJ08, p. 135, Example 7.3.1]. Hence, by a consequence of the quantifier elimination procedure for the theory of algebraically closed fields [FrJ08, p. 167, Corollary 9.2.2], that statement holds over $\tilde{\mathbb{F}}_l$ for every large prime number l. In addition, by [FrJ08, p. 179, Proposition 10.4.2], $S_{\mathbb{F}_l}$ and $T_{\mathbb{F}_l}$ are absolutely integral varieties over $\mathbb{F}_l$ for each large l.

For each l as in the preceding paragraph and for every $\mathbf{s} \in S(\tilde{\mathbb{F}}_l)$, let $U_{l,\mathbf{s}}$ be the Zariski-closed subset of $T_{\mathbb{F}_l(\mathbf{s})}$ defined by the polynomials

$$h_1(\mathbf{s}, \mathbf{T}), \ldots, h_r(\mathbf{s}, \mathbf{T}).$$

Since (4) holds over $\tilde{\mathbb{F}}_l$, we have

$$U_{l,\mathbf{s}}(\tilde{\mathbb{F}}_l) = \{\mathbf{t} \in T(\tilde{\mathbb{F}}_l) \mid \nu(f(\mathbf{s}, \mathbf{t}, X)) \leqslant d\}. \tag{5}$$

Moreover, the degrees of the polynomials $h_1(\mathbf{s}, \mathbf{T}), \ldots, h_r(\mathbf{s}, \mathbf{T})$ that define $U_{l,\mathbf{s}}$ are at most $\deg_{\mathbf{T}} h_1(\mathbf{S}, \mathbf{T}), \ldots, \deg_{\mathbf{T}} h_r(\mathbf{S}, \mathbf{T})$, respectively. Since the latter numbers are independent of $\mathbf{s}$, the second statement of the lemma is also true. □

§7. Counting points

Following [Zyw16], we find in this section a set Λ of prime numbers with positive Dirichlet density such that for all large $l \in \Lambda$ there are "many" points in $H_l(\mathbb{F}_l)$ having 1 as an eigenvalue, where H_l is the reductive subgroup of $\mathrm{GL}_{2g,\mathbb{F}_l}$ introduced in Proposition 4.1. Let n be a positive integer and let L be a finite Galois extension of K such that $\rho_{A,l}(\mathrm{Gal}(L))$ is contained in $H_l(\mathbb{F}_l)$ with index $\leqslant n$ (Proposition 4.1(b)). After fixing an $\mathbb{F}_l$-split maximal torus T of H_l, each of those points is of the form $\mathbf{b}\mathbf{t}^{n!}$, where $\mathbf{b} \in \rho_{A,l}(\mathrm{Gal}(K))$ depends only on l and $\mathbf{t}$ is an $\mathbb{F}_l$-rational point of T such that $\mathbf{t}^{n!}$ is a regular element of H_l.

7.1 Reduction modulo maximal ideals

Again, let K be a finitely generated extension of $\mathbb{Q}$, A an abelian variety over K of positive dimension g, and L the finite Galois extension of K given by Proposition 4.1. We use Section 3.2 to construct a regular domain R, which is a finitely generated extension of $\mathbb{Z}$ such that $\mathrm{Quot}(R) = K$ and the integral closure R_L of R in L is a ring cover. In particular, R_L/R is standard étale.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

Using [Mil85, p. 148, Remark 20.9], we replace R by a ring $R[u^{-1}]$, if necessary, where u is a nonzero element of R, such that A extends to an abelian scheme $\mathcal{A}$ over R. By Section 5.1, for each $\mathfrak{p} \in \mathrm{Max}(R)$ the reduction $A_\mathfrak{p}$ of A modulo $\mathfrak{p}$ is an abelian variety over the finite field $\overline{K}_\mathfrak{p} = R/\mathfrak{p}$.

7.2 Characteristic polynomials

We consider $\mathfrak{p} \in \mathrm{Max}(R)$ and $l \in \mathbb{L}$ such that $l \neq \mathrm{char}(\overline{K}_\mathfrak{p})$. Then, we choose a maximal ideal $\mathfrak{p}_l$ of $R_{K(A_l)}$ that lies over $\mathfrak{p}$ and a maximal ideal $\mathfrak{p}_{l^\infty}$ of $R_{K(A_{l^\infty})}$ that lies over $\mathfrak{p}_l$. By Lemma 5.6, reduction modulo $\mathfrak{p}_l$ (resp. modulo $\mathfrak{p}_{l^\infty}$) maps $A_l(\tilde{K})$ (resp. $A_{l^\infty}(\tilde{K})$) isomorphically onto $A_{\mathfrak{p},l}(\widetilde{\overline{K}_\mathfrak{p}})$ (resp. $A_{\mathfrak{p},l^\infty}(\widetilde{\overline{K}_\mathfrak{p}})$).

Moreover, by Section 5.7, the decomposition groups $D_{\mathfrak{p}_l/\mathfrak{p}}$ and $D_{\mathfrak{p}_{l^\infty}/\mathfrak{p}}$ are respectively naturally isomorphic to

$$\mathrm{Gal}(\overline{K}_\mathfrak{p}(A_{\mathfrak{p},l})/\overline{K}_\mathfrak{p}) \qquad \text{and} \qquad \mathrm{Gal}(\overline{K}_\mathfrak{p}(A_{\mathfrak{p},l^\infty})/\overline{K}_\mathfrak{p}).$$

Furthermore, these isomorphisms are compatible with the actions of those groups on A_l and $A_{\mathfrak{p},l}$ on the one hand and on A_{l^∞} and $A_{\mathfrak{p},l^\infty}$ on the other hand. By Section 3.3, $\overline{K}_\mathfrak{p}(A_{\mathfrak{p},l^\infty})$ is an algebraic extension of the finite field $\overline{K}_\mathfrak{p}$. As usual, we set $[\frac{K(A_{l^\infty})/K}{\mathfrak{p}_{l^\infty}}]$ for the element of $D_{\mathfrak{p}_{l^\infty}/\mathfrak{p}}$, which is mapped under that isomorphism onto the Frobenius element $\mathrm{Frob}_\mathfrak{p}$ of $\mathrm{Gal}(\overline{K}_\mathfrak{p}(A_{\mathfrak{p},l^\infty})/\overline{K}_\mathfrak{p})$. We denote the unit matrix in $\mathrm{GL}_m(B)$ by $\mathbf{1}$, whenever m is a positive integer and B is a ring, which are clear from the context. Then, we set

$$P_{A,\mathfrak{p}}(X) = \det\left(X \cdot \mathbf{1} - \rho_{A,l^\infty}\left[\frac{K(A_{l^\infty})/K}{\mathfrak{p}_{l^\infty}}\right]\right) \tag{1}$$

for the corresponding characteristic polynomial. Since all prime ideals of $R_{K(A_{l^\infty})}$ that lie over $\mathfrak{p}$ are conjugate over K, $P_{A,\mathfrak{p}}(X)$ is a well-defined monic polynomial of degree $2g$ with coefficients in $\mathbb{Z}_l$. The compatibility of the action of the Galois groups on A_{l^∞} and $A_{\mathfrak{p},l^\infty}$ mentioned at the beginning of this paragraph implies that

$$P_{A,\mathfrak{p}}(X) = \det(X \cdot \mathbf{1} - \rho_{A_\mathfrak{p},l^\infty}(\mathrm{Frob}_\mathfrak{p})). \tag{2}$$

Note that the endomorphism $\rho_{A_\mathfrak{p},l^\infty}(\mathrm{Frob}_\mathfrak{p})$ of $T_l(A_\mathfrak{p})$ is induced by the Frobenius endomorphism of $A_\mathfrak{p}$. Hence by [Mum74, p. 180, Theorem 4], $P_{A,\mathfrak{p}}$ is actually a monic polynomial of degree $2g$ with coefficients in $\mathbb{Z}$, which is independent of l (as long as $l \neq \mathrm{char}(\overline{K}_\mathfrak{p})$).

7.3 Conjugacy class

Let n, r, l_0, and L be the positive integers and the finite Galois extension of K introduced in Proposition 4.1. Then, in the notation introduced so far in this section, and in the notation of Section 3, we attach the following objects to a conjugacy class C of $\mathrm{Gal}(L/K)$:

(3a) $d(C)$ is the maximal number of distinct roots of $P_{A,\mathfrak{p}}(X^{n!})$ in $\tilde{\mathbb{Q}}$, where $\mathfrak{p}$ ranges over the elements of $\mathrm{Max}(R)$ that satisfy $(\frac{L/K}{\mathfrak{p}}) = C$. By Proposition 3.5, the latter set of primes is nonempty. Also, for each $\mathfrak{p} \in \mathrm{Max}(R)$, the number of distinct roots of $P_{A,\mathfrak{p}}(X^{n!})$ in $\tilde{\mathbb{Q}}$ is at most the degree of $P_{A,\mathfrak{p}}(X^{n!})$, which is $2g \cdot n!$ (by Section 7.2). Hence, $d(C)$ is well defined.

(3b) $\mathfrak{p}(C)$ is an element of $\mathrm{Max}(R)$ such that $(\frac{L/K}{\mathfrak{p}(C)}) = C$ and $P_{A,\mathfrak{p}(C)}(X^{n!})$ has exactly $d(C)$ distinct roots in $\tilde{\mathbb{Q}}$.

(3c) $\beta(C)$ is an element of $\mathrm{Gal}(K)$ whose restriction to L belongs to C.

(3d) M is a finite Galois extension of $\mathbb{Q}$ that satisfies the conditions of Lemma 4.3 and contains all of the roots of $P_{A,\mathfrak{p}(C)}(X^{n!})$, for all C.

Next, let Λ be the set of prime numbers l with the following properties:

(4a) l splits completely in M;

(4b) $l \geqslant l_0$ and $\mathrm{char}(R/\mathfrak{p}(C)) \neq l$ for each conjugacy class C of $\mathrm{Gal}(L/K)$;

(4c) for each conjugacy class C of $\mathrm{Gal}(L/K)$, the polynomial $P_{A,\mathfrak{p}(C)}(X^{n!})$ modulo l has exactly $d(C)$ distinct roots in $\tilde{\mathbb{F}}_l$; each of them belongs to $\mathbb{F}_l$.

By the Chebotarev density theorem for number fields, the set of prime numbers l that satisfy Condition (4a) has a positive density (equal to $1/[M : \mathbb{Q}]$). By [FrJ08, p. 167, Corollary 9.2.2], $P_{A,\mathfrak{p}(C)}(X^{n!})$ modulo l has exactly $d(C)$ distinct roots in $\tilde{\mathbb{F}}_l$, if l is sufficiently large. It follows from (3d) that if l satisfies (4a), then all of those roots belong to $\mathbb{F}_l$. Thus, Λ has a positive Dirichlet density.

7.4 Regular elements

We denote the set of $\mathbb{F}_l$-split maximal tori in H_l by $\mathcal{T}_l$ and recall that a semisimple element $\mathbf{t}$ of H_l is *regular* if $\mathbf{t}$ belongs to a unique maximal torus of H_l [Bor91, p. 160, Proposition]. We denote the set of all semisimple regular elements of H_l by $H_{l,\mathrm{ssreg}}$. By Section 4.2, the rank of H_l (denoted by r in Proposition 4.1) is $r = \dim(T)$ for each $T \in \mathcal{T}_l$.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

The following lemma generalizes [Zyw16, Section 3.2] from the case where K is a number field to our case where K is a finitely generated extension of $\mathbb{Q}$.

LEMMA 7.5. *In the notation of Section 7.3, let C be a conjugacy class in* $\mathrm{Gal}(L/K)$ *and let $l \in \Lambda$. Then:*

(a) *There exists $\mathbf{b} \in \rho_{A,l}(\beta(C)\mathrm{Gal}(L)) \cap \rho_{A,l}((L(A_l)/K)/\mathfrak{p}(C))$.*

(b) *For each $T \in \mathcal{T}_l$ and every $\mathbf{t} \in T(\mathbb{F}_l)$, we have $T(\mathbb{F}_l) \cong (\mathbb{F}_l^{\times})^r$ and $\mathbf{t}^{n!} \in \rho_{A,l}(\mathrm{Gal}(L))$.*

(c) *If $\mathbf{b}$ satisfies (a), then*

$$\begin{aligned}&|\{\mathbf{h} \in \rho_{A,l}(\beta(C)\mathrm{Gal}(L)) \mid \det(\mathbf{1}-\mathbf{h}) = 0\}|\\ &\quad \geqslant \frac{1}{(n!)^r} \sum_{T \in \mathcal{T}_l} |\{\mathbf{t} \in T(\mathbb{F}_l) \mid \det(\mathbf{1}-\mathbf{b}\mathbf{t}^{n!}) = 0 \text{ and } \mathbf{t}^{n!} \in H_{l,\mathrm{ssreg}}\}|.\end{aligned}$$

Proof of (a). By (4b), $\mathrm{char}(R/\mathfrak{p}(C)) \neq l$, so by Remark 5.3, $\mathfrak{p}(C)$ is étale in $R_{K(A_l)}$. By Section 3.2, R_L is a ring cover of R. Hence, by [FrJ08, p. 110, Remark 6.1.7], $R_{K(A_l)}R_L$ is a ring cover of $R_{K(A_l)}$; in particular, $R_{K(A_l)}R_L = R_{L(A_l)}$ is the integral closure of $R_{K(A_l)}$ in $L(A_l)$. Thus, $R_{L(A_l)}$ is étale over $R_{K(A_l)}$, hence also over R.

In particular, $\mathfrak{p}(C)$ is étale in $R_{L(A_l)}$, so $\rho_{A,l}(\frac{L(A_l)/K}{\mathfrak{p}(C)})$ makes sense. Moreover, by (3b) and by Section 3.4, $(\frac{L(A_l)/K}{\mathfrak{p}(C)})|_L = (\frac{L/K}{\mathfrak{p}(C)}) = C$. Hence, by (3c), there exists $\beta' \in (\frac{L(A_l)/K}{\mathfrak{p}(C)})$ such that $\beta'|_L = \beta(C)|_L$, so $\beta' \in \beta(C)\mathrm{Gal}(L)$. Then, $\mathbf{b} = \rho_{A,l}(\beta') \in \rho_{A,l}(\beta(C)\mathrm{Gal}(L)) \cap \rho_{A,l}(\frac{L(A_l)/K}{\mathfrak{p}(C)})$, as (a) claims.

Proof of (b). Since T belongs to $\mathcal{T}_l$, it splits over $\mathbb{F}_l$. Hence, by Section 4.2, $T(\mathbb{F}_l) \cong (\mathbb{F}_l^{\times})^r$. By Proposition 4.1(b), $(H_l(\mathbb{F}_l) : \rho_{A,l}(\mathrm{Gal}(L))) \leqslant n$. Therefore, if $\mathbf{t} \in T_l(\mathbb{F}_l)$, then $\mathbf{t}^{n!} \in \rho_{A,l}(\mathrm{Gal}(L))$.

Proof of (c). For all $T \in \mathcal{T}_l$ and $\mathbf{t} \in T(\mathbb{F}_l)$, we have by (a) and (b) that

$$\mathbf{b}\mathbf{t}^{n!} \in \rho_{A,l}(\beta(C)\mathrm{Gal}(L))\rho_{A,l}(\mathrm{Gal}(L)) = \rho_{A,l}(\beta(C)\mathrm{Gal}(L)).$$

Therefore,

$$\begin{aligned}&\bigcup_{T \in \mathcal{T}_l} \{\mathbf{b}\mathbf{t}^{n!} \mid \mathbf{t} \in T(\mathbb{F}_l), \det(\mathbf{1}-\mathbf{b}\mathbf{t}^{n!}) = 0, \mathbf{t}^{n!} \in H_{l,\mathrm{ssreg}}\}\\ &\quad \subseteq \{\mathbf{h} \in \rho_{A,l}(\beta(C)\mathrm{Gal}(L)) \mid \det(\mathbf{1}-\mathbf{h}) = 0\}. \qquad (5)\end{aligned}$$

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

Claim. The union in (5) is disjoint.

Indeed, consider distinct tori $T_1, T_2 \in \mathcal{T}_l$. Consider elements $\mathbf{t}_1 \in T_1(\mathbb{F}_l)$ and $\mathbf{t}_2 \in T_2(\mathbb{F}_l)$ such that $\mathbf{t}_1^{n!}, \mathbf{t}_2^{n!} \in H_{l,\mathrm{ssreg}}$ and $\mathbf{b}\mathbf{t}_1^{n!} = \mathbf{b}\mathbf{t}_2^{n!}$. Then, $\mathbf{t}_1^{n!} = \mathbf{t}_2^{n!}$, so $\mathbf{t}_1^{n!}$ and $\mathbf{t}_2^{n!}$ lie in the same maximal torus of H_l. Since $\mathbf{t}_1^{n!} \in T_1(\mathbb{F}_l)$ and $\mathbf{t}_2^{n!} \in T_2(\mathbb{F}_l)$, we have $T_1 = T_2$, as claimed.

If $T \in \mathcal{T}_l$ and $\mathbf{t}' \in T(\mathbb{F}_l)$, then by (b), there are at most $(n!)^r$ elements $\mathbf{t}$ in $T(\mathbb{F}_l)$ for which $\mathbf{t}^{n!} = \mathbf{t}'$. It follows from the claim that

$$\begin{aligned}
&|\{\mathbf{h} \in \rho_{A,l}(\beta(C)\mathrm{Gal}(L)) \mid \det(\mathbf{1} - \mathbf{h}) = 0\}| \\
&\quad \geqslant \sum_{T \in \mathcal{T}_l} |\{\mathbf{b}\mathbf{t}^{n!} \in \mathrm{GL}_{2g}(\mathbb{F}_l) \mid \mathbf{t} \in T(\mathbb{F}_l), \det(\mathbf{1} - \mathbf{b}\mathbf{t}^{n!}) = 0, \mathbf{t}^{n!} \in H_{l,\mathrm{ssreg}}\}| \\
&\quad = \sum_{T \in \mathcal{T}_l} |\{\mathbf{t}^{n!} \in T(\mathbb{F}_l) \mid \mathbf{t} \in T(\mathbb{F}_l), \det(\mathbf{1} - \mathbf{b}\mathbf{t}^{n!}) = 0, \mathbf{t}^{n!} \in H_{l,\mathrm{ssreg}}\}| \\
&\quad \geqslant \frac{1}{(n!)^r} \sum_{T \in \mathcal{T}_l} |\{\mathbf{t}' \in T(\mathbb{F}_l) \mid \det(\mathbf{1} - \mathbf{b}(\mathbf{t}')^{n!}) = 0, (\mathbf{t}')^{n!} \in H_{l,\mathrm{ssreg}}\}|,
\end{aligned}$$

as claimed. □

REMARK 7.6. We consider a prime number $l \in \Lambda$, a point $\mathbf{b} \in \mathrm{GL}_{2g}(\mathbb{F}_l)$, and a torus $T \in \mathcal{T}_l$. Let $W = W_{\mathbf{b}}$ be the Zariski-closed subset of T defined by the equation $\det(\mathbf{1} - \mathbf{b}\mathbf{t}^{n!}) = 0$. By Proposition 4.1(a), H_l contains the group of scalar matrices $\mathbb{G}_m$. Since $\mathbb{G}_m$ is contained in the center of H_l and each element of $\mathbb{G}_m$ is semisimple, $\mathbb{G}_m \leqslant T$ [Bor91, p. 151, Corollary 11.11].

Let $\varphi : W \to T/\mathbb{G}_m$ be the restriction to W of the quotient map $T \to T/\mathbb{G}_m$ and set $\bar{\mathbf{t}} = \varphi(\mathbf{t})$ for each $\mathbf{t} \in T(\tilde{\mathbb{F}}_l)$. Then,

$$\varphi^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l) = \{\lambda\mathbf{t} \in T(\tilde{\mathbb{F}}_l) \mid \lambda \in \tilde{\mathbb{F}}_l^{\times}, \det(\mathbf{1} - \lambda^{n!}\mathbf{b}\mathbf{t}^{n!}) = 0\}. \tag{6}$$

Hence, $|\varphi^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)|$ is equal to the number of solutions in $\tilde{\mathbb{F}}_l^{\times}$ of the equation $\det(\mathbf{1} - X^{n!}\mathbf{b}\mathbf{t}^{n!}) = 0$, hence also to the number of solutions in $\tilde{\mathbb{F}}_l^{\times}$ of the equation $\det(X^{n!}\mathbf{1} - \mathbf{b}\mathbf{t}^{n!}) = 0$. Since the polynomial $\det(X^{n!}\mathbf{1} - \mathbf{b}\mathbf{t}^{n!})$ is monic of degree $(n!) \cdot 2g$, the number of solutions in $\tilde{\mathbb{F}}_l^{\times}$ of the latter equation is at most $(n!) \cdot 2g$. Therefore,

$$d = \max_{\mathbf{t} \in W(\tilde{\mathbb{F}}_l)} |\varphi^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)| \leqslant (n!) \cdot 2g. \tag{7}$$

□

The following result is the analog of [Zyw16, Lemma 3.4] for finitely generated extensions of $\mathbb{Q}$ rather than only for number fields. The use of

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

the Chebotarev density theorem in the proof of [Zyw16, Lemma 3.4] is replaced here by an application of Proposition 3.5.

Lemma 7.7. *Let A, L, n, r, l_0, and H_l with $l \geqslant l_0$ be as in Proposition 4.1. Let M be as in Lemma 4.3. Let C, $d(C)$, $\beta(C)$, $\mathfrak{p}(C)$, and Λ be as in Section 7.3. We consider $T \in \mathcal{T}_l$, suppose in addition that l is a sufficiently large element of Λ, and use Lemma 7.5(a) to choose a matrix $\mathbf{b} \in \rho_{A,l}(\beta(C)\mathrm{Gal}(L)) \cap \rho_{A,l}(\frac{L(A_l)/K}{\mathfrak{p}(C)})$. Then, in the notation of Remark 7.6, there exists $\mathbf{t} \in T(\mathbb{F}_l)$ such that $\varphi^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)$ consists of d distinct points, each belonging to $W(\mathbb{F}_l)$.*

Proof. By (3b), the polynomial $P_{A,\mathfrak{p}(C)}(X^{n!})$ with coefficients in $\mathbb{Z}$ has exactly $d(C)$ distinct roots in $\tilde{\mathbb{Q}}$. Moreover, by (1), for each maximal ideal $\mathfrak{P}(C)$ of $R_{L(A_l)}$ that lies over $\mathfrak{p}(C)$ the reduction of $P_{A,\mathfrak{p}(C)}(X^{n!})$ modulo l is the polynomial $\det(X^{n!}\mathbf{1} - \rho_{A,l}[\frac{L(A_l)/K}{\mathfrak{P}(C)}])$ in $\mathbb{F}_l[X]$. The latter is equal to $\det(X^{n!}\mathbf{1} - \mathbf{b})$, because $\mathbf{b} \in \rho_{A,l}(\frac{L(A_l)/K}{\mathfrak{p}(C)})$. By (4c), the reduced polynomial has exactly $d(C)$ distinct roots in $\tilde{\mathbb{F}}_l$, each belonging to $\mathbb{F}_l$. By (6), this means that

$$\varphi^{-1}(\bar{\mathbf{1}})(\tilde{\mathbb{F}}_l) = \{\lambda\mathbf{1} \in T(\tilde{\mathbb{F}}_l) \mid \lambda \in \tilde{\mathbb{F}}_l^\times, \det(\mathbf{1} - \lambda^{n!}\mathbf{b}) = 0\}$$

consists of $d(C)$ distinct points, each belonging to $W(\mathbb{F}_l)$. Hence, by (7), $d(C) \leqslant d$. Thus, the unit matrix $\mathbf{1}$ will be the desired element $\mathbf{t}$ of $T(\mathbb{F}_l)$ as soon as we prove that $d \leqslant d(C)$.

We consider two systems $\mathbf{B}$ and $\mathbf{T}$ of variables for GL_{2g} (considered as a Zariski-closed subset of $\mathbb{A}^{(2g)^2+1}$) and the monic polynomial $\det(X^{n!}\mathbf{1} - \mathbf{B}\mathbf{T}^{n!})$ in X with coefficients in $\mathbb{Z}[\mathbf{B},\mathbf{T}]$. By Lemma 6.2, for each large $l \in \mathbb{L}$ and all $\mathbf{b}' \in \mathrm{GL}_{2g}(\mathbb{F}_l)$ there exists a Zariski-closed subset $V_{l,\mathbf{b}'}$ of $\mathrm{GL}_{2g,\mathbb{F}_l}$ such that

$$\begin{aligned} V_{l,\mathbf{b}'}(\tilde{\mathbb{F}}_l) = \{\mathbf{t} \in \mathrm{GL}_{2g}(\tilde{\mathbb{F}}_l) \mid \det(X^{n!}\mathbf{1} - \mathbf{b}'\mathbf{t}^{n!}) &\text{ has at most} \\ d-1 \text{ distinct roots in } \tilde{\mathbb{F}}_l\}&. \end{aligned}$$

Moreover, Lemma 6.2 gives positive integers c_1' and c_2', which are independent of l and $\mathbf{b}'$ such that $V_{l,\mathbf{b}'}$ is defined by at most c_1' polynomials of degree at most c_2'.

By Lemma 4.3, T is defined in $\mathbb{A}_{\mathbb{F}_l}^{4g^2+1}$ by at most c_1 polynomials of degree at most c_2, where c_1 and c_2 are positive integers that do not depend on l. Hence, by the preceding paragraph, $V = V_{l,\mathbf{b}'} \cap T$ is a Zariski-closed

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

subset of T, which is defined by at most $c_1'' = c_1' + c_1$ polynomials of degree at most $c_2'' = \max(c_2', c_2)$. Again, c_1'' and c_2'' are positive integers that do not depend on l nor on $\mathbf{b}'$. By Lemma 4.6, this implies that the number of absolutely irreducible components of $V_{l,\mathbf{b}'}$ is bounded by a constant c_3', which is independent of l and $\mathbf{b}'$. Moreover,

$$V(\tilde{\mathbb{F}}_l) = \{\mathbf{t} \in T(\tilde{\mathbb{F}}_l) \mid \det(X^{n!}\mathbf{1} - \mathbf{b}\mathbf{t}^{n!}) \text{ has at most } \\ d-1 \text{ distinct roots in } \tilde{\mathbb{F}}_l\}.$$

By (7), there exists $\mathbf{t} \in W(\tilde{\mathbb{F}}_l) \smallsetminus V(\tilde{\mathbb{F}}_l)$. In particular, V is a Zariski-closed proper subset of T. Since T is absolutely integral of dimension r (Section 4.2), $\dim(V) \leqslant r-1$.

By Proposition 4.4, $|V(\mathbb{F}_l)| \leqslant c_3 l^{r-1}$, where again c_3 is a positive integer that depends neither on l nor on $\mathbf{b}$. By Lemma 7.5(b), $|T(\mathbb{F}_l)| = (l-1)^r$. Thus, for sufficiently large $l \in \Lambda$ there exists $\mathbf{t}_1 \in T(\mathbb{F}_l)$ such that the polynomial $\det(X^{n!}\mathbf{1} - \mathbf{b}\mathbf{t}_1^{n!})$ with coefficients in $\mathbb{F}_l$ has exactly d distinct roots in $\tilde{\mathbb{F}}_l$. By Lemma 7.5(b), $\mathbf{t}_1^{n!} \in \rho_{A,l}(\mathrm{Gal}(L))$, so $\mathbf{b}\mathbf{t}_1^{n!} \in \rho_{A,l}(\beta(C)\mathrm{Gal}(L))\rho_{A,l}(\mathrm{Gal}(L)) = \rho_{A,l}(\beta(C)\mathrm{Gal}(L))$. Thus, there exists $\sigma \in \mathrm{Gal}(L)$ such that $\mathbf{b}\mathbf{t}_1^{n!} = \rho_{A,l}(\beta(C)\sigma)$. We consider the conjugacy class C' of $(\beta(C)\sigma)|_{L(A_l)}$ of $\mathrm{Gal}(L(A_l)/K)$ and note that $C'|_L = C$.

By Proposition 3.5, there is $\mathfrak{p} \in \mathrm{Max}(R)$ such that $l \neq \mathrm{char}(R/\mathfrak{p})$ and $((L(A_l)/K)/\mathfrak{p}) = C'$. Then, $((L/K)/\mathfrak{p}) = C$ and $\mathbf{b}\mathbf{t}_1^{n!} \in \rho_{A,l}((L(A_l)/K)/\mathfrak{p})$. By (1), $\det(X^{n!}\mathbf{1} - \mathbf{b}\mathbf{t}_1^{n!})$ is equal to the reduction of $P_{A,\mathfrak{p}}(X^{n!})$ modulo l. By the preceding paragraph, the former polynomial has d distinct roots in $\tilde{\mathbb{F}}_l$. Hence $P_{A,\mathfrak{p}}(X^{n!})$ has at least d distinct roots in $\tilde{\mathbb{Q}}$. It follows from (3a), that $d \leqslant d(C)$. Combining this inequality with the inequality proved in the first paragraph of the proof, we have $d = d(C)$, as claimed. □

LEMMA 7.8. *Let l, T, and W be as in Remark 7.6, and let $\mathbf{b} \in \mathrm{GL}_{2g}(\mathbb{F}_l)$ be the matrix chosen in Lemma 7.7.*

(a) *If l is sufficiently large, then each irreducible component of $W_{\tilde{\mathbb{F}}_l}$ has dimension $r-1$ and is defined over $\mathbb{F}_l$.*

(b) *There exists a real constant c_6 that does not depend on l nor on $\mathbf{b}$ such that $|W(\mathbb{F}_l)| \geqslant l^{r-1} - c_6 l^{r-3/2}$.*

Proof of (a). (After [Zyw16, Proof of Lemma 3.5]) By Remark 7.6, $W_{\tilde{\mathbb{F}}_l}$ is the intersection of $T_{\tilde{\mathbb{F}}_l}$ with the hypersurface defined by the equation $\det(\mathbf{1} - \mathbf{b}\mathbf{t}^{n!}) = 0$. This hypersurface does not contain $T_{\tilde{\mathbb{F}}_l}$, because $\mathbf{1} \in$

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

$T(\tilde{\mathbb{F}}_l)$, so $\lambda\mathbf{1}\in T(\tilde{\mathbb{F}}_l)$ for each $\lambda\in\tilde{\mathbb{F}}_l^\times$ (Remark 7.6), and there exists $\lambda\in\tilde{\mathbb{F}}_l^\times$ with $\det(\mathbf{1}-\mathbf{b}((\lambda\mathbf{1})^{n!}))\neq 0$. Since T is absolutely irreducible of dimension r, each of the irreducible components $W_1,\ldots,W_m$ of $W_{\tilde{\mathbb{F}}_l}$ is of dimension $r-1$ [Lan58, p. 36, Theorem 11]. It remains to prove that each of the W_i's is defined over $\mathbb{F}_l$.

To this end, we set $\overline{T}=(T/\mathbb{G}_m)_{\tilde{\mathbb{F}}_l}$. Recall that $\varphi:W\to T/\mathbb{G}_m$ is the restriction to W of the quotient map $T\to T/\mathbb{G}_m$. Let $\tilde{\varphi}:W_{\tilde{F}_l}\to\overline{T}$ be the morphism obtained from φ by base change from $\mathbb{F}_l$ to $\tilde{\mathbb{F}}_l$. For each $1\leqslant i\leqslant m$, let $\varphi_i:W_i\to\overline{T}$ be the restriction of $\tilde{\varphi}$ to W_i. By Remark 7.6 for $\mathbf{t}\in W(\tilde{\mathbb{F}}_l)$, we have that $|\tilde{\varphi}^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)|$ is finite and bounded by a constant d, which is independent of l. Since both W_i and $\overline{T}$ are irreducible algebraic varieties of dimension $r-1$, the morphism φ_i is dominant.

By [Mil80, p. 26, Theorem 3.14], $\overline{T}$ has a nonempty Zariski-open subset $\overline{T}_0$ and each W_i has a nonempty Zariski-open subset W_{i0} such that the restriction φ_{i0} of φ_i to W_{i0} is a standard étale morphism onto $\overline{T}_0$. In particular, φ_{i0} is a finite morphism [FrJ08, p. 109, Lemma 6.1.2 and Definition 6.1.3]. Let $d_i=\deg(\varphi_{i0})$ be the degree of the function field of W_{i0} over the function field of $\overline{T}$. By [Liu06, p. 176, Exercise 1.25(a) of Chapter 5],

$$|\varphi_{i0}^{-1}(\overline{\mathbf{u}})(\tilde{\mathbb{F}}_l)|=d_i\quad\text{for each }\overline{\mathbf{u}}\in\overline{T}_0(\tilde{\mathbb{F}}_l).\tag{8}$$

Next, we observe that for $i\neq j$ we have $\dim(W_i\cap W_j)\leqslant r-2$. Hence,

$$\dim\left(\bigcup_{i\neq j}W_i\cap W_j\right)\leqslant r-2.$$

Therefore, the dimension of the Zariski closure Z of $\varphi(\bigcup_{i\neq j}W_i\cap W_j)$ in $\overline{T}$ is also $\leqslant r-2$, so $\dim(Z)\leqslant r-2<r-1=\dim(\overline{T})$; in particular, $\overline{T}(\tilde{\mathbb{F}}_l)\smallsetminus Z(\tilde{\mathbb{F}}_l)$ is nonempty.

By Remark 7.6, $\tilde{\varphi}^{-1}(\overline{\mathbf{u}})(\tilde{\mathbb{F}}_l)$ is finite for each $\mathbf{u}\in W(\tilde{\mathbb{F}}_l)$, that is, $\tilde{\varphi}$ is a quasi-finite morphism. Let $\bar{\mathbf{t}}$ be the element of $T/\mathbb{G}_m$ given by Lemma 7.7 with the property that

$$\varphi^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)\quad\text{consists of }d\text{ points of }W(\tilde{\mathbb{F}}_l),\ \text{each lying in }W(\mathbb{F}_l).\tag{9}$$

By [Gro66, p. 231, Proposition 15.5.1(i)], the set of all $\overline{\mathbf{u}}\in\overline{T}$ such that $|\tilde{\varphi}^{-1}(\overline{\mathbf{u}})|\geqslant|\tilde{\varphi}^{-1}(\bar{\mathbf{t}})|=d$ is Zariski-open. Hence, there exists $\overline{\mathbf{u}}\in\overline{T}_0(\tilde{\mathbb{F}}_l)\smallsetminus Z(\tilde{\mathbb{F}}_l)$ such that $|\tilde{\varphi}^{-1}(\overline{\mathbf{u}})(\tilde{\mathbb{F}}_l)|\geqslant d$. It follows from (7), that $|\tilde{\varphi}^{-1}(\overline{\mathbf{u}})(\tilde{\mathbb{F}}_l)|=d$.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

Then, $\varphi_0^{-1}(\bar{\mathbf{u}})(\tilde{\mathbb{F}}_l) = \dot{\bigcup}_{i=1}^m \varphi_{i0}^{-1}(\bar{\mathbf{u}})(\tilde{\mathbb{F}}_l)$, so, by (8),

$$d = |\varphi_0^{-1}(\bar{\mathbf{u}})(\tilde{\mathbb{F}}_l)| = \sum_{i=0}^m |\varphi_{i0}^{-1}(\bar{\mathbf{u}})(\tilde{\mathbb{F}}_l)| = \sum_{i=0}^m d_i. \tag{10}$$

By [Gro66, p. 231, Lemme 15.5.2], $|\varphi_i^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)| \leqslant d_i$ for $i = 1, \ldots, m$. Since $\varphi^{-1}(\bar{t})(\tilde{\mathbb{F}}_l) = \bigcup_{i=1}^m \varphi_i^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)$, we have

$$d = |\varphi^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)| \leqslant \sum_{i=1}^m |\varphi_i^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)| \leqslant \sum_{i=1}^m d_i = d.$$

Hence,

$$\begin{aligned} &|\varphi_i^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)| = d_i \geqslant 1 \quad \text{for each } i \text{ between 1 and } m \\ &\text{and } \varphi^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l) = \dot{\bigcup_{i=1}^m} \varphi_i^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l). \end{aligned} \tag{11}$$

In other words, each point in $\varphi^{-1}(\bar{\mathbf{t}})(\tilde{\mathbb{F}}_l)$ belongs to $W_i(\tilde{\mathbb{F}}_l)$ for a unique i between 1 and m and $\varphi_i^{-1}(\mathbf{t})(\tilde{\mathbb{F}}_l) = \varphi^{-1}(\mathbf{t})(\tilde{\mathbb{F}}_l) \cap W_i(\tilde{\mathbb{F}}_l)$ is nonempty.

Finally we consider i between 1 and m and choose $\mathbf{w}_i \in W_i(\mathbb{F}_l)$ (by (9)). Then, for each $\sigma \in \mathrm{Gal}(\mathbb{F}_l)$ we have $\mathbf{w}_i^\sigma = \mathbf{w}_i$, so $\mathbf{w}_i \in W_i(\mathbb{F}_l) \cap W_i(\mathbb{F}_l)^\sigma$. It follows from the uniqueness property mentioned in the preceding paragraph, that $W_i^\sigma = W_i$. Since $\mathbb{F}_l$ is a perfect field, it follows from [Lan58, p. 74, the equivalence between the conditions C2 and C6] that W_i is defined over $\mathbb{F}_l$, as claimed.

Proof of (b). Statement (b) follows from (a) and from Lemma 4.6 and Proposition 4.4. □

LEMMA 7.9. *There exists a positive real number c_4 that depends only on r such that $|T(\mathbb{F}_l) \smallsetminus H_{l,\mathrm{ssreg}}(\mathbb{F}_l)| \leqslant c_4 l^{r-1}$ for all $l \in \Lambda$ and every maximal torus T of H_l.*

Proof. Our lemma coincides with [Zyw16, Lemma 3.6], which depends only on the fact that the H_l's are split reductive groups over $\mathbb{F}_l$ of rank r, which is independent of l. By Proposition 4.1, this fact holds in our case.

Alternatively, Proposition 4.1 ensures that the groups H_l arise from an abelian variety A_0 of dimension g over a number field. Hence, we may use [Zyw16, Lemma 3.6] for our abelian variety A.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

Nevertheless, for the convenience of the reader we highlight the main points of Zywina's proof. For references and more details, the reader is referred to the original proof.

Let $X(T)$ be the group of all characters $\alpha : T \to \mathbb{G}_{m,\mathbb{F}_l}$ of T and let R be the finite set of *weights* of T. By definition, each $\alpha \in R$ is an element of $X(T)$ for which there exists a nonzero $\mathbf{v} \in \mathbb{F}_l^{2g}$ such that $\mathbf{t}\mathbf{v} = \alpha(\mathbf{t})\mathbf{v}$ for all $\mathbf{t} \in T$. One knows that an element $\mathbf{t} \in T(\mathbb{F}_l)$ is regular if and only if $\alpha(\mathbf{t}) \neq \mathbf{1}$ for each $\alpha \in R$, so

$$\{\mathbf{t} \in T(\mathbb{F}_l) \mid \mathbf{t} \text{ is not regular in } H_l\} = \bigcup_{\alpha \in R} \mathrm{Ker}(\alpha)(\mathbb{F}_l).$$

Thus, it suffices to bound the order of R and the order of $\mathrm{Ker}(\alpha)(\mathbb{F}_l)$ for each $\alpha \in R$ in terms of r only.

One also knows that $\mathrm{Ker}(\alpha) = D_\alpha^0 \times F_\alpha$, where D_α^0 is a split torus over $\mathbb{F}_l$ of rank $r - 1$ and F_α is finite. Since $\dim(T) = r$, the group F_α is isomorphic to a subgroup of $\tilde{\mathbb{F}}_l^\times$, so F_α is cyclic. It follows that $|\mathrm{Ker}(\alpha)(\mathbb{F}_l)| \leqslant |F_\alpha| l^{r-1}$. Thus, it suffices to bound $|R|$ and $|F_\alpha|$ for each $\alpha \in R$ in terms of r only.

In order to do this we assume that H_l, T, and $\mathrm{Ker}(\alpha)$ are defined over $\tilde{\mathbb{F}}_l$. Then, using the theory of *root datum* and the fact that F_α is cyclic, one finds $\beta \in X(T)$ such that $\alpha = n\beta$ for some positive integral multiple n of $|F_\alpha|$. Then, with $\alpha^\vee$ being the dual of α we have $2 = \langle \alpha, \alpha^\vee \rangle = n\langle \beta, \alpha^\vee \rangle \equiv 0 \mod |F_\alpha|$. It follows that $|F_\alpha| \leqslant 2$.

Finally, we view R as a root system in a Euclidean space of dimension at most r. Using the correspondence between such systems and Dynkin diagrams, one recalls that there are only finitely many root systems of rank $\leqslant r$ (up to isomorphisms). In particular, $|R|$ is bounded in terms of r only, as desired. □

LEMMA 7.10. *Let l be a sufficiently large element of Λ, C a conjugacy class of* $\mathrm{Gal}(L/K)$, *and* $\mathbf{b}$ *a matrix in* $\mathrm{GL}_{2g}(\mathbb{F}_l)$ *that satisfies Condition (a) of Lemma 7.5. Then, there exists a positive real number c_5 not depending on the choice of l and* $\mathbf{b}$ *such that* $|\{\mathbf{t} \in T(\mathbb{F}_l) \mid \det(\mathbf{1} - \mathbf{b}\mathbf{t}^{n!}) = 0$ *and* $\mathbf{t}^{n!} \in H_{l,\mathrm{ssreg}}\}| \geqslant l^{r-1} - c_5 l^{r-(3/2)}$.

Proof. We consider the set $D = \{\mathbf{t} \in T(\mathbb{F}_l) \mid \mathbf{t}^{n!} \notin H_{l,\mathrm{ssreg}}\}$. Since $T(\mathbb{F}_l) \cong (\mathbb{F}_l^\times)^r$ (Lemma 7.5(b)), for each $\mathbf{t}' \in T(\mathbb{F}_l)$ there exist at most $(n!)^r$ elements $\mathbf{t} \in T(\mathbb{F}_l)$ such that $\mathbf{t}^{n!} = \mathbf{t}'$. Hence, by Lemma 7.9 we have for sufficiently large l in Λ that

$$|D| \leqslant (n!)^r |\{\mathbf{t}' \in T(\mathbb{F}_l) \mid \mathbf{t}' \notin H_{l,\mathrm{ssreg}}\}| \leqslant c_4 (n!)^r l^{r-1}. \tag{12}$$

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

Note that the group $\mathbb{F}_l^\times$ acts on D by multiplication. Indeed, let $\mathbf{t} \in D$ and $\lambda \in \mathbb{F}_l^\times$. Then, there exists a torus $T' \in \mathcal{T}_l$ such that $T' \neq T$ and $\mathbf{t}^{n!} \in T(\mathbb{F}_l) \cap T'(\mathbb{F}_l)$. Hence, $\lambda\mathbf{t} \in T(\mathbb{F}_l)$ and $(\lambda\mathbf{t})^{n!} \in T(\mathbb{F}_l) \cap T'(\mathbb{F}_l)$, so $\lambda\mathbf{t} \in D$.

By (7), for each $\mathbf{t} \in D$ there are at most d values of λ in $\mathbb{F}_l^\times$ such that $\lambda\mathbf{t} \in W(\mathbb{F}_l)$. Hence, by (12), $|\{\mathbf{t} \in W(\mathbb{F}_l) \mid \mathbf{t}^{n!} \notin H_{l,\mathrm{ssreg}}\}| \leqslant d|D|/(l-1) \leqslant dc_4(n!)^r l^{r-2}$. It follows from Lemma 7.8(b) that there exists a real positive constant c_5 such that

$$|\{\mathbf{t} \in T(\mathbb{F}_l) \mid \mathbf{t} \in W(\mathbb{F}_l) \text{ and } \mathbf{t}^{n!} \in H_{l,\mathrm{ssreg}}\}| \geqslant l^{r-1} - c_5 l^{r-(3/2)},$$

as claimed. □

§8. Main result

The results achieved so far lead in this section to the proof of the main theorem of our work: For almost all $\sigma \in \mathrm{Gal}(K)$, there are infinitely many $l \in \mathbb{L}$ such that $A_l(\tilde{K}(\sigma)) \neq 0$. The proof uses an analog of a combinatorial argument that appears in [Zyw16, Section 1].

Lemma 8.1. *Let K be a finitely generated extension of $\mathbb{Q}$, and let A be an abelian variety over K of positive dimension g. Let $\mathbb{L}, n, r$ be as in Proposition 4.1. Let Λ be the set of prime numbers of positive Dirichlet density introduced in Section 7.3. Then, there exists a positive real number c such that after deleting finitely many elements from Λ, the following hold:*

(a) *For all $l \in \Lambda$ and $\beta \in \mathrm{Gal}(K)$, we have*

$$\frac{|\{\mathbf{h} \in \rho_{A,l}(\beta\mathrm{Gal}(L)) \mid \det(\mathbf{1} - \mathbf{h}) = 0\}|}{|\rho_{A,l}(\beta\mathrm{Gal}(L))|} \geqslant \frac{c}{l}.$$

(b) *The family $(L(A_l))_{l\in\mathbb{L}}$ of Galois extensions of L is linearly disjoint.*

Proof. Statement (b) holds by virtue of Proposition 4.1(b) and Remark 2.3, so we only have to prove (a).

We consider an element $\beta \in \mathrm{Gal}(K)$ and the conjugacy class C of $\mathrm{Gal}(L/K)$ that contains $\beta|_L$. Then $\beta(C) = \beta$ satisfies (3c) in Section 7.3. Let $\mathfrak{p}(C)$ be the chosen element of $\mathrm{Max}(R)$ that satisfies (3b) in Section 7.3. Next we consider $l \in \Lambda$ and use Lemma 7.5(a) to choose a point $\mathbf{b} \in \rho_{A,l}(\beta\mathrm{Gal}(L)) \cap \rho_{A,l}(\frac{L(A_l)/K}{\mathfrak{p}(C)})$.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

By Lemma 7.5(c) and Lemma 7.10,

$$\begin{aligned}
&|\{\mathbf{h}\in\rho_{A,l}(\beta\mathrm{Gal}(L))\mid\det(\mathbf{1}-\mathbf{h})=0\}|\\
&\quad\geqslant\frac{1}{(n!)^r}\sum_{T\in\mathcal{T}_l}|\{\mathbf{t}\in T(\mathbb{F}_l)\mid\det(\mathbf{1}-\mathbf{bt}^{n!})=0,\,\mathbf{t}^{n!}\in H_{l,\mathrm{ssreg}}\}|\\
&\quad\geqslant\frac{1}{(n!)^r}\sum_{T\in\mathcal{T}_l}(l^{r-1}-c_5l^{r-3/2}),\tag{1}
\end{aligned}$$

where c_5 is a positive constant that does not depend on l.

We consider $T\in\mathcal{T}_l$. Since H_l is a reductive group (Proposition 4.1), T coincides with its centralizer in H_l [Bor91, p. 175, Corollary 2(c)]. Hence, denoting the normalizer of T in H_l by N, we get that $\mathcal{W}_{H_l}=N/T$ is the Weyl group of H_l. It follows that the subgroup $N_l=\{\mathbf{h}\in H_l(\mathbb{F}_l)\mid T^{\mathbf{h}}=T\}$ of $H_l(\mathbb{F}_l)$ satisfies $N_l/T(\mathbb{F}_l)\leqslant\mathcal{W}_{H_l}$.

By Section 4.2, all elements of $\mathcal{T}_l$ are conjugate in $H_l(\mathbb{F}_l)$ and $|T(\mathbb{F}_l)|=(l-1)^r$. Hence,

$$\begin{aligned}
|\mathcal{T}_l|&=\frac{|H_l(\mathbb{F}_l)|}{|N_l|}=\frac{|H_l(\mathbb{F}_l)|}{(N_l:T(\mathbb{F}_l))|T(\mathbb{F}_l)|}\\
&=\frac{|H_l(\mathbb{F}_l)|}{(N_l:T(\mathbb{F}_l))(l-1)^r}\geqslant\frac{|H_l(\mathbb{F}_l)|}{|\mathcal{W}_{H_l}|(l-1)^r}.
\end{aligned}$$

Therefore, by (1),

$$\begin{aligned}
&|\{\mathbf{h}\in\rho_{A,l}(\beta\mathrm{Gal}(L))\mid\det(\mathbf{1}-\mathbf{h})=0\}|\\
&\quad\geqslant\frac{1}{(n!)^r}\frac{|H_l(\mathbb{F}_l)|(l^{r-1}-c_5l^{r-\frac{3}{2}})|}{|\mathcal{W}_{H_l}|(l-1)^r}.\tag{2}
\end{aligned}$$

Note that

$$\frac{l^{r-1}-c_5l^{r-\frac{3}{2}}}{(l-1)^r}=\frac{l^{r-1}(1-c_5l^{-\frac{1}{2}})}{(l-1)^r}\geqslant\frac{l^{r-1}(1-c_5l^{-\frac{1}{2}})}{l^r}=\frac{1-c_5l^{-\frac{1}{2}}}{l}.$$

Therefore, by (2),

$$|\{\mathbf{h}\in\rho_{A,l}(\beta\mathrm{Gal}(L))\mid\det(\mathbf{1}-\mathbf{h})=0\}|\geqslant\frac{1}{(n!)^r}\frac{|H_l(\mathbb{F}_l)|(1-c_5l^{-\frac{1}{2}})}{|\mathcal{W}_{H_l}|\cdot l}.\tag{3}$$

Using the relations $|H_l(\mathbb{F}_l)|\geqslant|\rho_{A,l}(\mathrm{Gal}(L))|=|\rho_{A,l}(\beta\mathrm{Gal}(L))|$, we get from (3) that

$$\frac{|\{\mathbf{h}\in\rho_{A,l}(\beta\mathrm{Gal}(L))\mid\det(\mathbf{1}-\mathbf{h})=0\}|}{|\rho_{A,l}(\beta\mathrm{Gal}(L))|}\geqslant\frac{1}{(n!)^r|\mathcal{W}_{H_l}|}\frac{1-c_5l^{-\frac{1}{2}}}{l}.\tag{4}$$

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

By [Zyw16, end of Section 3.2], there exists a positive constant c_7 such that $|\mathcal{W}_{H_l}| \leqslant c_7$ for all $l \in \mathbb{L}$. Hence, using (4), we get for $c = 1/(2(n!)^r c_7)$, that for each $l \in \Lambda$ with $l \geqslant (2c_5)^2$, we have

$$\frac{|\{\mathbf{h} \in \rho_{A,l}(\beta \mathrm{Gal}(L)) \mid \det(\mathbf{1} - \mathbf{h}) = 0\}|}{|\rho_{A,l}(\beta \mathrm{Gal}(L))|} \geqslant \frac{c}{l},$$

as claimed. ∎

This allows us to prove our main result.

Theorem 8.2. *Let K be a finitely generated extension of $\mathbb{Q}$, and let A be an abelian variety over K of positive dimension. Then, for almost all $\sigma \in$* Gal(K) *there are infinitely many prime numbers l such that $A_l(\tilde{K}(\sigma)) \neq 0$.*

Proof. Let L and Λ be as in Lemma 8.1. Let μ_K be the normalized Haar measure of $\mathrm{Gal}(K)$ and for each $\beta \in \mathrm{Gal}(K)$, let $\mu_{L,\beta}$ be the measure of the space $\beta\mathrm{Gal}(L)$ defined for each measurable set B of $\mathrm{Gal}(K)$, which is contained in $\beta\mathrm{Gal}(L)$ by $\mu_{L,\beta}(B) = [L:K]\mu_K(B)$. In particular, $\mu_L = \mu_{L,1}$ is the normalized Haar measure of $\mathrm{Gal}(L)$. Since μ_K is a Haar measure, the map $\tau \mapsto \beta^{-1}\tau$ is a measure-preserving homeomorphism from $\beta\mathrm{Gal}(L)$ onto $\mathrm{Gal}(L)$.

For $l \in \mathbb{L}$, let $U_{\beta,l} = \{\sigma \in \beta\mathrm{Gal}(L) \mid \det(\mathbf{1} - \rho_{A,l}(\sigma)) = 0\}$. The condition $\det(\mathbf{1} - \rho_{A,l}(\sigma)) = 0$ holds if and only if 1 is an eigenvalue of $\rho_{A,l}(\sigma)$. The latter condition is equivalent to the existence of a nonzero point $\mathbf{a}$ of $A_l(\tilde{K})$ such that $\sigma\mathbf{a} = \mathbf{a}$. It follows that $U_{\beta,l} = \{\sigma \in \beta\mathrm{Gal}(L) \mid A_l(\tilde{K}(\sigma)) \neq 0\}$.

By definition, $\beta^{-1}U_{\beta,l} \subseteq \mathrm{Gal}(L)$ and $(\rho_{A,l}|_{\mathrm{Gal}(L)})^{-1}(\rho_{A,l}(\beta^{-1}U_{\beta,l})) = \beta^{-1}U_{\beta,l}$. Let c be the constant mentioned in Lemma 8.1. Then, by (a) of that lemma,

$$\begin{aligned} \mu_{L,\beta}(U_{\beta,l}) &= \mu_L(\beta^{-1}U_{\beta,l}) = \frac{|\rho_{A,l}(\beta^{-1}U_{\beta,l})|}{|\rho_{A,l}(\mathrm{Gal}(L))|} = \frac{|\rho_{A,l}(U_{\beta,l})|}{|\rho_{A,l}(\beta\mathrm{Gal}(L))|} \\ &= \frac{|\{\mathbf{h} \in \rho_{A,l}(\beta\mathrm{Gal}(L)) \mid \det(\mathbf{1} - \mathbf{h}) = 0\}|}{|\rho_{A,l}(\beta\mathrm{Gal}(L))|} \geqslant \frac{c}{l}. \end{aligned} \tag{5}$$

Now let U_β be the set of all $\sigma \in \beta\mathrm{Gal}(L)$ that belong to infinitely many of the sets $U_{\beta,l}$ with $l \in \Lambda$. Since the Dirichlet density of Λ is positive, (5)

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

implies that $\sum_{l\in\Lambda}\mu_L(\beta^{-1}U_{\beta,l})\geqslant\sum_{l\in\Lambda}(c/l)=\infty$ [FrJ08, first paragraph of Section 6.3]. It follows from (b) of Lemma 8.1 and from Borel–Cantelli [FrJ08, Lemma 18.3.4] that the set of all $\sigma\in\mathrm{Gal}(L)$ that belong to infinitely many sets $\beta^{-1}U_{\beta,l}$ has μ_L-measure 1. Hence, by the first paragraph of the proof, $\mu_{L,\beta}(U_\beta)=1$.

Finally, we choose a set of representatives B for $\mathrm{Gal}(K)$ modulo $\mathrm{Gal}(L)$. Thus, $\mathrm{Gal}(K)=\dot\bigcup_{\beta\in B}\beta\mathrm{Gal}(L)$ and $|B|=[L:K]$. Moreover, since $U_\beta\subseteq\beta\mathrm{Gal}(L)$, the sets $U_{\beta,l}$, where β ranges over B, are disjoint. Therefore, by the preceding paragraph, $\mu_K(\bigcup_{\beta\in B}U_\beta)=\sum_{\beta\in B}\mu_K(U_\beta)=\sum_{\beta\in B}(\mu_{L,\beta}(U_\beta)/[L:K])=\sum_{\beta\in B}(1/[L:K])=|B|/[L:K]=1$. By the definition of the U_β's, for each element of $\bigcup_{\beta\in B}U_\beta$ there are infinitely many $l\in\Lambda$ with $A_l(\tilde K(\sigma))\neq 0$. Hence, the set of all $\sigma\in\mathrm{Gal}(K)$ for which there exist infinitely many $l\in\mathbb{L}$ with $A_l(\tilde K(\sigma))\neq\emptyset$ has μ_K-measure 1, as claimed. $\square$

Acknowledgments. Part of this work was done during research visits of Moshe Jarden at the University of Kassel. We thank Wulf-Dieter Geyer and Aharon Razon for a careful reading of this work and the referee for helpful comments to an earlier version of it.

References

[Bor91] A. Borel, *Linear Algebraic Groups*, 2nd enlarged edn., Graduate Texts in Mathematics **126**, Springer, New York, 1991.

[Cad15] A. Cadoret, *An open adelic image theorem for abelian schemes*, Int. Math. Res. Not. IMRN **20** (2015), 10208–10242.

[CaT12] A. Cadoret and A. Tamagawa, *A uniform open image theorem for l-adic representations*, Duke Math. J. **161** (2012), 2605–2634.

[CaT13] A. Cadoret and A. Tamagawa, *A uniform open image theorem for l-adic representations II*, Duke Math. J. **162** (2013), 2301–2344.

[Eis95] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics **150**, Springer, New York, 1995.

[EnP10] A. J. Engler and A. Prestel, *Valued Fields*, Springer, Berlin, Heidelberg, 2010.

[FrJ08] M. D. Fried and M. Jarden, *Field Arithmetic*, 3rd edn., Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2008, Revised by Moshe Jarden.

[GaP13] W. Gajda and S. Petersen, *Independence of l-adic Galois representations over function fields*, Compositio Math. **149** (2013), 1091–1107.

[GeJ78] W.-D. Geyer and M. Jarden, *Torsion points of elliptic curves over large algebraic extensions of finitely generated fields*, Israel J. Math. **31** (1978), 157–197.

[GeJ05] W.-D. Geyer and M. Jarden, *Torsion of Abelian varieties over large algebraic fields*, Finite Field Theory Appl. **11** (2005), 123–150.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

[GoW10] U. Görtz and T. Wedhorn, *Algebraic Geometry I*, Vieweg + Teubner, Wiesbaden, 2010.

[Gro65] A. Grothendieck, *Éléments de Géométrie Algébrique IV, seconde partie*, Publ. Math. Inst. Hautes Études Sci. **24** (1965), 5–231.

[Gro66] A. Grothendieck, *Éléments de Géométrie Algébrique IV, troisième partie*, Publ. Math. Inst. Hautes Études Sci. **28** (1966), 5–255.

[Gro71] A. Grothendieck, *Revêtement étales et groupe fondamental (SGA 1)*, Lecture Notes in Mathematics **224**, Springer, Berlin, 1971.

[Har77] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977.

[JaJ84] M. Jacobson and M. Jarden, *On torsion of abelian varieties over large algebraic extensions of finitely generated fields*, Mathematika **31** (1984), 110–116.

[JaJ85] M. Jacobson and M. Jarden, *On torsion of abelian varieties over large algebraic extensions of finitely generated fields: erratum*, Mathematika **32** (1985), 316.

[JaJ01] M. Jacobson and M. Jarden, *Finiteness theorems for torsion of abelian varieties over large algebraic fields*, Acta Arith. **98** (2001), 15–31.

[Lan58] S. Lang, *Introduction to Algebraic Geometry*, Interscience Publishers, New York, 1958.

[Liu06] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford Graduate Texts in Mathematics **6**, Oxford University Press, Oxford, 2006.

[Mat80] H. Matsumura, *Commutative Algebra*, 2nd edn. Benjamin, Reading, 1980.

[Mil80] J. S. Milne, *Étale Cohomology*, Princeton University Press, Princeton, 1980.

[Mil85] J. S. Milne, "*Abelian varieties*", in *Arithmetic Geometry* (eds. G. Cornell and J. H. Silverman) Springer, New York, 1985.

[Mum74] D. Mumford, *Abelian Varieties*, Oxford University Press, London, 1974.

[Mum88] D. Mumford, *The Red Book of Varieties and Schemes*, Lecture Notes in Mathematics **1358**, Springer, Berlin, 1988.

[Ray70] M. Raynaud, *Anneaux Locaux Henséliens*, Lecture Notes in Mathematics **169**, Springer, Berlin, 1970.

[Ser65] J.-P. Serre, "*Zeta and L-functions*", in *Arithmetical Algebraic Geometry* (ed. Schilling) Harper and Row, New York, 1965, 82–92.

[Ser86] J.-P. Serre, *Groupes linéaires modulo p et points d'ordere fini des varietés abéliennes*, Note of a cours at Collège de France given in 1986, taken by Eva Bayer-Flukiger.

[Ser00] J.-P. Serre, *Œuvres. Collected Papers, IV, 1985–1998*, Springer, Berlin, 2000.

[Ser13] J.-P. Serre, *Un critère d'indépendance pour une famille de représentation l-adiques*, Comment. Math. Helv. **88** (2013), 451–554.

[SeT68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–571.

[Shi98] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions*, Princeton University Press, Princeton, 1998.

[Spr98] T. A. Springer, *Linear Algebraic Groups*, 2nd edn. Birkhäuser, Boston, 1998.

[Tat66] J. Tate, *Endomorphisms of Abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[Zyw16] D. Zywina, *Abelian varieties over large algebraic fields with infinite torsion*, Israel J. Math. **211** (2016), 493–508.

https://doi.org/10.1017/nmj.2017.33 Published online by Cambridge University Press

Moshe Jarden
School of Mathematics
Tel Aviv University, Ramat Aviv
Tel Aviv 6139001, Israel
jarden@post.tau.ac.il

Sebastian Petersen
Universität Kassel
Wilhelmshöher Allee 71–73
34121 Kassel, Germany
petersen@mathematik.uni-kassel.de